TECHNISCHE UNIVERSITÄT WIEN

Diploma Thesis

Delta-RCS Characterization of RFID Tags and Implications on Localization Accuracy

performed at the

Institute of Electrodynamics, Microwave and Circuit Engineering
Technische Universität Wien

supervised by

Assoc. Prof. Dipl.-Ing. Dr. techn. Holger Arthaber
and
Univ. Ass. Dipl.-Ing. Bernhard Pichler, BSc.

by

Daniel Neunteufel, BSc.
Matr. Nr. 1026984
Pfeilgasse 3A/846, 1080 Vienna

Vienna, January 17, 2018

Abstract

Radio-frequency identification (RFID) is widely deployed nowadays. Intentionally used for identification purposes, the extension to the localization of RFID tags is a rather new topic, which is still under development.
One novel technique uses small amplitude wideband signals superimposed on a continuous wave carrier for time-of-flight based localization. In this context, the so-called delta radar cross-section of tags is an essential parameter. It describes the generally complex-valued difference between the two possible states of reflection which a tag can show during tag-to-interrogator communication. For this, an extension of the scalar radar cross-section to a complex value is necessary.
A comprehensive measurement system capable of determining the delta radar cross-section in different frequency bands, for different power levels, and for different incident angles of the electromagnetic waves is not commercially available so far. The development and assembly of such a system is in the main focus of this thesis.
The developed system is used to examine several different passive tags in the UHF frequency range around 900 MHz and in the ISM band around 2.45 GHz. Furthermore, a 2.45 GHz electronic shelf label is modified to allow for battery assisted backscatter modulation. The delta radar cross-section values of the tags are analyzed and compared regarding their behavior over frequency, power, and spatial angle.
Besides that, the interferences situation in a typical electronics retail store is analyzed with regard to the possible use of the introduced wideband signal based localization technique in the ISM bands in such an environment.

Kurzfassung

Radio-frequency identification (RFID) ist eine heute bereits weit verbreitete Technik, die in ihrer ursprünglichen Anwendung zur Identifikation von Objekten dient. Das Lokalisieren von RFID Tags ist hingegen ein neues Anwendungsfeld, das sich derzeit noch weitgehend in Entwicklung befindet.
Ein solches neuartiges Lokalisierungsverfahren basiert auf breitbandigen Signalen mit kleiner Amplitude, welche einem stärkeren Continuous-Wave Träger überlagert werden. Dies ermöglicht Laufzeitmessungen und damit eine Lokalisierung der Tags. In diesem Zusammenhang ist der sogenannte Delta-Radarquerschnitt eines Tags ein essenzieller Parameter. Er beschreibt die im Allgemeinen komplexwertige Differenz zwischen den zwei möglichen Radarquerschnitten, die ein Tag für die Kommunikation mit einem RFID-Reader verwendet. Dafür ist eine Erweiterung des skalaren Radarquerschnittes auf eine komplexe Größe notwendig.
Ein umfassendes Messsystem, welches das Erfassen des Delta-Radarquerschnitts für verschiedene Frequenzen, Leistungspegel und Einfallswinkel der elektromagnetischen Wellen ermöglicht, ist kommerziell nicht verfügbar. Die Entwicklung und der Aufbau eines solchen Messsystems stehen daher im Mittelpunkt der vorliegenden Arbeit.
Dieses Messsystem wird anschließend dafür genutzt, verschiedene passive Tags bei UHF Frequenzen um 900 MHz und im ISM Band bei 2.45 GHz zu charakterisieren. Außerdem wird ein batteriebetriebenes, sogenanntes Electronic Shelf Label dahingehend modifiziert, dass es auf Basis von Radarquerschnittsmodulation bei 2.45 GHz ebenfalls als Testobjekt für das Lokalisierungsverfahren dienen kann.
Neben diesen Messungen wird auch der Einfluss von Störquellen in ISM Bändern in großräumigen Elektrofachmärkten analysiert. Dies geschieht in Hinblick auf die potenzielle Anwendung des erwähnten Lokalisierungsverfahrens in einer solchen Umgebung.

Acknowledgements

First of all, I would like to thank my parents for their great support and also all the friends who have accompanied me on my journey so far.

Further, I am very grateful for all the advice I received from the members of the Microwave Engineering Group at TU Wien, especially Florian Galler. I could count on their great expertise any time.

Thanks also to SES-imagotag for providing test objects and supporting this work.

Table of Contents

1 Introduction **1**

2 RFID & Localization **3**
2.1 Localization of RFID Tags . . . 3
2.2 Delta Radar Cross-Section . . . 7
2.2.1 Definition RCS . . . 7
2.2.2 Definition ΔRCS . . . 10
2.2.3 Measurement of the ΔRCS . . . 12
2.3 Potential DUTs . . . 14
2.4 Interferences . . . 16

3 ΔRCS Measurement Setup **18**
3.1 Requirements . . . 19
3.2 Components & Functionality . . . 19
3.2.1 Measurement Device . . . 20
3.2.2 Carrier Signal Generation . . . 20
3.2.3 Carrier Cancellation . . . 24
3.2.4 EPC Communication & Triggering . . . 30
3.2.5 Anechoic Chamber . . . 31
3.2.6 Band Separation . . . 33
3.3 Measurement Setup Overview . . . 34
3.3.1 Block Diagram . . . 34
3.3.2 Link Budget . . . 36
3.4 Calibration . . . 38
3.4.1 Theory . . . 39
3.4.2 Source Calibration . . . 42
3.4.3 Forward Path Calibration . . . 43
3.4.4 Backward Path Calibration . . . 44
3.4.5 Surface Power Density Calibration . . . 46
3.5 Parameters & Postprocessing . . . 46
3.5.1 Parameters . . . 47
3.5.2 Postprocessing . . . 48

4 Results **50**
4.1 System Verification Measurement . . . 50
4.2 UHF-Measurements . . . 53
4.2.1 Power Dependency – Minimum Surface Power Density . . . 53
4.2.2 Scalar ΔRCS . . . 54
4.2.3 Group Delay . . . 55
4.3 DUTs at 2.45 GHz ISM Band . . . 60
4.3.1 Power Dependency . . . 60
4.3.2 Scalar ΔRCS . . . 60
4.3.3 Group Delay . . . 61

5 Noise Level Measurement **66**
5.1 Measurement Setup . . . 66
5.2 Results . . . 68

6 Implications for Localization Accuracy **71**
6.1 ΔRCS of Tags . . . 71
6.2 Noise Level . . . 72

7 Conclusion & Outlook **73**

A Modifications of the Anechoic Chamber **74**
A.1 Additional Absorbers . . . 74
A.2 Installation Tutorial . . . 75

B Active Backscatter Modulation Circuit **78**

References **80**

List of Figures

2.1 DSSS Path Diagram . . . 6
2.2 Measurement Setup for Radar Targets . . . 8
2.3 Equivalent Circuit RFID Tag Input Stage . . . 11
2.4 Modulation States of an RFID Tag . . . 11
2.5 EPC Miller Sequences . . . 15
2.6 SES-IMAGOTAG Electronic Shelf Label . . . 16

3.1 Measurement Setup Overview . . . 18
3.2 Phase Noise Illustration . . . 21
3.3 Block Diagram VSA . . . 21
3.4 Carrier Signal Generation Block Diagram . . . 22
3.5 Source Phase Noise . . . 23
3.6 Phase Noise Comparison . . . 23
3.7 CC Reflections . . . 25
3.8 CC Principle . . . 26
3.9 CC Block Diagram . . . 27
3.10 CC IQ Diagram . . . 28
3.11 EPC Modulation . . . 31
3.12 Anechoic Chamber . . . 32
3.13 Mounted Tag . . . 32
3.14 Full Measurement Setup Block Diagram . . . 35
3.15 Full Measurement Setup Picture . . . 36
3.16 Measurement System Link Budget . . . 37
3.17 Three-Term Error Model . . . 39
3.18 RCS Calculation Concept: Probe & Tag . . . 41
3.19 Forward Path Calibration . . . 44
3.20 Backward Path Calibration . . . 44
3.21 Backscatter Signal Example . . . 48
3.22 Backscatter Signal IQ Diagram. . . . 49

4.1 Planar Reference Target . . . 52
4.2 RCS Planar Reference Target . . . 52
4.3 DUTs UHF Range . . . 53
4.4 Non-linear ΔRCS . . . 54
4.5 Minimum Surface Power Density . . . 54
4.6 Polar Minimum Surface Power Density . . . 55

4.7 ΔRCS over Frequency . . . 56
4.8 Polar delta radar cross-section (ΔRCS) . . . 57
4.9 Group Delay over Frequency . . . 58
4.10 Phase over Frequency . . . 59
4.11 ESL as DUT . . . 60
4.12 Power Dependency ISM DUTs . . . 61
4.13 ΔRCS over Frequency ISM . . . 62
4.14 Polar ΔRCS ISM . . . 63
4.15 Frequency-Angle Dependency ISM REFlex . . . 64
4.16 Group Delay over Frequency ISM . . . 64
4.17 Phase over Frequency ISM . . . 65

5.1 Noise Level Measurement Overview . . . 67
5.2 Measurement Setup . . . 68
5.3 Spectrograms . . . 69
5.4 Band Occupancy . . . 70

A.1 Uncovered *Phi*-Stage . . . 75
A.2 End Stop Sensors . . . 75
A.3 End Stop Sensor Connection . . . 76
A.4 Absorber Table . . . 76
A.5 Cylindrical Center Absorber . . . 77
A.6 Additional Spacers . . . 77
A.7 Pillar . . . 77
A.8 Additional Absorbers . . . 77

B.1 Backscatter Modulation Circuit . . . 79

List of Tables

3.1 Frequency Bands Overview 33

4.1 Spherical Reference Target 51
4.2 Planar Rectangular Reference Target 52

B.1 Backscatter Modulation Circuit Components 78
B.2 Backscatter Modulation Circuit Parameters 79

Abbreviations

BLF backscatter link frequency

BPF band-pass filter

CC carrier cancellation

DAC digital-to-analog converter

DANL displayed average noise level

ΔRCS delta radar cross-section

DSSS direct-sequence spread spectrum

DUT device under test

ESL electronic shelf label

EPC electronic product code

FSPL free space path loss

ISM industrial, scientific, and medical (radio band)

ITU international telecommunication union

LNA low-noise amplifier

LO local oscillator

PN phase noise

PSD power spectral density

RCS radar cross-section

RFID radio-frequency identification

SNR signal-to-noise ratio

ToF time-of-flight

UHF ultra high frequency

VSA vector signal analyzer

1 Introduction

Radio-frequency identification or RFID nowadays is a widely deployed wireless technology. It is used for identifying and tracking of objects. Possible applications are wherever one or more readers at fixed locations should track and identify a mobile tag or even entire populations of tags. However, also reversed roles are possible.
Being such a versatile technique, RFID has gained more and more popularity over the last years. In retail trade it is used for asset tracking, item-level tagging, and general supply chain management. Biometric e-passports have been introduced all around the world. RFID microchips are implanted in pets and stock to allow for identification. Just recently, approaches were even made by companies to inject RFID microchips in their employees [1]. In this case, while allowing for convenient access management and cashless payment on the one hand, privacy concerns may rise on the other hand. It goes without saying that, as always, with great power comes great responsibility and that a reasonable handling of this topic is essential. Not least, broad acceptance by the users is a major key for long term success of a product and even entire technologies.

An RFID system in general consists of two parts. A reader or interrogator and a transponder or tag. Communication may take place using a half-duplex link. In this case, the reader provides a continuous wave signal which is modulated using amplitude-shift keying (ASK) during the reader-to-tag communication. The subsequent tag-to-reader link is based on the use of different impedance states connected to the antenna of the tag, internally. This leads to a modulation of the radar cross-section (RCS) and hence a varying amount of energy scattered back from the tag towards the reader antenna.
Tags may be entirely passive like it is suggested in the electronic product code (EPC) specifications [2]. In this form of application, the tag solely uses the electromagnetic field of the continuous wave signal of the reader as a power supply at any time.
Additionally, systems with tags using an internal power supply, e.g. in form of a battery may be used. Apart from this the same half-duplex communication link is used.
As for the used frequency band, [2] for example specifies a range from 860 MHz to 960 MHz. In fact, the actual band in use is subject to national regulations. In Europe, for instance, the frequency ranges allocated to ultra high frequency (UHF) RFID are 865 MHz to 868 MHz and 915 MHz to 921 MHz, as stated in the according ETSI standard [3].
Another prominent example based on the RFID technology is near field communication (NFC). It makes use of the industrial, scientific, and medical (ISM) radio band at 13.56 MHz.

While identification is the initial purpose of the RFID technology, providing the possibility to locate the tags becomes more and more a desired feature these days. For this, several techniques have been proposed in the past. The use of a broadband sequence superimposed on the original continuous wave signal of the reader for example is highly promising. The use of this direct-sequence spread spectrum (DSSS) technique is described in [4]. An actual implementation of this concept can be found in [5]. The thesis at hand is based on the technique described there and meant to allow for further improvement.

The aspect that is to be examined here is the description of tags in terms of their so-called delta radar cross-section (ΔRCS). In the simplest case, the ΔRCS can be seen as a scalar value with unit square meter or decibel relative to one square meter (dBsm), similar to the well-known property RCS of radar targets. In fact, it describes the difference between two states of RCS. A more sophisticated description of this parameter is the extension to complex-valued ΔRCS. This is based on the fact, that the impedance connected to the antenna within the chip of the RFID tag is complex-valued in general. Therefore, a change between two impedance states not only changes the amplitude of the backscattered wave, but also the phase. This requires a well-defined reference plane and a suitable calibration to obtain this phase information.
The development and implementation of a measurement system that provides a solution for a comprehensive determination of the ΔRCS is the main focus of this work. This comprises the ΔRCS of tags in dependence on frequency as well as direction in space. Since the possibilities for localization using broadband signals such as DSSS are limited in the relatively narrow standard UHF band, the extension to the ISM bands at 2.45 GHz and 5.8 GHz is envisaged. Hence, a ΔRCS characterization of tags in this context is also desired. All of the mentioned features that the current off-the-shelf measurement solutions are not able to provide in this extent.

Besides the measurement system, a second point shall be covered in this work. Leaving the reserved UHF band at 865 MHz and extending the localization to the ISM bands leads to inevitable conflicts with other services using these open bands. There, the proposed ranging and localization technique for RFID tags is competing with e.g. wireless local area networks (Wireless LAN) or BLUETOOTH®. Interference resulting from those services has to be considered when implementing such an application. Measurements in real world scenarios are conducted and described, to assess the general situation in environments where the RFID localization could be used, such as shopping malls and large stores.

2 RFID & Localization

This chapter is an introduction on the basic concepts this work is based on as well as the theoretical background and the possible devices under test (DUTs).
Although RFID in general comprises a wide range of standards, the work at hand strongly relates to the EPCglobal Class-1 Generation-2 specification. The measurement system described within this thesis is designed to cover the frequency range specified there, that is 860 MHz to 960 MHz. The additional ISM frequency bands around 2.45 GHz and 5.8 GHz are not to be seen so much in the context of RFID, but rather from a mere localization point of view. This is meant to be added *"on top"* of the RFID functionality.

Section 2.1 gives an overview of available localization techniques for RFID. While for most of them only a short outline will be given, the one based on DSSS will be described in detail. The connection to the ΔRCS of tags in this context will be explained. In section 2.2 the concept of radar cross-section and delta radar cross-section is given. An extension to a complexed valued ΔRCS and a possible measurement principle will be introduced. The description of the actual implementation can be found in chapter 3. Section 2.3 contains an overview of possible DUTs as well as a short introduction on the EPC specifications. Since the technical details of the communication procedures between interrogator and tag are not so much of relevance in the scope of this work, only a very brief overview is given. For more information on this standard refer to [2]. Finally, in section 2.4 some considerations regarding problems with interfering services will be described. Also, some basic background on the ISM bands will be given.

2.1 Localization of RFID Tags

The original functionality of RFID is only the identification of certain objects provided with a tag. Localization is a feature added later on top of this. Hence, a major point is the compliance of localization techniques with the already existing standards and regulations regarding RFID. On the other hand, by using battery-less tags, very energy efficient and long-living ways of localization can be implemented.
An overview on the topic can be found in [6]. A short summary of localization principles is given here:

- **Received Signal Strength Indication (RSSI)**

  According to the radar equation[1], the power of the signal reflected by a passive tag back to the interrogator is inversely proportional to the fourth power of the distance between the tag and the interrogator. Measuring the received power allows to estimate this distance. By deploying multiple receivers, the distance information gathered can be used for trilateration and thus, estimation of the position of the tag.

- **Time-of-Flight (ToF)**

  The round-trip ToF principle is based on the measurement of the time it takes an electromagnetic wave to travel there and back over the distance between the interrogator and the tag. A modulated sine wave signal (e.g. pulsed) may be used. With the known propagation velocity of waves in free space, the distance can be calculated. Similar to the RSSI principle, the position of the tag can then be calculated. Additionally, the fact that the backscattered signal is modulated by the tag allows it in principle to distinguish it from reflections coming from other objects.

- **Angle of Arrival (AoA)**

  The so-called radio-goniometry, which makes use of the angle of the incoming electromagnetic wave, can be used for a position estimation. This technique requires multiple antennas or even an entire antenna array at one end of the communication link, usually at the interrogator side. By comparing the phase difference of the signals received by different antennas, the angle can be calculated. Again, multiple receivers can be deployed, which allows for triangulation and estimation of the position of the tag.

For all this basic localization principles, there are some important terms and issues that have to be considered in this context. Those are:

- **Standard Tag vs. Modified Tag**

  An important question is if it is necessary to add additional functionality to the RFID tag itself to facilitate the desired localization technique. The EPC standard allows for the implementation of custom commands. Such commands may be used to perform some localization specific tasks.
  Another option is to allow the tag to utilize a larger frequency range than initially intended. An extension to higher frequencies provides larger bandwidths which again has the potential to improve the localization accuracy. However, this is not possible without hardware modification to the tags.
  Besides these possible modifications, the most convenient and versatile way is to use off-the-shelf tags and a localization principle which can be used independently of the underlying RFID protocols and hardware.

[1] The radar equation is introduced in section 2.2.1.

- **Signal Processing**

  The signal processing load for localization techniques might be considerably large. Hence, it is not feasible to deploy the signal processing part in the passive tag. Even for common RFID readers, the requirements may exceed their default capabilities. An implementation using more hardware resources may be necessary.
  Furthermore, for localization scenarios where more readers at different locations are in use, they have to be connected which means additional effort regarding networking.

- **Mobile Reader**

  In contrast to concepts utilizing several RFID readers at fixed locations in order to track a mobile node in form of a tag, the reverse principle is also possible. A designated area is provided with numerous tags at fixed and known locations as part of the infrastructure of a so-called "smart space". Measuring the distances to the tags in range allows the mobile reader to determine its location.

There is also a novel, highly promising technique for ranging, based on a ToF measurement using DSSS. This is the base for this work and is therefore introduced in detail in what follows.

Direct-Sequence Spread Spectrum (DSSS) Localization Technique

The basic idea of the ranging technique introduced in [4] is the superposition of a cyclic, low-power DSSS signal onto the standard continuous wave signal of the reader during the tag-to-interrogator communication. In equivalent baseband form the normalized transmission signal can be written as

$$s_{tx}(t) = 1 + a\, s_{dsss}(t \bmod T_{dsss}) \ , \tag{2.1}$$

where the continuous wave appears as a constant to which the DSSS signal with amplitude a is added. With "$x \bmod y$" denoting the modulo function, it repeats after the fixed time T_{dsss}. Due to the low-power used for this sequence this method is able to fulfill the spectral mask requirements of the EPC Class-1 Generation-2 standard, despite the fact, that the bandwidth is much wider than the narrow bands used for the actual RFID functionality. The received signal consists of a part which is scattered back from the tag and thus, is modulated by the tag according to the EPC standard together with the superimposed DSSS sequence. Beside this, also a static component appears which results from non-ideal decoupling of the transmit and the receive path and reflections not stemming from the tag. Again, in equivalent baseband this can be expressed as

$$s_{rx}(t) = \left(\left[h_{cpl} + h_{dl} * h_{tag}^{m(t)} * h_{ul} \right] * s_{tx} * h_{tx} * h_{rx} \right)(t) + n(t) \ , \tag{2.2}$$

with the impulse responses $h_{cpl}(t)$ for the static component, $h_{dl}(t)$ and $h_{ul}(t)$ for the downlink and the uplink path between the interrogator and the tag, respectively, $h_{tag}^{m(t)}(t)$ for the tag in its modulation state $m(t) \in \{0, 1\}$ and $h_{tx}(t)$ and $h_{rx}(t)$ for the transmit and receive paths of the interrogator, including the according antennas, as well as the received

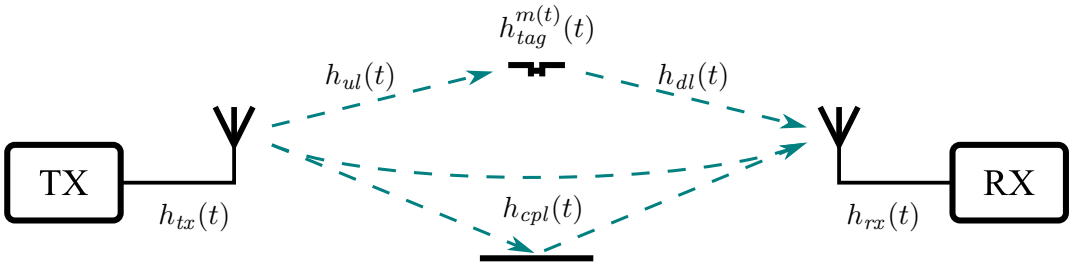


Figure 2.1: Example of a bistatic localization scenario with the impulse responses of the involved paths and the (passive) tag, respectively.

noise $n(t)$, with "$*$" denoting the convolution operation. An overview of the involved quantities is given in Fig. 2.1.
By making use of the cyclic nature of the DSSS sequence the received sequence can be segmented and aligned with the modulation states of the tag response, such that a whole DSSS sequence fits into each modulation state, respectively. Demodulating the received tag response allows to separate the sections of the received signal into two sets of signal sections corresponding to the two modulation states of the tag, containing always one DSSS sequence. With this, a set averaging can be carried out for the two sets belonging to the two modulation states, respectively. Assuming that the occurrence of the two modulation states is uniformly distributed, i.e. they occur equally often, subtracting the two averaged signals results in

$$s'_{avg}(\tau) = \frac{1}{2}\Big(s_{tx} \otimes h_{tx} \otimes h_{rx} \otimes h_{dl} \otimes h_{ul} \otimes \left[h^0_{tag} - h^1_{tag}\right]\Big)(\tau) + n_{avg}(\tau) \ , \tag{2.3}$$

with the adjusted time variable $\tau = [0, T_{dsss}[$, where $h_{cpl}(t)$ and hence all static coupling entirely disappears. Here, "$\otimes$" denotes the circular convolution. For ranging, this signal can be correlated with the initial DSSS sequence to obtain

$$s_{corr}(\tau) = \left(s'_{avg} \star s_{dsss}\right)(\tau) \ , \tag{2.4}$$

which becomes

$$s_{corr}(\tau) = G_{tx}\, G_{rx}\, G_{dl}\, G_{ul}\Big(\left[h^{\Delta}_{tag} \otimes s_{tx}\right] \star s_{dsss}\Big)(\tau - T_{dl} - T_{ul}) + \left(n_{avg} \star s_{dsss}\right)(\tau) \ , \tag{2.5}$$

when assuming flat frequency responses for the antennas, i.e. $h_{tx}(t) = G_{tx}\ \delta(t)$ and $h_{rx}(t) = G_{rx}\ \delta(t)$, and flat frequency response delay channels for downlink and uplink, i.e. $h_{dl}(t) = G_{dl}\ \delta(t - T_{dl})$ and $h_{ul}(t) = G_{ul}\ \delta(t - T_{ul})$, with "$\star$" denoting the cyclic cross-correlation and "$\delta(t)$" the Dirac delta function. Furthermore, the differential tag impulse response is defined as

$$h^{\Delta}_{tag}(t) := \frac{1}{2}\left[h^0_{tag} - h^1_{tag}\right](t) \ . \tag{2.6}$$

The time-of-flight $T_{tof} = T_{dl} + T_{ul}$ can be directly estimated by comparing eq. (2.5) with the cross-correlation $\left(s_{tx} \star s_{dsss}\right)(\tau)$, in case also the differential tag impulse response $h^{\Delta}_{tag}(t)$ can be assumed to be frequency flat.
Since such a frequency flat tag response can only be an approximation of the actual behavior of the tag, $h^{\Delta}_{tag}(t)$ has to be known in order to perform equalization and improvement

of the ranging result. In frequency domain this differential impulse response corresponds to the ΔRCS over frequency. It becomes clear that the ΔRCS plays an essential role for the DSSS localization technique. Therefore, a further examination of this parameter is necessary.

2.2 Delta Radar Cross-Section

The RCS in general is a measure to allow characterizing radar targets. In the case of RFID tags, tag to interrogator communication is based on two defined back-scatter states of the tag. The information sent by the tag is coded into the modulation between these two states. The actual difference in magnitude and phase between the two back-scattered waves, corresponding to the two different states, determines the signal-to-noise ratio (SNR) the interrogator experiences. As explained in section 2.1, in the case of DSSS-localization, the difference and even the differential impulse response are of interest when using the cross-correlation eq. (2.5).
In order to calculate this differential impulse response, the complex-valued ΔRCS over frequency has to be known. The measurement setup shown in this work has the purpose of determining precisely this. For this, a clear definition of the complex-valued ΔRCS is necessary and therefore, shown in what follows. It is done step-by-step, starting from the simple scalar RCS.

2.2.1 Definition RCS

Scalar RCS

According to the well-known radar equation as it is described e.g. in [7], the incident surface power density S_i, resulting from a highly directive probe antenna with gain G at a certain measurement distance R, fed with a transmit power P_t is given by

$$S_i = \frac{P_t G}{4\pi R^2} \ . \tag{2.7}$$

A target at this distance will re-radiate a certain amount of power, depending on its RCS, denoted as σ. The RCS has the unit of area and describes the size of the target as seen by the radar[2]. After traveling again the distance R, back to the probe antenna, the reflected wave causes a surface power density of

$$S_r = S_i \ \sigma \ \frac{1}{4\pi R^2} \ , \tag{2.8}$$

at the position of the probe antenna. With an effective antenna area of the antenna A_{eff}, the received power is

$$P_r = S_r \ A_{\mathit{eff}} = \frac{P_t G}{4\pi R^2} \ \sigma \ \frac{A_{\mathit{eff}}}{4\pi R^2} \ . \tag{2.9}$$

[2] Although the RCS has a dimension of square meters, it is not only related to the actual size of the targeted object. Parameters as shape, orientation in space and the nature of its surface may also influence this value.

Using the relationship between the receiving effective area of the antenna A_{eff} and its transmitting gain G, given by

$$G = \frac{4\pi}{\lambda^2} A_{eff} \ , \tag{2.10}$$

where λ denotes the wavelength in air, the RCS of the target can be expressed as

$$\sigma = \frac{P_r}{P_t} \frac{4\pi R^4}{G^2} \left(\frac{4\pi}{\lambda}\right)^2 \ . \tag{2.11}$$

The use of the antenna gain and spherical waves here implicitly require far field conditions.

Despite being a very intuitive approach to RCS, the definition eq. (2.11) lacks any phase information. In order to allow for a more advanced description, necessary to define a complex-valued ΔRCS later on, a slightly different approach using electric field strengths is more suitable here.

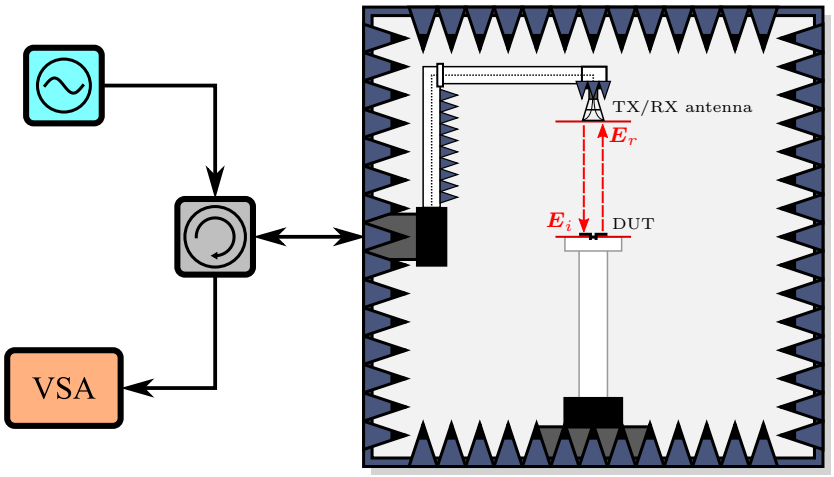


Figure 2.2: Schematic of a measurement setup for radar targets in an anechoic chamber. The source signal is applied to the antenna in the anechoic chamber via a circulator, which at the same time redirects the reflected wave towards a vector signal analyzer. $\boldsymbol{E}_i$ and $\boldsymbol{E}_r$ represent the electric field strength of the incident and the reflected wave in air, respectively.

A possible *monostatic* measurement setting for radar targets (e.g. RFID tags) in an anechoic chamber[3] is shown in Fig. 2.2. Monostatic means that only one probe antenna is used for both the transmitting and the receiving path. This is in accord with the actual setting used in this work as described later in chapter 3.

Sticking to the concept of surface power density introduced in eq. (2.7), this means a well-known relationship to the complex-valued (bold letters) electric field strength of the incident electromagnetic wave at the reference plane of the DUT of

$$S_i = \frac{|\boldsymbol{E}_i|^2}{2Z_0} \ , \tag{2.12}$$

[3] More details on the anechoic chamber follow in section 3.2.5 and appendix A.

where $Z_0 \approx 376.73\,\Omega$ is the impedance of free space [8].
Analogous to eq. (2.8), for the surface power density at the position of the probe antenna the following is true

$$S_r = S_i \, \sigma \, \frac{1}{4\pi R^2} \, . \tag{2.13}$$

Using this relation and expressing S_r in terms of electric field strength as

$$S_r = \frac{|\boldsymbol{E}_r|^2}{2Z_0} \, , \tag{2.14}$$

the RCS can be defined as

$$\sigma := 4\pi \lim_{R\to\infty} R^2 \left| \frac{\boldsymbol{E}_r}{\boldsymbol{E}_i} \right|^2 \, . \tag{2.15}$$

The limit $R \to \infty$ in eq. (2.15) ensures far-field conditions. These conditions can be assumed to be fulfilled in what follows and thus, the limit operator is omitted.
It should be noted, that the received electric field strength at the probe antenna $\boldsymbol{E}_r$ is the result of a spherical wave, originating in the phase center of the DUT. The fact, that $\boldsymbol{E}_r$ in a certain distance to the DUT is considered, allows for a defined measurement of the RCS using this definition.

Complex RCS

The definitions considered so far still leave the question regarding a complex-valued RCS unanswered. A possible extension to such a RCS definition is explained in [9]. The concept shown there does not disregard the phase information of the fraction $\frac{\boldsymbol{E}_r}{\boldsymbol{E}_i}$ by using only its absolute value, which is in contrast to eq. (2.15). Instead, $\boldsymbol{E}_r$ is examined further using a fictitious scattered field strength $\boldsymbol{E}_s$ in a very close proximity to the DUT with distance R_0 is introduced. Due to isotropic radiation, this field results in a received field strength

$$\boldsymbol{E}_r(R) = \frac{\sqrt{4\pi R_0^2}}{\sqrt{4\pi R^2}} \, e^{-jk_0(R-R_0)} \, \boldsymbol{E}_s \, , \tag{2.16}$$

at a distance R. Here, k_0 is the wavenumber for a given frequency in free space, which is defined as

$$k_0 = \frac{2\pi}{\lambda_0} = \frac{2\pi f}{c_0} \, . \tag{2.17}$$

Taking a closer look at eqs. (2.13) to (2.15), reveals that in fact the introduction of $\boldsymbol{E}_r$ already comprises a correction by a factor $1/\sqrt{4\pi R^2}$. This is necessary, since a metrological characterization in the immediate vicinity of the DUT is not feasible. Mathematically, a singularity occurs, while physically, the necessary far-field conditions are not fulfilled any more.
Analogously, the phase information of $\frac{\boldsymbol{E}_r}{\boldsymbol{E}_i}$ can be kept and corrected in a similar manner, using the phase propagation term $e^{-jk_0(R-R_0)}$ of eq. (2.16). To allow for a general definition, $R_0 \ll \lambda_0$ is assumed in any case, which means that R_0 can be neglected in the phase correction.
Finally, this leads to an expression for the complex-valued RCS

$$\begin{aligned} \boldsymbol{\sigma} &= 4\pi R^2 \left(\frac{1}{e^{-jk_0R}} \frac{\boldsymbol{E}_r}{\boldsymbol{E}_i} \right)^2 \\ &= 4\pi R^2 \, e^{j2k_0R} \left(\frac{\boldsymbol{E}_r}{\boldsymbol{E}_i} \right)^2 \, . \end{aligned} \tag{2.18}$$

Defining further the complex-valued *square-root RCS*

$$\left[\sqrt{\boldsymbol{\sigma}}\right] := \sqrt{4\pi R^2}\, e^{jk_0R}\, \frac{\boldsymbol{E}_r}{\boldsymbol{E}_i}\ , \tag{2.19}$$

allows for another way of representing the RCS in its special quadratic form eq. (2.18) as

$$\boldsymbol{\sigma} = \left(\left[\sqrt{\boldsymbol{\sigma}}\right]\right)^2\ . \tag{2.20}$$

In contrast to the power quantity $\boldsymbol{\sigma}$ (RCS), the square-root RCS $\left[\sqrt{\boldsymbol{\sigma}}\right]$ has the nature of a field or root-power quantity. This has the advantage, that no phase ambiguity is introduced by squaring the measured factor $\frac{\boldsymbol{E}_r}{\boldsymbol{E}_i}$.
In this context it should be emphasized, that the term $\left[\sqrt{\boldsymbol{\sigma}}\right]$ does not simply represent one of the two possible solutions of $\sqrt{\boldsymbol{\sigma}}$, but is the unambiguous result of the correction of the directly measured $\frac{\boldsymbol{E}_r}{\boldsymbol{E}_i}$.

Obviously, the (linear) scalar RCS can be obtained from this expression by

$$\begin{aligned}\sigma &= |\boldsymbol{\sigma}| \\ &= \left|\left[\sqrt{\boldsymbol{\sigma}}\right]\right|^2\ .\end{aligned} \tag{2.21}$$

The widely-used (logarithmic) representation of RCS in terms of decibel referenced to one square-meter (dBsm) is be obtained as

$$\begin{aligned}\sigma(\text{dBsm}) &= 10\log_{10}\left(\frac{\sigma}{1\,\text{m}^2}\right) \\ &= 20\log_{10}\left(\frac{\left|\left[\sqrt{\boldsymbol{\sigma}}\right]\right|}{\sqrt{1\,\text{m}^2}}\right) &(2.22)\\ &= 20\log_{10}\left(\left|\frac{\boldsymbol{E}_r}{\boldsymbol{E}_i}\right|\right) + 10\log_{10}\left(\frac{4\pi R^2}{1\,\text{m}^2}\right)\ . &(2.23)\end{aligned}$$

While the magnitude representation makes use of the power quantity RCS, it is not suitable for the angle. Here, the argument of the field quantity square-root RCS is used to represent the obtained results as

$$\arg\left(\left[\sqrt{\boldsymbol{\sigma}}\right]\right) = \arg\left(\frac{\boldsymbol{E}_r}{\boldsymbol{E}_i}\right) + k_0R\ . \tag{2.24}$$

This concept shown here is similar to the representation of S-parameters as magnitude in decibel and argument in degree. In fact, just like S-parameters, RCS describes the relation between two power waves. Thus, this representation will be used in what follows.

2.2.2 Definition ΔRCS

In contrast to the RCS, the ΔRCS is nonzero only in the case of a change in the behavior of the radar target. This very behavior is the distinct property of an RFID tag. Therefore, it is best understood taking a closer look on such a tag.
A simplified equivalent circuit of the possible input stage of an RFID tag is shown in Fig. 2.3. For the ΔRCS, the antenna and modulator part is of interest. The two different modulation impedances $Z_m^{(a)}$ and $Z_m^{(b)}$ represent the two different backscattering states. In

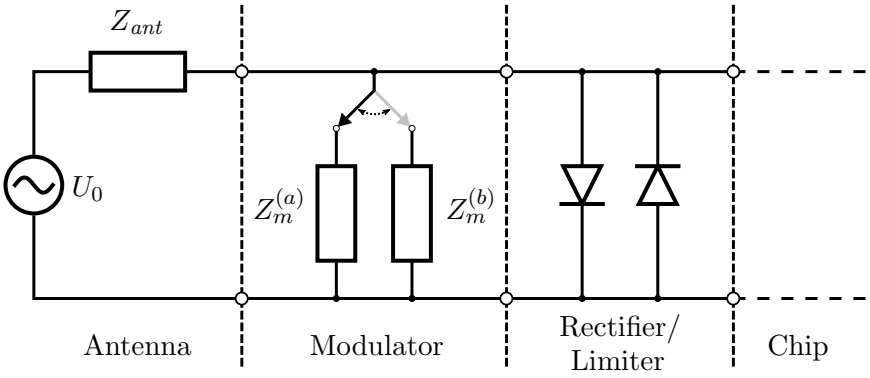


Figure 2.3: Equivalent circuit of an RFID tag input stage. The chip is assumed to have a high input impedance here.

a real system this modulation may be achieved by simply switching a transistor on and off to achieve different reflection coefficients.
In general, the modulation impedances are complex-valued. Hence, the modulator input port may exhibit any possible complex reflection coefficient. Thus, also the respective RCS values are complex-valued in general. Therefore, it is not sufficient to use the mere difference between the scalar RCS values corresponding to the two states to obtain the actual ΔRCS. This is only possible in the case of no phase difference between the two states. Since this phase difference does not only depend on the actual modulation impedances of the chip, but also the respective matching of these impedances to the antenna impedance Z_{ant} of the tag, the situation becomes too complex to derive the correct result from the two scalar RCS states. A more sophisticated description of the situation can be provided using the square-root RCS as defined in eq. (2.19).

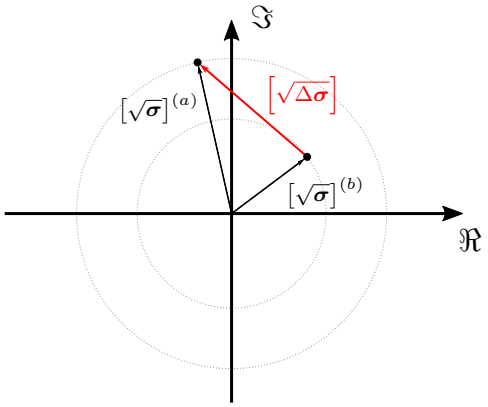


Figure 2.4: Schematic representation of the possible modulation states of an RFID tag in the complex IQ plane including the ΔRCS. In terms of $\left[\sqrt{\boldsymbol{\sigma}}\right]$.

An example of two measured square-root RCS values for the two different modulation states $\left[\sqrt{\boldsymbol{\sigma}}\right]^{(a)}$ and $\left[\sqrt{\boldsymbol{\sigma}}\right]^{(b)}$ of a tag are shown in Fig. 2.4. As it can be seen clearly, the difference of the squared absolute values corresponding from the scalar RCS does not represent the modulation depth of the system at all. Also, the angular dependence becomes clear. The appropriate definition of the RCS has to make use of the magnitude as well as the angle information. This may be expressed as the complex-valued *square-root delta*

radar cross-section

$$\left[\sqrt{\Delta\boldsymbol{\sigma}}\right] := \left[\sqrt{\boldsymbol{\sigma}}\right]^{(a)} - \left[\sqrt{\boldsymbol{\sigma}}\right]^{(b)} \ , \tag{2.25}$$

using the square-root RCS values of the two possible modulation states (a) and (b), as it is also introduced for example in [10]. Analogous to eqs. (2.21) to (2.24), the ΔRCS can be reduced to a scalar value as

$$\begin{aligned} \Delta\sigma &= |\Delta\boldsymbol{\sigma}| \\ &= \left|\left[\sqrt{\Delta\boldsymbol{\sigma}}\right]\right|^2 \ . \end{aligned} \tag{2.26}$$

This as well can be expressed in magnitude given in dBsm

$$\begin{aligned} \Delta\sigma(\mathrm{dBsm}) &= 10\log_{10}\left(\frac{\Delta\sigma}{1\,\mathrm{m}^2}\right) \\ &= 20\log_{10}\left(\frac{\left|\left[\sqrt{\Delta\boldsymbol{\sigma}}\right]\right|}{\sqrt{1\,\mathrm{m}^2}}\right) \qquad (2.27) \\ &= 20\log_{10}\left(\frac{\left|\left[\sqrt{\boldsymbol{\sigma}}\right]^{(a)} - \left[\sqrt{\boldsymbol{\sigma}}\right]^{(b)}\right|}{\sqrt{1\,\mathrm{m}^2}}\right) \ , \qquad (2.28) \end{aligned}$$

and argument

$$\arg\left(\left[\sqrt{\Delta\boldsymbol{\sigma}}\right]\right) = \arg\left(\left[\sqrt{\boldsymbol{\sigma}}\right]^{(a)} - \left[\sqrt{\boldsymbol{\sigma}}\right]^{(b)}\right) \ . \tag{2.29}$$

2.2.3 Measurement of the ΔRCS

Equation (2.15) already suggests a simple way of determining the RCS of a target by measuring the received electric field strength $\boldsymbol{E}_r$ at a defined distance R, sufficient to provide far-field conditions. This value has to be set into relation to the electric field strength $\boldsymbol{E}_i$ at the reference plane of the DUT. Disregarding for now the details of the necessary calibration to capture these values, this mentioned ratio can be defined as

$$\boldsymbol{\Gamma}(R) := \frac{\boldsymbol{E}_r}{\boldsymbol{E}_i} \ , \tag{2.30}$$

where both $\boldsymbol{E}_r$ and $\boldsymbol{E}_i$ are the complex-valued electric field strength vectors of isotropic waves at the same distance R of their origin in the same medium with an impedance of Z_0. Here, the distance R is big enough that far-field conditions can be assumed. This means that the waves behave similar to simple plane waves. Since R is fixed in the measurement setup described in this work, it is omitted in the notation of $\boldsymbol{\Gamma}$ in what follows.
As seen in Fig. 2.2, the reference plane for $\boldsymbol{E}_i$ is parallel to the incoming plane wave with the center of the tag located in it. The reference plane of $\boldsymbol{E}_r$ is at the front edge of the probe antenna. Via gain and aperture of the antenna, a connection between field strengths and received power at the antenna port can be established.

The parameter $\boldsymbol{\Gamma}$ describes the relation between the complex-valued electric field components of the incident and reflected wave, respectively. Although the reference planes of $\boldsymbol{E}_r$ and $\boldsymbol{E}_i$ are non-identical, $\boldsymbol{\Gamma}$ represents the reflection state of the RFID tag and is

therefore termed its reflection coefficient here to stress this fact.
Now, following the definition eq. (2.19), the square-root RCS can be expressed in terms of this new parameter

$$\left[\sqrt{\boldsymbol{\sigma}}\right] = \sqrt{4\pi R^2}\, e^{jk_0 R}\, \boldsymbol{\Gamma} \ . \tag{2.31}$$

The same can be done for the square-root ΔRCS

$$\begin{aligned}\left[\sqrt{\Delta\boldsymbol{\sigma}}\right] &= \sqrt{4\pi R^2}\, e^{jk_0 R}\, \boldsymbol{\Gamma}^{(a)} - \sqrt{4\pi R^2}\, e^{jk_0 R}\, \boldsymbol{\Gamma}^{(b)} \\ &= \sqrt{4\pi R^2}\, e^{jk_0 R} \left(\boldsymbol{\Gamma}^{(a)} - \boldsymbol{\Gamma}^{(b)}\right) \ . \end{aligned} \tag{2.32}$$

Introducing a new parameter

$$\Delta\boldsymbol{\Gamma} = \boldsymbol{\Gamma}^{(a)} - \boldsymbol{\Gamma}^{(b)} \ , \tag{2.33}$$

leads to the decent form

$$\left[\sqrt{\Delta\boldsymbol{\sigma}}\right] = \sqrt{4\pi R^2}\, e^{jk_0 R}\, \Delta\boldsymbol{\Gamma} \ . \tag{2.34}$$

This shows, that besides the known correction term $\sqrt{4\pi R^2}\, e^{jk_0 R}$, simply $\Delta\boldsymbol{\Gamma}$ has to be measured using a suitable measurement system, described in section 3.2, with an adequate calibration applied. The latter will be introduced in section 3.4. Some important points that have to be considered are listed here:

Frequency Behavior

It goes without saying that with regard to the internal buildup of the RFID chip the measured parameter will not be constant over frequency. Also the tag antenna has a frequency depending behavior. Thus, a suitable measurement system must comprise the possibility to perform measurements over a broad frequency band around the operational center frequency of the tag. Especially, since for the DSSS based localization method, introduced in section 2.1, the differential impulse response is of interest. This implicitly calls for a broadband measurement setup.

Spatial Behavior

Besides the measurement over frequency, another aspect comes into play when examining RFID tags using an antenna. No matter what antenna may be employed, it will not have an isotropic antenna pattern. For example, electric dipoles are widely used with commercially available tags, which exhibit two zeros in the pattern in the directions of the axis of the dipole. In order to fully capture the spatial behavior of a tag measurements have to be performed at least along two perpendicular angular cuts, at best over a full sphere with the tag in its center.

Non-linear Behavior

Like it can be seen in the right-hand side part of Fig. 2.3, diodes are deployed within the chip. For instance EPC compliant tags, on the one hand, they provide a DC power supply for the chip, rectifying the received RF signal. On the other hand, they ensure that the voltage does not exceed the admissible level. From a ΔRCS point of view this means a more or less strong non-linear behavior. Hence, a suitable measurement system has to be

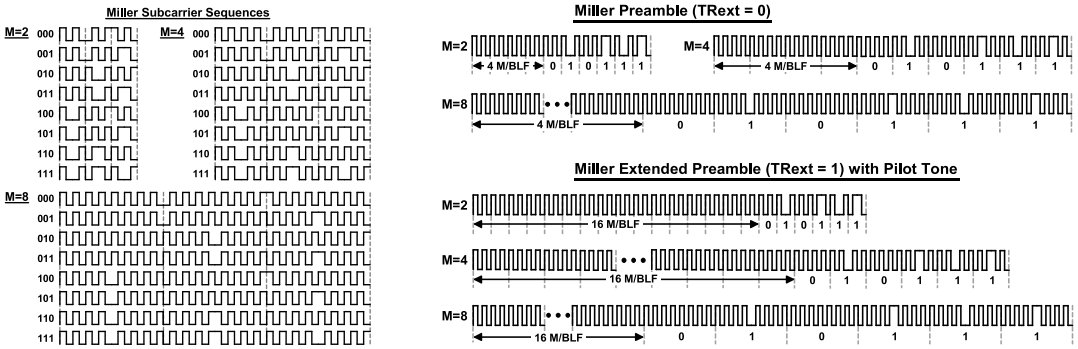
able to adjust the applied power level. This is the only way to find the minimum level of surface power density or equivalently the electric field strength at the position of the tag, necessary to activate it and get a response. This again is a prerequisite, since the ΔRCS of RFID tags is only meaningful when defined relative to the minimum power level necessary for the tag to become fully activated, as stated in [11]. Additionally, a wide range of possible power levels allow to quantify the non-linear behavior, which may be beneficial for further research activities in this field.

2.3 Potential DUTs

As already indicated in section 2.1, several different kind of tags are interesting for localization. This section gives an overview of the tags that are examined in this work. As a basic category they can be differentiated by the frequency band they are operating in.

UHF Band Tags

As for UHF tags, there is the classical EPC compliant RFID tag, which is already widely deployed and hence of special interest. An EPC RFID system is based on the interrogator-talks-first principle. This means that whenever a response of the tag is desired, the tag has to be told to do so. Since this is also the case when a certain parameter like the ΔRCS should be measured, some details on the actual communication process cannot be ignored altogether, although the details of RFID are not in the focus of this work in principle. Because of the fact that no specific information from the tag itself is of interest, it is enough to initiate a communication link using the so called *query-select* command and analyze the first response of the tag.
The basic principle of the interrogator-to-tag communication link R$\Rightarrow$T is an ASK in form of a simple on-off keying of the otherwise continuous carrier frequency. Besides the fact, that it has to be provided in order set the basic parameters of the tag and to receive an answer, the nature of the signal itself does not have any influence on the measurement conducted in this work.
The case is different for the tag-to-interrogator link T$\Rightarrow$R. Several parameters can be set during the initial R$\Rightarrow$T communication stage which have direct influence on the signal available for the extraction of ΔRCS. The data encoding and the data rate are to be chosen by the interrogator, according to [2, Subcl. 6.3.1.3]. For the encoding, several different options are available. For the purpose of ΔRCS measurements, it is best to have a T$\Rightarrow$R sequence as long as possible to allow for averaging of the respective state of the modulation impedance and thus, an improvement of the experienced SNR. Fig. 2.5a shows available sub-carrier sequences based on the so-called Miller encoding. Every T$\Rightarrow$R communication starts with the according preamble as seen in Fig. 2.5b. Obviously, a long tag response sequence is obtained for $M = 8$ and $TRext = 1$.
The modulation frequency is set via the so called backscatter link frequency (BLF), which determines the duration of the preamble as well as each bit. The BLF of course also determines the spacing in frequency domain between the carrier signal provided by the interrogator and the spectral lines resulting from the backscatter modulation of the tag. Considerations regarding the best choice for the BLF can be found in section 3.5.1, where



(a) Sub-carrier sequences. [2, Fig. 6.13]

(b) Sub-carrier T⇒R preambles. [2, Fig. 6.15]

Figure 2.5: Miller sequences as defined in the EPC standard [2].

it is seen in the context of the whole measurement setup.
Although a continuous modulation would be convenient for the ΔRCS measurements, this is not possible using standard EPC communication since the first response of the tag contains the so-called RN16 pseudo-random sequence. This results in the undesired broadening of the spectral lines of the tag response. Nonetheless, the continuously modulated preamble guarantees for sufficiently thin spectral lines when the captured time frame is chosen correctly.

The list of UHF tags actually examined in this work contains the following:

- NXP Ucode7 on Teflon
- NXP Ucode7
- Philips EPC Gen.2 V4 EU
- REFlex (dual band)
- Kathrein MTP-110-K-A

Except for the first one in the list, all tags are mounted on a structure entirely made of ROHACELL®[4].

ISM Band Tags

Especially for the DSSS based localization technique introduced earlier, the available bandwidth in the UHF frequency range is quite limited due to the standard requirements and national regulations. This is why prototype chips[5] have been developed which comprise an additional port besides also meeting the classical EPC requirements. The impedance of this additional port can be modulated separately and may be connected to a second antenna, matched to this port for the ISM band around 2.45 GHz. In this case, the DSSS

[4] Dielectric properties quite similar to air.

[5] In the course of the *"RFID Real-Time Localization for Flexible Production Environments"* (REFlex) project. Austrian Research Promotion Agency (FFG); Project Number 845630 [12].

localization technique may make use of this additional available bandwidth, while the basic EPC communication and, hence, activation of the tag as well as the power supply still takes place in the UHF band. However, for the ΔRCS measurement it is enough to trigger the tag once with the necessary EPC command in the beginning of a measuring cycle and simply provide it with a continuous wave UHF signal afterwards. A continuous wave carrier in the ISM band has to be provided by the measurement setup which is to be modulated by the tag for the ΔRCS measurement.
The ISM port BLF of the REFLEX tag can be chosen between the two values of 30 kHz and 960 kHz. Additionally, this chip possesses two different modes of modulation, a weak and a strong one, which differ in the impedance of one of the two modulation states and hence, also in their ΔRCS.

Besides the REFLEX tag, a second tag operating at the ISM band around 2.45 GHz is examined in this work. It is based on the modification of a so called electronic shelf label (ESL) by the company SES-IMAGOTAG, as shown in Fig. 2.6.

Figure 2.6: SES-IMAGOTAG electronic shelf label, as it is used in this work for ΔRCS measurements.

Intentionally made for convenient price labeling in shops, the DSSS localization technique may also be used with these tags by adding a backscatter circuit similar to the one shown in Fig. 2.3. The basic idea of the circuit is to switch the bias voltage of a pin-diode connected to the antenna between high and low to change the modulation impedance between an open and a short circuit. Since it is powered by an internal battery, no supplying UHF carrier is necessary in this case. A more detailed description of the modifications made to the ESL can be found in appendix B.

2.4 Interferences

Naturally, the obvious band to use for the DSSS based localization technique is the UHF band where the standard EPC communication takes places. The bandwidth available for this is relatively small, in the order of some MHz, and although the sequence superimposed for localization is weak enough in power to fulfill the regulations, more freedom in regards of frequency and power level are beneficial.
Since in general, the frequency spectrum nowadays is an expensive resource, which is

subject to strict regulations, the only bands available for such an additional service are the bands designated for industrial, scientific, and medical applications as stated in the international telecommunication union (ITU) radio regulations (RR). The possible ISM bands in the ITU Region 1[6] are in the range from 2.4 GHz to 2.5 GHz (denoted here as "ISM 2.45") and from 5.725 GHz to 5.875 GHz (denoted here as "ISM 5.8")[7].
However, it goes without saying, that the use of the open ISM bands has the drawback of being shared with numerous other services. The ITU states the following[7]: *"Radiocommunication services operating within these bands must accept harmful interference, which may be caused by these applications."*
Expecting such harmful interferences, an extension of the localization technique to these ISM bands requires an assessment of possible disturbances. Both ISM bands mentioned here are used by highly popular and widely used services such as wireless LAN or BLUETOOTH®. They are present in every possible environment interesting for the RFID localization. To get an idea of the severity of this issue, measurements in real world scenarios are performed in the course of this work and presented in chapter 5.

[6] Europe, Africa, former Soviet Union, Middle East, according to [13, RR Nos. 5.2 to 5.9].
[7] ITU radio regulations [13, RR No 5.150].

3 ΔRCS Measurement Setup

This chapter gives a detailed description of the measurement setup implemented in order to measure the ΔRCS of RFID tags. The basic problems and requirements are stated and the chosen solutions are presented. This comprises the hardware of the system as well as the essential parts of the underlying algorithms. In general, all software is implemented in MATLAB, all communication with the involved equipment takes place via VISA[1] and SCPI[2] over both GPIB[3] and LAN.

The setup is generally based on the monostatic measurement system for radar targets introduced in section 2.2. As it can be seen in Fig. 3.1, the basic concept of splitting the wave reflected by the target from incident wave using a circulator is improved by adding additional features. A source coherent to the frequency reference of the signal analyzer is used to reduce impairments due to phase noise. Further, a programmable attenuator allows for power adjustment of the source. In order to avoid problems with strong unwanted reflections due to mismatch of the TX/RX antenna, a carrier cancellation is implemented. Finally, a vector signal analyzer (VSA) is used to capture the signal reflected by the tag.

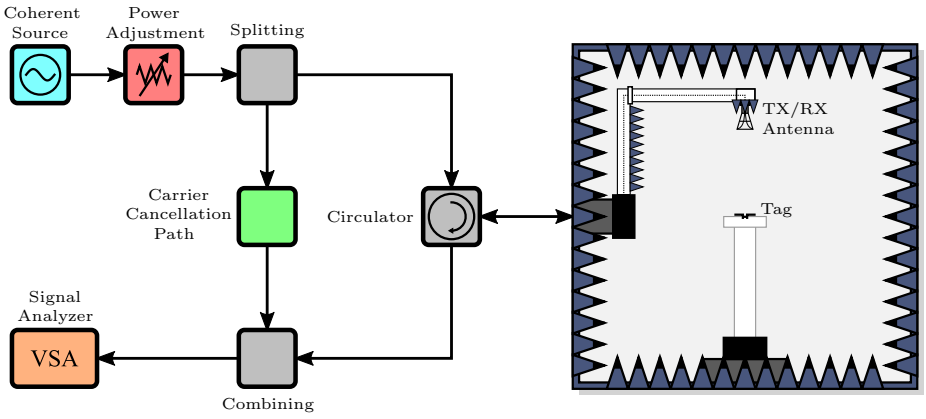


Figure 3.1: Overview of the implemented measurement setup.

[1] *Virtual Instrument Software Architecture*
[2] *Standard Commands for Programmable Instruments*
[3] *General Purpose Interface Bus* (IEEE-488)

The general requirements on the measurement setup and the basic ideas of the respective solutions are specified in section 3.1. Section 3.2 consists of a step by step presentation of all components necessary to allow for ΔRCS measurements. Subsequently, a summary of the full measurement setup as well as an evaluation of the involved signal power and noise levels is given in section 3.3. In section 3.4, the calibration necessary to obtain correction terms for the measurement system is explained. Those are used in order to get to calibrated $\mathbf{\Gamma}$ values from the raw results. Finally, section 3.5 lists the parameters to be set for the different DUTs. Furthermore, it is shown how a signal measured by the VSA and corrected by the correction terms yields the actual ΔRCS.

3.1 Requirements

In order to obtain useful results, the measurement system has to meet certain demands:

- Since the $\mathbf{\Gamma}$ value has the nature of a reflection coefficient, which shall be determined not only in amplitude, but also in phase, the system has to provide a source signal with a stable phase relation to the receiver.
- A severe challenge is to correctly measure a comparatively low signal stemming from the tag which is overlaid with much stronger signals caused by reflections other than the tag. For this, the system has to be capable of getting rid of this unwanted reflections, performing a carrier cancellation.
- In principle, numerous DUTs can be characterized in terms of their ΔRCS, as long as they are based on the modulation of an alterable impedance connected to an antenna. Naturally, different DUTs have different requirements on how they are activated. This is why the measurement system must have some flexibility on how to stimulate various DUTs and even supply them with power if necessary, for example in the case of passive RFID tags.
- Tags are supposed to work in any spatial orientation towards the reader. This means that usually some kind of omni-directional antenna is used. However, it is interesting to quantify its ΔRCS for different directions in space, similar to a radiation pattern. For this it is necessary to provide an anechoic environment in which the tag can be placed in any position relative to the interrogating antenna.
- As stated in chapter 2, different frequency bands are of interest, especially in the context of localization based on DSSS. In order to make switching between different bands possible without any additional effort, the system shall be constructed in a way that the signal is routed over the band-specific hardware components automatically. This means that several parallel signal paths must be provided which can be chosen by the software using a microwave multiplexer.

3.2 Components & Functionality

This section contains a systematic listing of all components involved in the measurement setup. These are the measurement device (3.2.1), the source signal generation (3.2.2), the

carrier cancellation (3.2.3), the parts used for EPC communication and triggering (3.2.4), the anechoic chamber (3.2.5), and the circuitry necessary to measure in different frequency bands.

3.2.1 Measurement Device

In principle scattering parameters and hence, also RCS measurements may be performed using a network analyzer. A source is being swept over a certain frequency range while an output and an input receiver are capturing the incident and the reflected wave. Using a common reference, two complex valued waves are obtained and their ratio yields the desired value after applying a proper error correction.
In this measurement setup the basic principle is the same. Nevertheless, some issues have to be considered in this case, which make the use of a VSA a more convenient solution.
RFID tags change their backscatter state over time with a defined BLF. Capturing this signal with a sufficiently high sampling rate allows to obtain the full spectrum of the tag modulation at once, while a swept network analyzer will always only capture one frequency at once. In principle, this is enough to get the RCS for a certain carrier frequency, but due to the ever-changing reflection coefficient, the two different states had to be measured separately from each other. Hence, accurate triggering of the network analyzer in synchronization with the tag is necessary. Since real-time synchronization with the internal local oscillator (LO) of the tag is far from trivial, the subsequent analysis of the captured time domain signal proves to be a much simpler solution.
The VSA actually used in this setup is the Keysight M9391A PXIe, together with the Keysight 89600 vector signal analysis software[4].

3.2.2 Carrier Signal Generation

Challenge: Phase Noise

As previous measurements with RFID tags have shown, phase noise (PN) always tends to be a problem. In case the signal source and the LO signal used for down-conversion by the signal analyzer are not perfectly synchronized, a spreading of the spectrum of the captured signal is the result. This is especially a problem with RFID due to the relatively small values of the BLF of the tag. This means that in frequency domain, the lines belonging to the modulation products of the backscatter signal are so close to the carrier, that the phase noise of the carrier can be the limiting factor (noise floor). An RFID system is self-interfering while the thermal noise floor is usually not problematic. The situation is illustrated in Fig. 3.2.
Even though high-quality synchronization of the reference frequency of source and down-conversion frequency of the analyzer may be possible in principle, this can only provide limited accuracy. Clearly, a better solution to confine the phase noise is the use of the down-conversion signal of the VSA as a source signal.
Fig. 3.3 shows the essential parts of the internal receiver chain structure of the VSA used in this setup. As it can be seen there, the analyzer uses superheterodyning to convert the input signal to an intermediate frequency (IF) of 300 MHz. Sampling takes place at this

[4] Version 22.0.

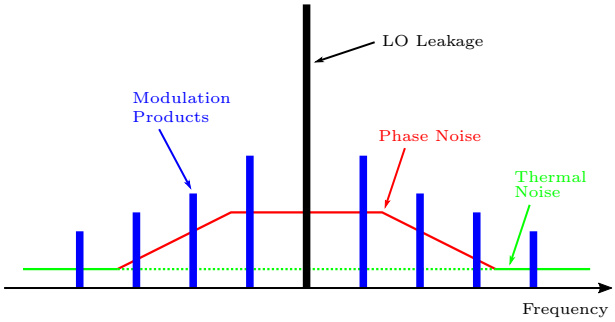


Figure 3.2: The phase noise can be the limiting factor in self-interfering RFID systems.

frequency with a rate of 400 MS/s. The final conversion to baseband is done in digital domain. All this steps are performed by separate parts within different slots of the PXIe rack.

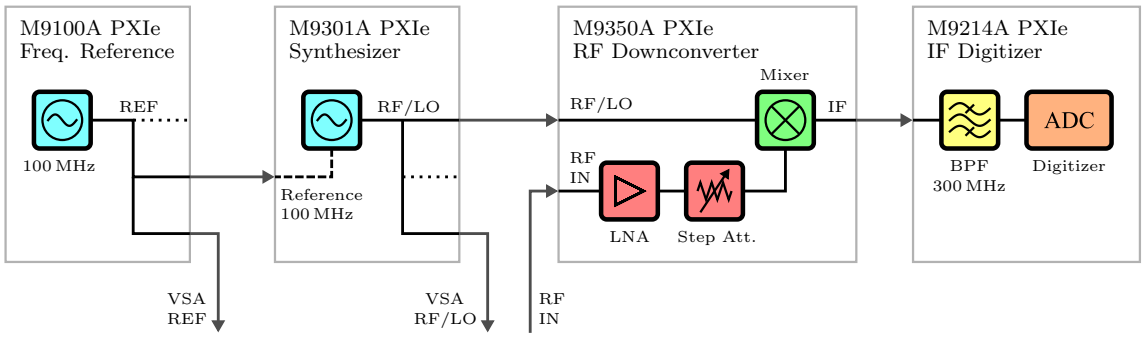


Figure 3.3: Basic block diagram of the KEYSIGHT M9391A PXIe VSA. It consists of four separate components, mounted together in a so-called PXIe rack. The IF frequency can be fixed to 300 MHz. As indicated, the VSA has additional unused outputs for the REF and the RF/LO signals. Together with the RF IN connector, these are used in the measurement setup as VSA REF and VSA RF/LO.

For the measurement setup introduced here this means that the RF/LO signal used for heterodyning is available. Nevertheless, a fixed offset of 300 MHz remains[5]. In order to make this signal usable for the intended purpose, a modification in form of a frequency shift by the IF is necessary. That is to get a carrier signal with the exact frequency of the current center frequency of the VSA.
To avoid additional phase noise caused by the introduction of an external source, the internal reference frequency of 100 MHz is best to be used here. This signal is denoted as REF. The implementation of the introduced concept comprises a simple frequency multiplier which uses non-linear effects to produce harmonics. Since the desired third harmonic is not the only one that will occur at the output, an additional band-pass filter (BPF) with a center frequency of 300 MHz is used. The thereby obtained sine wave is then mixed with the RF/LO signal. Because of the varying power of the RF/LO signal over frequency, an attenuator-low-noise amplifier (LNA)[6] combination is used to achieve a constant level. An

[5] Given the appropriate setting of the device *Input* → *Extensions* → *Magnitude Trigger Bandwidth* → *Wideband* and *Input* → *Extensions* → *Conversion* → *Auto*.
[6] MINI-CIRCUITS ZX60-83LN-S+, Low Noise Amplifier

additional LNA is used for pre-amplification of the otherwise weak signal after the mixer. Fig. 3.4 shows an overview of the implemented solution.

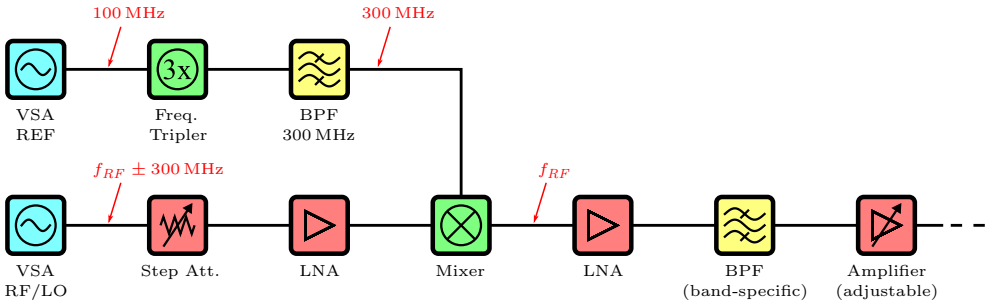


Figure 3.4: Block diagram of the carrier signal generation circuit. With $f_{REF} = 100\,\text{MHz}$ and $f_{RF/LO} = f_{RF} \pm 300\,\text{MHz}$.

The mixing of the 300 MHz signal with the RF/LO signal results in spurious frequency components in the spectrum of the signal. Thus, in order to obtain high spectral purity, filtering is necessary. Since the measurement setup is intended to work in three different frequency bands, each one requiring a different BPF, these filters are placed in a later stage in the actual measurement setup. The respective stage will be introduced in section 3.2.6.

The mixing of the signals lead to the phase noise of the RF signal depicted in Fig. 3.5 for different frequency bands as introduced later in section 3.2.6. For a comparison with the nominal phase noise of the VSA source at those frequencies, the phase noise of the RF/LO signal tuned to the same frequencies is shown as well. These measurements are performed using a Keysight UXA, which has a significantly better phase noise performance than the VSA. The situation must be expected to degrade due to the additional phase noise stemming from the VSA REF source. However, there is no significant difference between the RF and the RF/LO phase noise. A slight disparity is due to limited measurement accuracy and different VSA source frequencies, i.e. including the 300 MHz offset.

In order to assess the benefit of the produced carrier signal in terms of phase noise, measurements of the overall setup performance are made. As the VSA uses the coherent RF/LO signal for down-conversion, an improvement might be expected. Fig. 3.6 shows the phase noise of the carrier signal measured using the UXA and the VSA. It can be seen that the situation can be improved for a frequency offset greater than 30 kHz, which is also the typical range for the BLF. This effect shows that coherence can be achieved this way.

The final measurement system also comprises cables into the anechoic chamber which lead to a length of the signal path somewhat shorter than 30 m. To analyze the loss of coherence due to this long connections, the phase noise measurement is repeated with an additional 30 m cable inserted between the coherent source and the VSA. This shows a degradation of phase noise for frequency offsets of some 100 kHz, where the cable length becomes a considerable fraction of the wavelength. In this range the phase noise curve approaches the original one.
For even higher frequencies, the noise floor of the VSA as a measurement device limits the phase noise measurement.

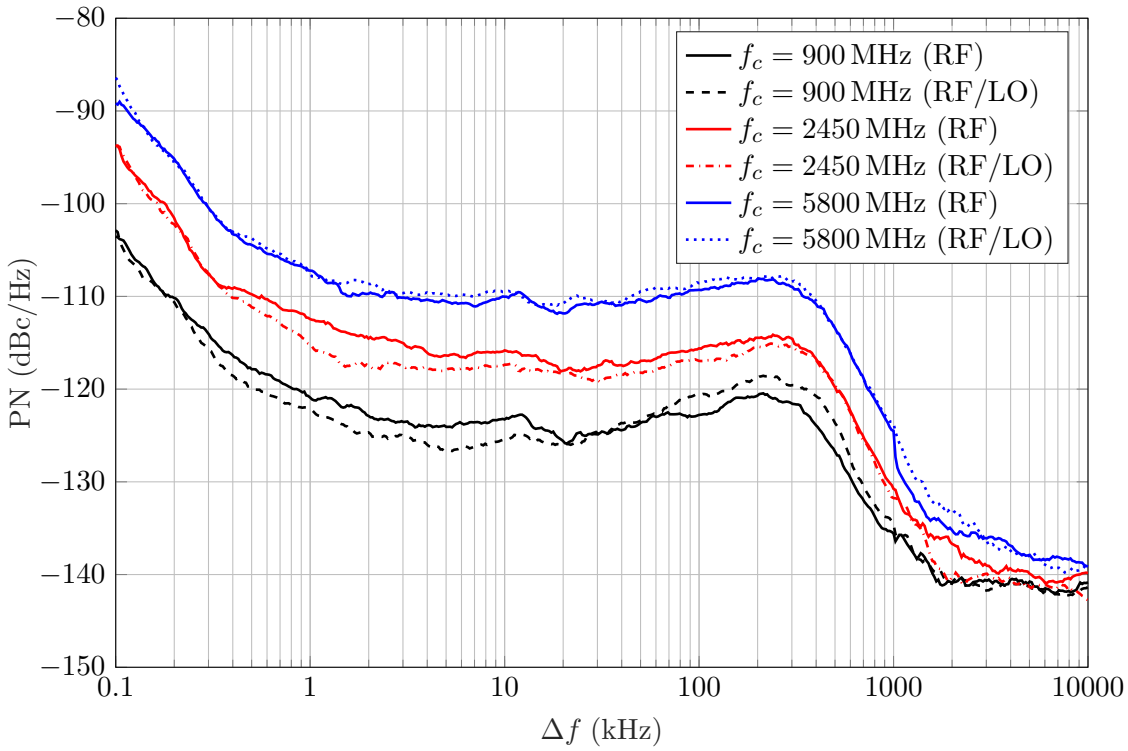


Figure 3.5: Single sideband phase noise over frequency distance Δf to the center frequency f_c. Comparison of the RF and RF/LO signals at certain frequencies.

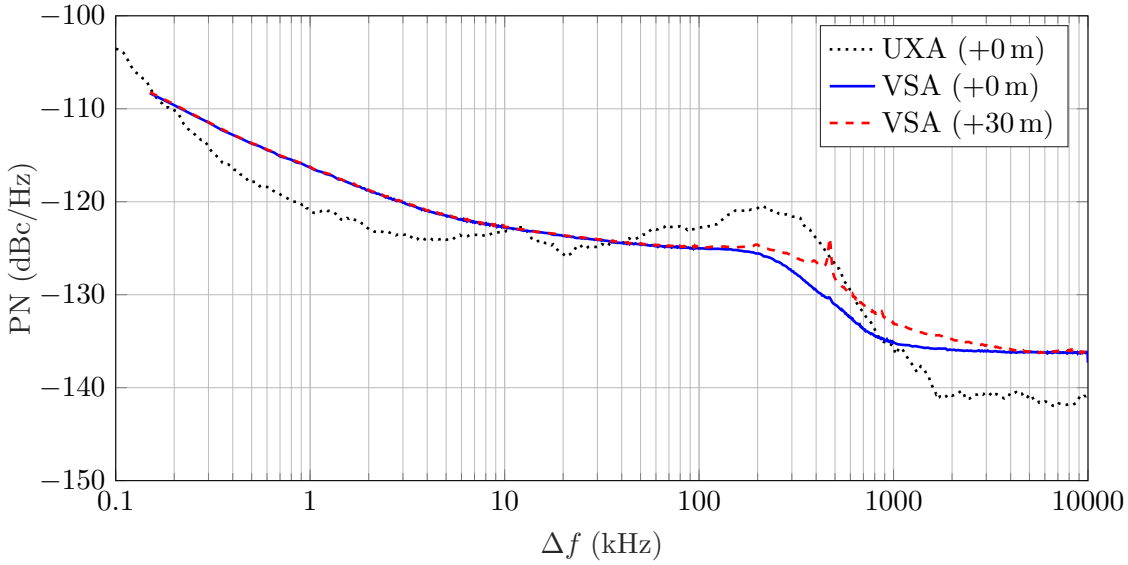


Figure 3.6: Single sideband phase noise of the RF signal at 900 MHz. Measurements performed using the UXA as an independent measurement device and the VSA using its coherent LO. Adding a 30 m cable shows a degradation in phase noise for higher frequencies. The absolute noise floor visible at the highest frequencies is due to the limited range of the measurement devices.

Power Adjustment

Like described in section 2.2.3, in order to fully characterize an RFID tag, it is necessary to adjust the power of the carrier signal. In this setup, this is achieved by using a combination of an attenuator and an amplifier, represented by an adjustable amplifier in Fig. 3.4. Since the attenuation due to the long cables into the anechoic chamber and the free space path loss (FSPL) are quite high, a power amplifier with an output power up to 40 dBm is used[7]. This high power is necessary since the EPC tags have to be powered by this signal. Despite the disadvantageous situation in terms of noise this makes it necessary to put the attenuator in front of the amplifier, since most programmable attenuators are not capable of handling such high power levels.
In order to achieve a good power resolution, a programmable attenuator with attenuation steps of 0.25 dB is used[8]. The dynamic range achieved is 25 dB. The upper limit of 40 dBm is simply given by the used amplifier and some safety margin. Since the power level always has to be sufficient to drive the carrier cancellation circuit, which is introduced in section 3.2.3, a lower limit is implicitly given as well. Besides that, at such low power levels, the tag does not receive enough power to become active and hence, no ΔRCS can be measured.

Phase Lock Calibration Path

In principle the derivation of the carrier frequency signal from the internal reference signal (RF/LO) of the VSA ensures phase coherence between the signal used for down-converting in the receiver chain and the carrier signal provided to the tag. Nonetheless, a random phase lock occurs during the startup of the VSA. This means that although for all center frequency settings a defined phase constellation can be assumed, they all are subject to the same phase offset, which is constant after initialization. To take this phase offset into account, an initialization path is introduced, bypassing the entire measurement system and providing a direct connection between the generated carrier frequency and the receiver path. This part is marked in the system overview in Fig. 3.14 as a dashed line. The path allows to measure and store the offset for later correction of the measurement results.

3.2.3 Carrier Cancellation

Challenge: Reflections

A theoretical approach to measure the ΔRCS has already been introduced in section 2.2, especially Fig. 2.2. A source signal is sent towards the tag, the reflection is captured using a signal analyzer. A circulator is used to combine the path of the incident and the reflected wave. It allows to use only one antenna for the transmit as well as for the receive path.
In reality, this simple approach turns out to be problematic. Due to non-ideal components and connectors in the path between the circulator and the DUT, the desired reflections from the tag are of much smaller magnitude than the unwanted ones. It turns out that the critical points are the match of the probe antenna and certain connectors between the cables into the anechoic chamber. As a consequence, the signal analyzer might run into an

[7] Mini-Circuits ZHL-30W-252-S+, High Power Amplifier.
[8] Mini-Circuits RCDAT-6000-60, Programmable Att., 0 dB to 60 dB, 0.25 dB step, 1 MHz to 6000 MHz

overload. The severity of the problem can be seen in Fig. 3.7, where the relative powers at the different nodes through the measurement path in the chamber are depicted. The block diagram represents one circulator and the measurement chamber. On the one hand, the reflections are of much higher power than the signal component reflected by the tag. On the other hand, due to multiple reflections, they may vary strongly over frequency. Note, that the paths into and out of the chamber are shown consecutively, even though being physically identical. This is indicated by the port numbers P1 to P3 of the circulator.
In order to avoid this and to ensure that the analyzer settings can be optimized for the expected weak signals[9] coming from the tag, a carrier cancellation (CC) is a possible solution.

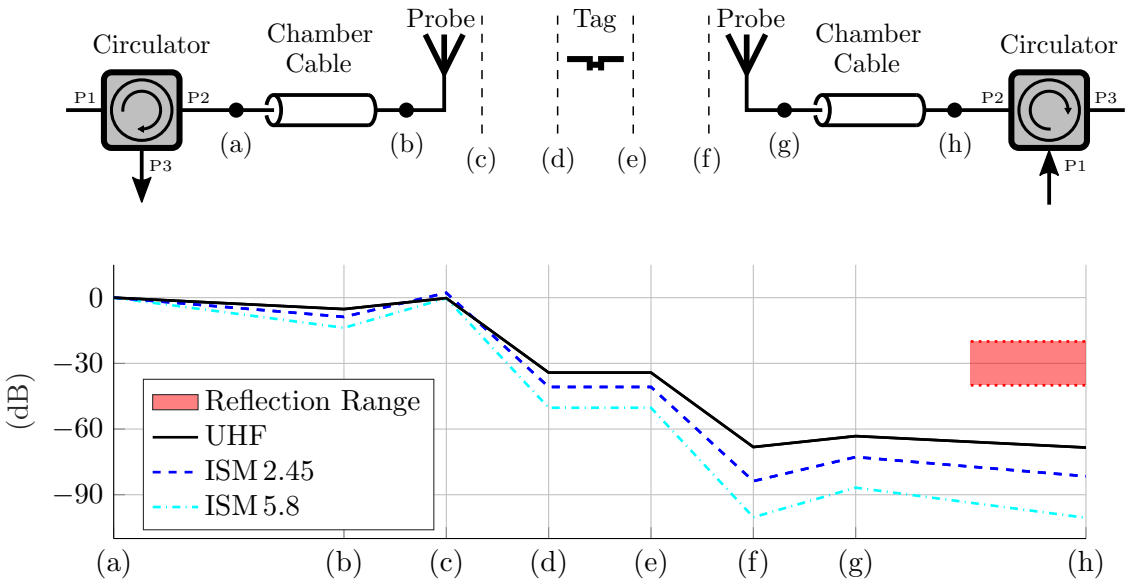


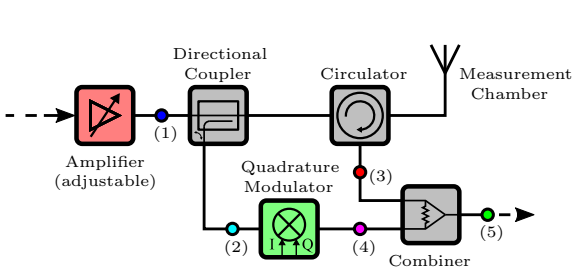
Figure 3.7: Range of unwanted reflections versus the signal component reflected by the tag for the different frequency bands as introduced in section 3.2.6. The gain of the tag is assumed as 0 dB for a rough estimation. The setting is actually monostatic.

Hardware

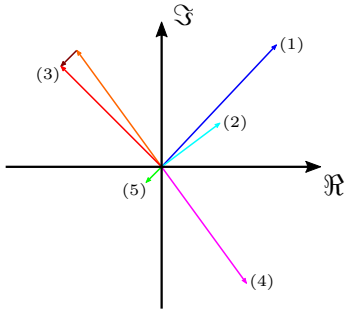
The basic idea of a carrier cancellation is shown in Fig. 3.8a. The first step is to split off a part of the carrier before it is sent towards the measurement chamber. This coherent signal can then be used to compensate for the undesired reflections on the path. For this purpose it is combined with the signal coming from the chamber. The prerequisite is the correct magnitude and phasing of the compensation signal, in order to cancel out the unwanted carrier. Fig. 3.8b shows the described situation in an IQ representation of the involved wave quantities. This magnitude and phase adjustment can be achieved using an IQ modulator, which is capable of reaching any necessary point in the complex IQ representation of the signal. At the same time, the center frequency has to remain unchanged.

For the magnitude and phase modulation as the central part, the chosen solution is a

[9] Preamplifier on, step-attenuator set to low values.



(a) Block diagram. The signals at the points (1)-(5) are of interest in the context of the carrier cancellation.



(b) Exemplary illustration of the involved wave quantities in the IQ diagram. Arrows not to scale.

Figure 3.8: Principle of the carrier cancellation. Signal (3) consists of a weak modulated component coming from the tag and much stronger unwanted reflections. The carrier cancellation (4) allows to remove the unwanted reflections.

combination of a wide-band quadrature modulator with differential I and Q baseband inputs[10] and a four-port 16-bit digital-to-analog converter (DAC)[11]. The DAC is used to drive the baseband input of the modulator at DC level, i.e. 0 Hz. Hence, the frequency of the modulated signal is not different from the frequency of the input signal.
The power levels involved require special attention. The power level available on the carrier cancellation path depends on the power of the carrier signal. However, the IQ modulator used in the setup requires a typical power level in the vicinity of 0 dBm at its LO input. To ensure an appropriate level in all states of the carrier signal power, a programmable attenuator[12] is used to reduce the power level. This is done automatically for any particular setting of the carrier power level, since the relation is known from the coupling of the used splitter or directional coupler. The 3 dB step-size is sufficient since the admissible LO power range of the IQ modulator exceeds this value.

The resolution of the system is primarily determined by the capabilities of the deployed DAC. Although the one used here provides a 16-bit resolution, the effective resolution is confined by the limited admissible input voltage of the DAC baseband ports. Since the baseband inputs are differential, the differential voltage V_{DM} at the two ports has to be set antipodal around the required common-mode voltage of $V_{CM} = 1.7\,\mathrm{V}$. The maximum differential input voltage that can be used is about 1.5 V. Up to this value linear behavior is observed. This means that only a limited voltage range and hence resolution can be used. Thus, the effective resolution is about 14-bit for the in-phase and quadrature component, respectively.
In order to achieve the best use of the available resolution, it is beneficial to drive the system at rather high values of baseband voltage. In this region of operation, the highest possible resolution relative to the current magnitude can be reached. For a precise compensation of the carrier signal, this is preferable. However, experiments have shown that the IQ modulator also amplifies the phase noise present at its LO input when driven at higher levels. At some point, this amplified phase noise becomes dominant over the noise floor of the reflected signal coming from the chamber. This means that such high baseband

[10] Texas Instruments TRF370417, 50 MHz to 6000 MHz Quadrature Modulator
[11] Texas Instruments DAC80004, Quad 16-Bit Digital-to-Analog Converter
[12] Analog Devices HMC629ALP4E, 3 dB LSB 4-Bit Digital Attenuator, DC to 10 GHz

voltages may deteriorate the effective noise floor. Because of this fact, rather low levels of the compensation signal are preferable and therefore used in the measurement setup.
In addition, the question may be raised if a very precise carrier cancellation is even necessary. On the one hand, it allows to turn the receiver settings to the highest sensitivity. On the other hand, recalling from Fig. 3.8b the fact that the receiver input is the sum of two rather long vectors, shows that a slight change in magnitude or phase of one of these two vectors is enough to render the sensitive receiver setting useless. This might be the case for a slightly changed reflection from the chamber, e.g. due to movements of the *theta*-stage[13].

The power range of the IQ modulator also indicates the possible power range of the reflections coming from the chamber. With a return loss of roughly 20 dB[14], the power of the wave coming from the chamber might take on values of up to 20 dBm at high power levels. In order to get it into the feasible range of the IQ modulator, another programmable attenuator[15] is inserted, before finally combining the two paths. As it is the case at the input side of the IQ modulator, a 3 dB step-size is sufficient. The modulator itself offers a wide enough power range as well.
Although this attenuator is at the beginning of the receiver chain it does not impair the SNR. This is due to the inevitably high noise floor stemming from the amplifier necessary to get a sufficient amount of power into the chamber and to the tag.
Fig. 3.9 shows an overview of the full carrier cancellation part of the measurement setup as it has been implemented finally.

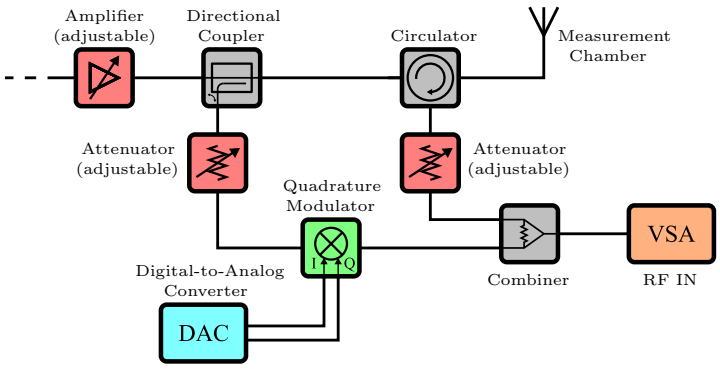


Figure 3.9: Full carrier cancellation part of the measurement setup in the UHF band. Due to the reduced range of the power level in the ISM bands, the adjustable attenuators are omitted there.

Algorithm

In order to set the necessary carrier cancellation, an algorithm was implemented to set the differential I and Q inputs of the IQ modulator to the appropriate values. This algorithm is based on a coordinate transformation between a two-dimensional plane representing the differential I and Q voltages of the DAC on the one side and the complex-valued representation of the wave measured by the VSA after the combination of the two paths

[13] A more detailed description of the anechoic chamber and its interior will follow in section 3.2.5.
[14] Due to the numerous reflections along the cables into the chamber, the actual return loss of the chamber varies tremendous at certain frequencies.
[15] Analog Devices HMC629ALP4E, 3 dB LSB 4-Bit Digital Attenuator, DC to 10 GHz

on the other side. For this, real-valued voltage vectors are defined to represent points in these planes. For the differential DAC voltages as

$$\vec{x} := \begin{bmatrix} V_{DM,I} \\ V_{DM,Q} \end{bmatrix} \ , \tag{3.1}$$

and for the peak baseband voltages measured by the VSA as

$$\vec{y} := \begin{bmatrix} V_{pk,I} \\ V_{pk,Q} \end{bmatrix} \ . \tag{3.2}$$

Due to the nature of the IQ modulator, the relation between $\vec{x}$ and $\vec{y}$ is not linear. However, as a first approximation it is written as

$$\vec{y} = \underline{S}\,(\vec{x} - \vec{x}_0) \ , \tag{3.3}$$

with the offset-vector $\vec{x}_0$ and the 2×2 transformation matrix $\underline{S}$. The non-linearity can be taken into account by iterating the carrier cancellation as it will be explained later.
The transformation matrix $\underline{S}$ consists of a shearing (IQ imbalance of the modulator), a rotation (phase offset), and a scaling (modulator gain & cable losses) component. For reasons of readability, and because it is simply not necessary in this case, they are not defined separately. Fig. 3.10 shows points in both coordinate systems, respectively and the relation between them.

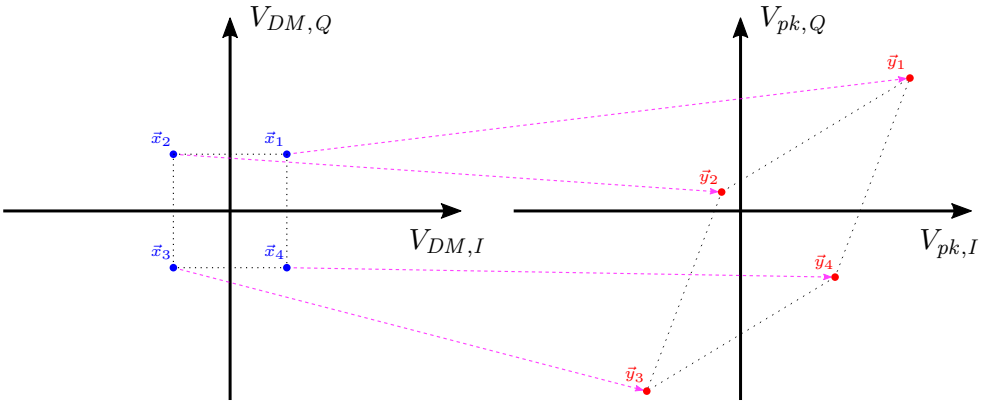


Figure 3.10: The two vectorized IQ diagrams. Left: DAC differential voltages. Right: baseband peak voltages of the measured waves resulting from combining the paths. The generally non-linear relation between points in the two diagrams is approximated as $\vec{y} = \underline{S}\,(\vec{x} - \vec{x}_0)$.

The carrier cancellation algorithm comprises the following steps:

1. **Power Range Leveling:**

   Since the actual reflections coming from the chamber depend on many factors such as movement of the *theta*-stage, frequency, and power level of the source, it is hardly possible to predict the power level of the reflected wave which should be compensated. This is why the first step is to measure the received power at the VSA and adjust the attenuator in the path coming from the anechoic chamber until the feasible range of the IQ modulator is reached.

2. **Measuring:**

   In a second step, the DAC is successively set to four different I,Q combinations, represented by the vectors $\vec{x}_1 \dots \vec{x}_4$. The corresponding waves are measured by the VSA and represented as vectors $\vec{y}_1 \dots \vec{y}_4$, respectively.

   The points are best to be chosen as far apart as possible. Since the shearing component of the transformation matrix $\underline{S}$ is not known beforehand, it is assumed to be rather weak and hence, the points are set in a square-shape.

3. **Solving Equation System:**

   The four measured points are further used to calculate $\vec{x}_0$ and $\underline{S}$. For this, first, the differentials are calculated as

   $$\Delta\vec{x}_{1,i} = \vec{x}_1 - \vec{x}_i \ , \qquad \Delta\vec{y}_{1,i} = \vec{y}_1 - \vec{y}_i \ , \tag{3.4}$$

   for $i = \{2, 3, 4\}$. Inserting this differential into eq. (3.3) leads to

   $$\Delta\vec{y}_{1,i} = \underline{S}\ \Delta\vec{x}_{1,i} \ . \tag{3.5}$$

   Combining these differentials into matrices as

   $$\Delta\underline{X} = \begin{bmatrix}\Delta\vec{x}_{1,2} & \Delta\vec{x}_{1,3} & \Delta\vec{x}_{1,4}\end{bmatrix} \ , \qquad \Delta\underline{Y} = \begin{bmatrix}\Delta\vec{y}_{1,2} & \Delta\vec{y}_{1,3} & \Delta\vec{y}_{1,4}\end{bmatrix} \ , \tag{3.6}$$

   an overdetermined equation system is obtained as

   $$\Delta\underline{Y} = \underline{S}\ \Delta\underline{X} \ . \tag{3.7}$$

   The use of more than three points to get an overdetermined equation system allows to apply a form of linear regression. Some measurement error is removed and the result is improved.
   Choosing the points $\vec{x}$ farther apart from each other, improves the conditioning of $\Delta\underline{X}$.
   $\underline{S}$ can now be calculated using the pseudo-inverse of the 2×3 matrix $\Delta\underline{X}$ as

   $$\underline{S} = \Delta\underline{Y}\ \Delta\underline{X}^{\dagger} \ , \tag{3.8}$$

   and $\vec{x}_0$ using one of the point-pairs, e.g. the first, as

   $$\vec{x}_0 = \vec{x}_1 - \underline{S}^{-1}\vec{y}_1 \ . \tag{3.9}$$

4. **Setting to Zero:**

   Using the calculated $\underline{S}$ and $\vec{x}_0$ allows to set the necessary x values for any desired y as

   $$\vec{x} = \underline{S}^{-1}\vec{y} + \vec{x}_0 \ . \tag{3.10}$$

   Since for the carrier cancellation the desired point is simply $\vec{y} = \begin{bmatrix}0 & 0\end{bmatrix}^T$, the corresponding $\vec{x}$ equals $\vec{x}_0$.

5. **Adjusting the VSA Settings:**

   With the carrier cancellation set, the necessary VSA settings can be set to high sensitivity. Especially the expected power range of the input signal can be set to low levels.

6. **Iterating:**

   The accuracy of this algorithm is limited by non-linear behavior of the IQ modulator. The assumption of linearity is violated. However, the carrier cancellation settings can be improved by repeating the procedure while using the results of previous iterations to restrict the possible range.
   In this case, it is necessary to go back to step 2 in order to achieve a higher accuracy.

3.2.4 EPC Communication & Triggering

As explained in section 2.3, an EPC compliant tag requires a certain stimulation in the form of an on-off keying of the carrier signal to become active and respond to the reader. This is a prerequisite to measure the ΔRCS. This means that the possibility to modulate the carrier signal has to be implemented in the measurement system. However, it is not necessary to provide an active communication, i.e. a response to the RN16 sequence of the tag. Thus, it is sufficient to generate an appropriate R⇒T sequence and simply replay it whenever the tag shall be activated. The measurement has to be triggered subsequently, when the tag response is expected. This is achieved by using another programmable attenuator as a switch. In accordance with the necessary sequence, it is switched between minimum and full attenuation at the input of the main amplifier.
In the ISM bands the situation is different. In cases of DUTs modulating independently from an external stimulation, the measurement simply has to be triggered whenever the setting is ready. A special case are the tags which require an EPC compliant stimulation in the UHF band, but also perform a modulation in the ISM bands, which shall be measured. They require an external carrier signal, independent of the measurement system itself. This is done by an external source at a fixed frequency in the admissible range, modulated by the same sequence as mentioned before. This signal can be provided to the tag via the *phi*-stage and an additional antenna in the base of the chamber. The two different ways of signal modulation are shown in Fig. 3.11, where the pillar used for the mounting of the DUT in the center of the chamber is not depicted for reasons of clarity.
Because of the frequency selective behavior of the measurement setup, this additional signal in the UHF band does not impair the measurement in the ISM band.

The actual implementation of signaling and triggering is done using a signal generator[16] with the ability of producing arbitrary waveforms. The RF output is used to generate the modulated external carrier signal. To control the programmable attenuator used for signaling in the actual measurement setup, a marker output is used, while a second marker output triggers the VSA in both cases.
Details on the content of the EPC signaling are to follow in section 3.5.1.

[16] Rohde & Schwarz SMBV100A, Vector Signal Generator

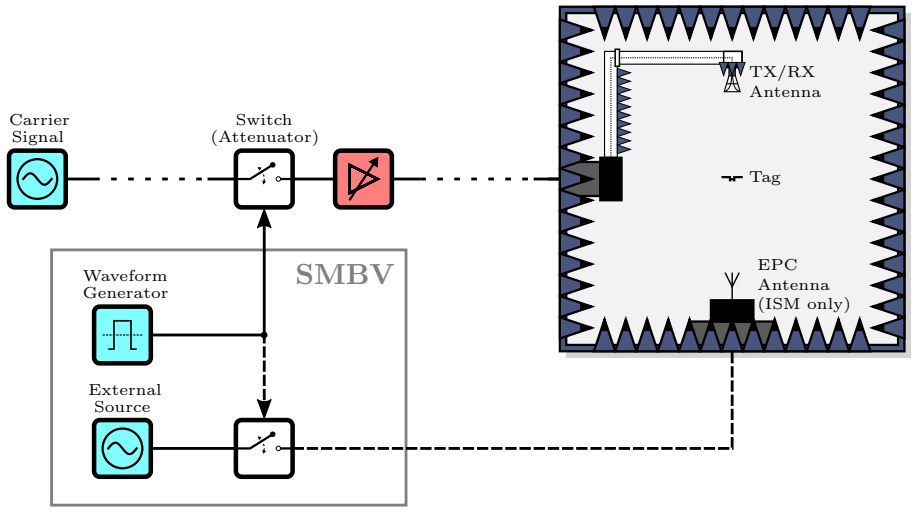


Figure 3.11: An external signal generator provides a marker signal to control an attenuator for modulation of the source and a modulated RF signal in the UHF range for the REFLEX tags.

3.2.5 Anechoic Chamber

The measurement chamber used in this measurement setup provides an anechoic environment, also shielded from outside interferences. It also allows to cover an almost full sphere around the DUT located in the center of the chamber. This is achieved by a rotatable platform in the center of the bottom of the chamber, where the DUT can be mounted using a pillar of appropriate height. This part of the chamber is referred to as *phi*-stage. Additionally, the probe antenna can be moved along a perpendicular arc reaching from the zenith right above the DUT down as far as the *phi*-stage allows. This part is referred to as *theta*-stage.
A third movable part is the probe antenna itself. This is necessary to allow a linearly polarized probe antenna covering the two orthogonal components of the electric field. It is therefore termed *pol*-stage.
The fact, that there is only one single probe antenna available which in this measurement setup serves as the transmitting as well as the receiving antenna at the same time, means that only monostatic measurements are possible. For any linearly polarized incident wave coming from a certain direction, only the wave reflected towards the exact same direction can be measured. Components scattered in other directions cannot be captured. The same is true for a wave component with a polarization orthogonal to the incident wave, since the probe antenna cannot receive it.

All the parts of the chamber as well as the coordinate system are indicated in Fig. 3.12. The picture shows the interior of the anechoic chamber including the Cartesian and spherical coordinate systems. Rotary joints are used to couple RF signals to their respective destinations on the *phi* and the *theta*-stage of the chamber. The axes can be controlled via a GPIB interface. Besides the standard setting of the chamber, the behavior in terms of reflections may be further improved using additional absorbers on the bottom of the chamber. A detailed description hereof can be found in appendix A.

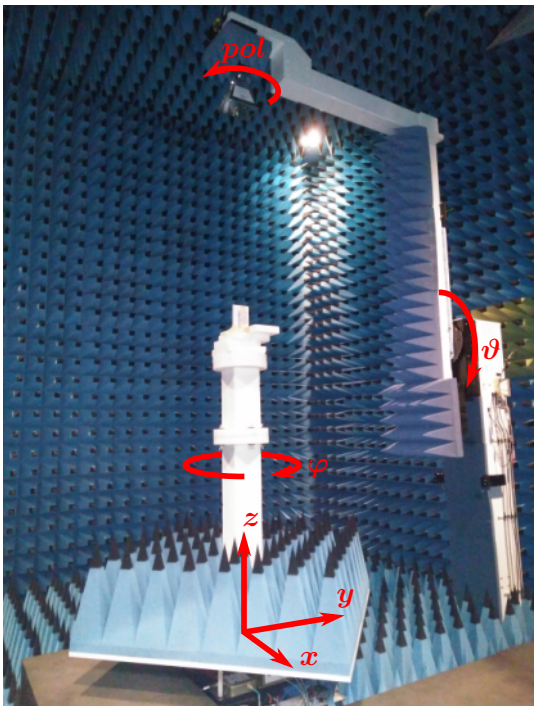


Figure 3.12: Overview of the anechoic chamber including coordinate systems, the probe antenna mounted on the *pol*-stage, and an RFID tag mounted on the *phi*-stage pillar.

An important question is also the mounting of the DUT itself. In the case of RFID tags, dipole, or dipole-like antennas are deployed. They exhibit linear polarization parallel to the axis of the dipole. In such a case it is beneficial to mount the tag perpendicular, that is parallel to the z-axis of the chamber as indicated in Fig. 3.13. This has the advantage that the tag antenna is always in co-polarization with one polarization state of the probe antenna in the given default φ-ϑ roll-over-azimuth coordinate system of this anechoic chamber[17]. This means that the tag and the probe antenna are coupled best for every (ϑ, φ)-tuple corresponding to a certain point on the sphere with the DUT in its center in exactly one and the same state of the *pol*-stage. It turns out, that in this case the coupling between probe and tag antenna in cross-polarization is so weak that the measurement does not yield useful results and hence, can be omitted entirely.

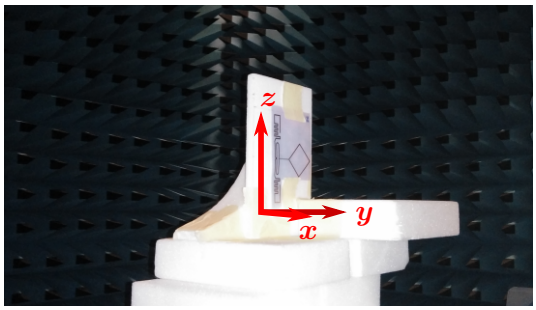


Figure 3.13: RFID REFLEX tag mounted in the anechoic chamber upright in z-direction.

[17] Information on spherical coordinate systems can be found in [14].

Another point of interest is the characterization of certain components of the chamber. These are primarily the cables connecting the probe antenna and the *phi*-stage, which have to be known in magnitude and phase for the calibration introduced later in section 3.4. Here, the long cable lengths cause problems which can be solved using a vector network analyzer with an *unknown thru* two-port calibration as described in [15].
As it will become clear later in section 3.4.5, it is also necessary to know the exact absolute gain of the probe antenna in order to calculate the actual field strength the tag is exposed to. The anechoic chamber can also be used to determine this gain. Plentiful information on this topic can be found in the literature, such as [16].

3.2.6 Band Separation

The measurement setup shall be capable of measuring the ΔRCS in three different bands. The standard EPC compliant band in the UHF range and also two ISM bands, where a higher bandwidth is available. An overview of these three bands is given in table 3.1. As seen there, the frequency bands are spaced from each other by several GHz and thus, the involved components have to meet certain demands, specific to the respective band.

Description	UHF	ISM 2.45	ISM 5.8
f_{low}	820 MHz	2.4 GHz	5.725 GHz
f_{center}	900 MHz	2.45 GHz	5.8 GHz
f_{high}	970 MHz	2.5 GHz	5.875 GHz
FSPL	34 dB	43 dB	50 dB
$S_{meas,min}$	0 dBm/m^2	-20 dBm/m^2	-27 dBm/m^2
$S_{meas,max}$	25 dBm/m^2	-12 dBm/m^2	-19 dBm/m^2

Table 3.1: The three measurement bands. Also shown is the expected FSPL and the approximate range of surface power density $S_{meas,min}$ to $S_{meas,max}$ that can be provided by the source at the tag position.

This is especially the case for the BPF introduced in section 3.2.2. Naturally, the mixing of the RF/LO signal with the 300 MHz IF signal results in additional unwanted lines at a distance of 600 MHz as well as a feed-through at a distance of 300 MHz from the final center frequency. Hence, the filters have to be chosen such, that on the one hand a sweep over the entire desired band is possible while on the other hand sufficiently suppressing all spurious lines at the same time. For this purpose, the filters are specially designed for each band. This means, that the signal has to take a different path through the setup for each of the bands. This prerequisite also limits the width of the bands to 300 MHz, reduced by a cutoff margin for the filters.
A similar situation is given for the circulators. Frequency selectivity is not required there, but a broadband solution is simply not available. As for the carrier cancellation, one solution for all bands is possible. This means that the signal-paths have to be recombined for the input of the IQ modulator. This is also the case for the access path to the anechoic chamber and the backward path of the reflected signal.
To allow all this without any additional reassembling, a microwave multiplexer[18] with

[18] LXI 60-800-008, 8-Bank, 6-Channel Microwave Multiplexer

a sufficient amount of multiplexer banks is used to split and combine the signal paths wherever necessary. The separation of the bands into different paths is shown in Fig. 3.14 together with the full measurement setup, where the microwave multiplexer banks are denoted by 'MW MUX'.

Another difference between the three bands is the necessary power level that has to be provided. While in the ISM bands the desired DUTs do not have to be powered by the measurement signal as described in section 2.3, this is only the case for the EPC UHF tags. For this reason, the UHF path comprises a power amplifier whose output power can be regulated. In the other two bands, the power provided by the source signal generation described in section 3.2.2 is sufficient. A programmable attenuator is sufficient to allow for a certain power regulation. This is of particular interest with regards to the (non-)linear behavior of the DUT.
In order to measure the actual power going into the anechoic chamber and towards the tag, a directional coupler is used to split off a part of the signal. A power sensor[19] is used to record the power level of this signal each time a ΔRCS measurement is performed. From this, after a correction, the power of the signal at the output of the through path of the directional coupler is obtained. Subsequently, this port also serves as a reference plane for the incident wave a_0, as it is shown in Fig. 3.14 and explained in detail in section 3.4.

3.3 Measurement Setup Overview

3.3.1 Block Diagram

Up to now only single parts of the measurement setup have been presented. Especially in the context of the parallel paths belonging to the three different frequency bands, it is hard to grasp the full structure of the system by considering each part in its own. For this, Fig. 3.14 shows the full measurement setup including all components that have been mentioned so far.
Also introduced in this figure are two reference planes for the incident wave a_0 and the reflected wave b_0, at the locations where they are measured, respectively. In what follows, a_0 is referred to as the *source signal*, while the reference plane belonging to it is termed *source port*. This is crucial with regard to section 3.4, which describes the calibration of the system.

[19] Keysight U2001A, USB Power Sensor

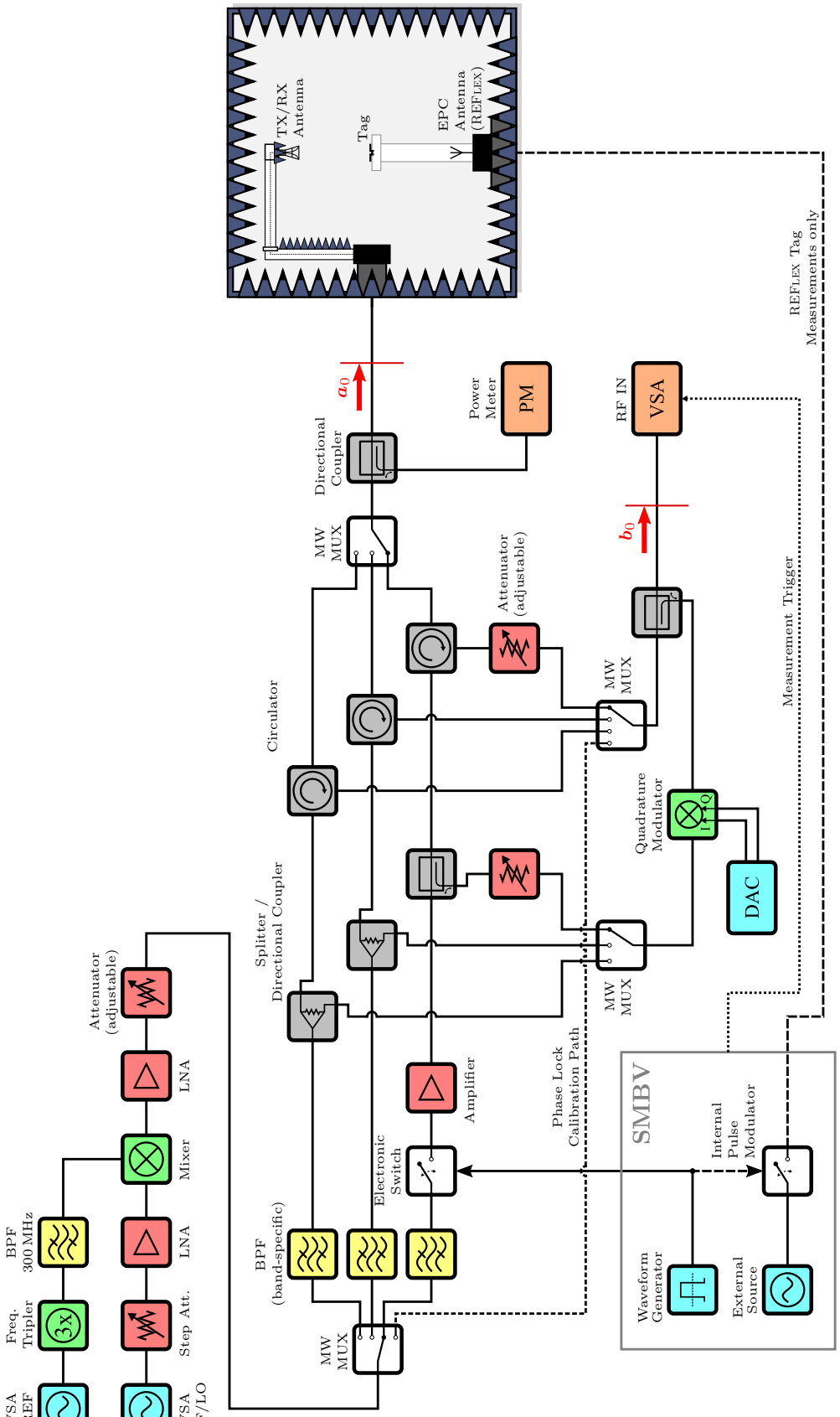


Figure 3.14: Measurement setup including all deployed components. Also the reference planes of the incident wave (a_0) and the measured wave (b_0) are indicated. The frequency path is set here for the UHF band. The parts of the previously indicated 'adjustable attenuators', used to set the power level for the measurement, are depicted here separately at their respective position in the setup.

Further, Fig. 3.15 shows an overview picture of the setup.

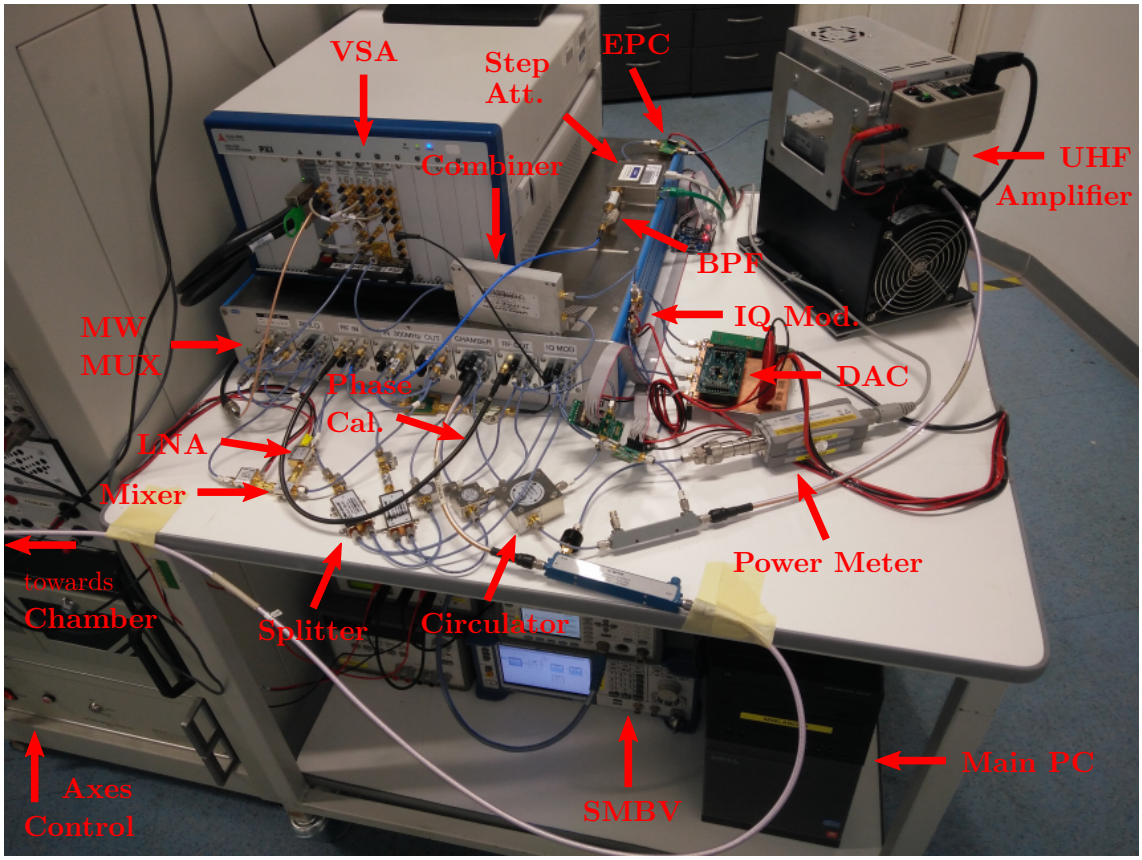


Figure 3.15: The main components of the full measurement setup are indicated in this picture. Note that a second cable into the chamber is necessary for the REFLEX tags, which is not present here.

3.3.2 Link Budget

With regard to the small signal levels that are to be measured using the introduced setup, a consideration of all involved signal and noise levels is apposite. Fig. 3.16 shows a simplified block diagram like it is used for one single frequency band as well as a link budget from the point where the (still unfiltered) carrier signal[20] is present, up to the VSA. For reasons of clarity, and since their influence can be considered to be minor, the multiplexers and the directional coupler used for the power level measurement are omitted, their insertion loss is included in adjacent components. The adjustable attenuators and the amplifier marked as '(UHF)' are not part of the paths through the setup for the two higher frequency bands. They are not necessary there due to the lower power levels involved as well as the reduced power range of the source signal.

[20] The indicated power levels are valid for the carrier frequency. Spurious lines are not of interest and removed by the BPF.

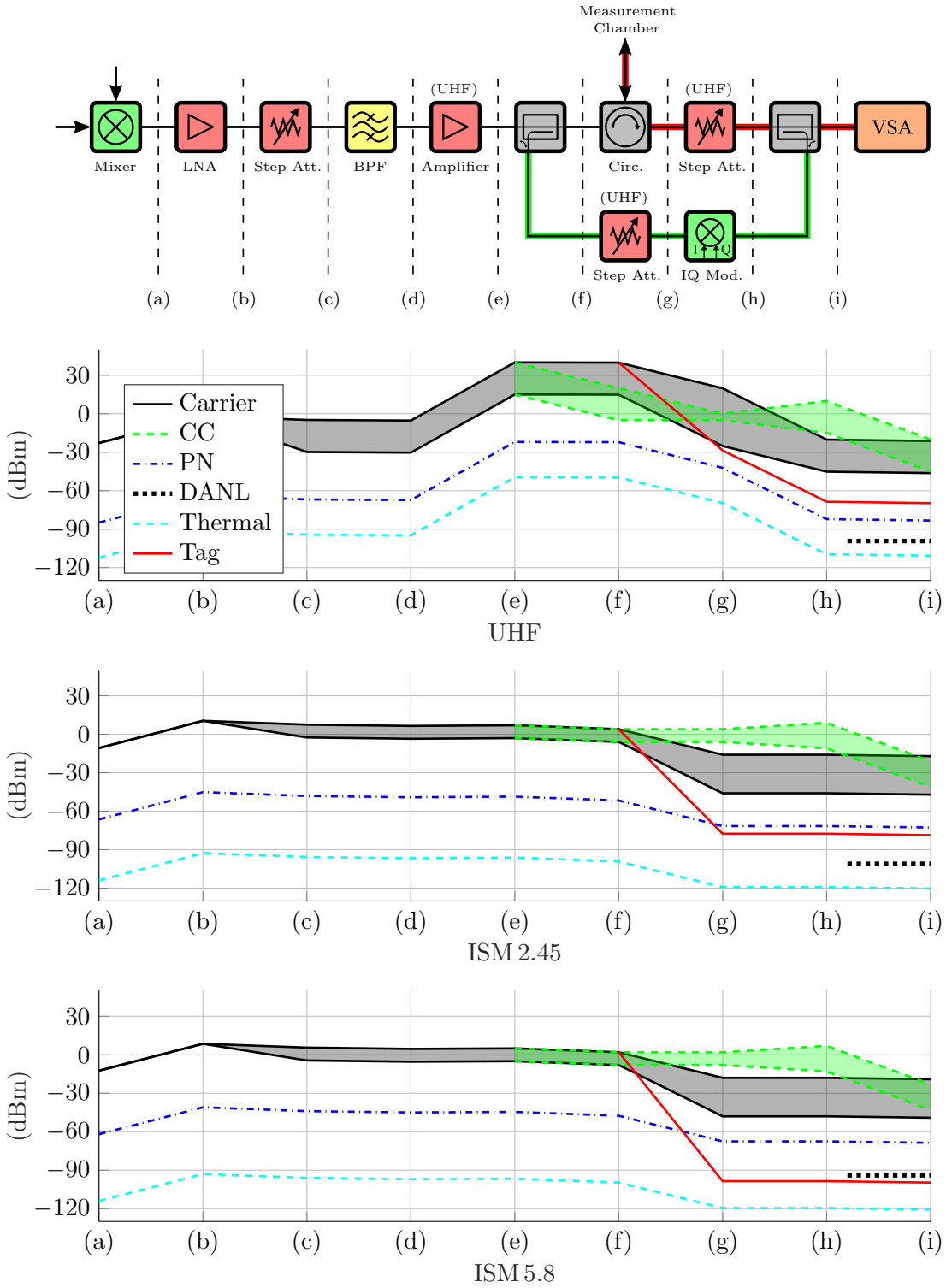


Figure 3.16: Link budget of the entire measurement system. The block diagram only depicts the circuit for a single frequency band.

At node (a), the source signal is present the first time. It is pre-amplified by the LNA at node (b), to achieve a certain power level, which is already ready to be used as such for the

ISM bands and can be amplified by an amplifier more powerful, though worse performing in terms of its noise figure. The programmable attenuator at node (c) is used to adjust the power level finally radiated towards the tag. In the link budget, it spans a range of 25 dB in the UHF and 10 dB in the ISM bands, respectively. The signal is then filtered by the band-specific BPF at node (d) and amplified in the case of the UHF band at node (e). At (f), the signal is split into main path and carrier cancellation (CC) (highlighted green). The main path is routed to the measurement chamber via the circulator, comprising the component scattered back by the DUT[21] (highlighted in red). For the UHF band, the CC signal has to be attenuated to meet the LO demands of the IQ modulator at node (g). This is also the case for the component on the main path at node (h). This of course means that also the desired signal component is attenuated, which turns out to be irrelevant, since the limiting phase noise (PN) is attenuated in the same way. After recombining the two paths at node (i), the unwanted reflections on the main path and the adjusted signal on the CC path cancel out. The tag reflection and the residual carrier signal are then sampled by the VSA.

Besides the actual signal components, also the disruptive noise levels for the respective measurement bandwidths are indicated. First, the PN level is derived from the values measured in section 3.2.2 by integrating the curves up to the frequencies according to the band-dependent measurement bandwidths. This is only an approximation, since the actual impairments due to PN also depend on the phasing of the desired signal. While the signal reflected by the tag is modulated between to complex values with arbitrary phase position, the PN does not influence the magnitude. Accordingly, it may or may not have an influence on the resulting noise. Also, since the signal coming from the tag is recorded over some period of time, averaging and demodulation techniques can be used to improve the experienced SNR. All in all, this means that although the PN is the limiting factor for at least the UHF and the ISM 2.45 band, the signal levels are high enough to obtain useful results. Because the PN remains always in a fixed relation to the carrier, additional amplification does not improve the SNR. The PN is marked in Fig. 3.16 as blue chain dotted line.
The constant black chain dotted line marks the so called displayed average noise level (DANL) of the used measurement device for the used settings, which are optimized to keep it as low as possible. It can be seen as the absolute noise floor of the setup which cannot be lowered any more in any way. Nevertheless, similar to the PN averaging of the measured signal and demodulation can be used to achieve improvements.
For comparison, finally also the thermal noise for room temperature is marked in the plot as light blue dashed line. However, the measurements have shown that it is not the limiting factor of the system.

3.4 Calibration

This section describes the calibration of the measurement setup. This is an essential part of the measurement procedure, since it allows for the correct calculation of the ΔRCS using the measured results.

[21] See Fig. 3.7 for the relative levels of unwanted reflections and the component reflected by the tag. A lower limit of the tag component does not make sense, since the actual level may be much smaller, depending on the current view on the antenna pattern of the tag.

In section 3.4.1, the theoretical background is stated. Also a simplification is suggested and its legitimacy is proven. In what follows, the particular steps of the calibration are described. Besides the characterization of the involved cables and the probe antenna as already mentioned in section 3.2.5, the calibration consists of three major parts. The calibration of the phase state of the source in section 3.4.2, the calibration of the forward path into the chamber in section 3.4.3 and the calibration of the backward path to the measurement device in section 3.4.4. Moreover, some considerations regarding the source power are stated in section 3.4.5.

3.4.1 Theory

The ΔRCS is related to

$$\Delta\boldsymbol{\Gamma} = \boldsymbol{\Gamma}^{(a)} - \boldsymbol{\Gamma}^{(b)} \ , \tag{3.11}$$

by

$$\left[\sqrt{\Delta\boldsymbol{\sigma}}\right] = \sqrt{4\pi R^2}\, e^{jk_0 R}\, \Delta\boldsymbol{\Gamma} \ , \tag{3.12}$$

where $\boldsymbol{\Gamma}^{(a)}$ and $\boldsymbol{\Gamma}^{(b)}$ are the reflection coefficients of the tag in the two possible modulation states, respectively, as defined in section 2.2.

The calibration has to take into account all components in the setup, from producing the carrier frequency, over the path switching network, the separation of the waves to and from the anechoic chamber, the chamber itself including the probe antenna, and finally the air path to the tag. Due to the complexity of the system, a calibration piece by piece is not feasible. Also the air path is difficult to capture. Therefore, an overall calibration is preferred.

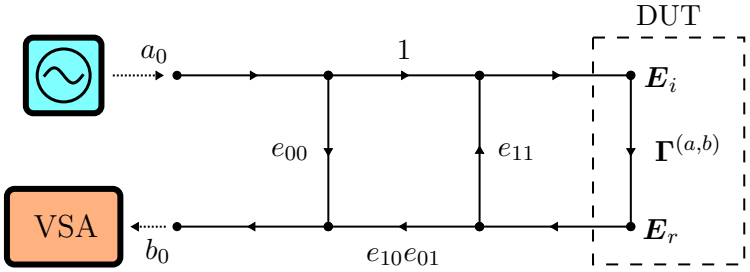


Figure 3.17: Three-term error model.

An approach using a full standard one-port calibration method with a three-term error model as seen in Fig. 3.17 turns out to be problematic. The carrier cancellation has to be able to adapt to each state of the setting with fine accuracy. Its state can be seen as unknown beforehand in general. A mathematical examination of the problem leads to the expression

$$\Delta\boldsymbol{\Gamma} = \frac{\Delta\boldsymbol{\Gamma}_0}{e_{10}e_{01}} \left[\left(1 + \frac{e_{11}\left(\boldsymbol{\Gamma}_0^{(a)} - e_{00}\right)}{e_{10}e_{01}} \right) \left(1 + \frac{e_{11}\left(\boldsymbol{\Gamma}_0^{(b)} - e_{00}\right)}{e_{10}e_{01}} \right) \right]^{-1} \ , \tag{3.13}$$

where $\Delta\mathbf{\Gamma}_0$ is defined analogous to eq. (3.11) for the measured reflection coefficients of the two modulation states $\mathbf{\Gamma}_0^{(a,b)} = \frac{b_0^{(a,b)}}{a_0}$ as

$$\Delta\mathbf{\Gamma}_0 = \mathbf{\Gamma}_0^{(a)} - \mathbf{\Gamma}_0^{(b)} \ . \tag{3.14}$$

It is calculated from the normalized power waves[22] a_0 and b_0 for the two modulation states of the tag and must be corrected to obtain $\Delta\mathbf{\Gamma}$. The error term e_{00} corresponds to the *directivity*, e_{11} to the *port match* and $e_{10}e_{01}$ to the *tracking* of the error box[23].
Obviously, the e_{00} term containing the carrier cancellation path does not disappear from eq. (3.13) by simply calculating the difference of the measured values $\mathbf{\Gamma}_0^{(a)}$ and $\mathbf{\Gamma}_0^{(b)}$. This means that it has direct influence on the error terms and hence, the result. A calibration valid for one specific state of the carrier cancellation will fail for any other state.
Nevertheless, it can be shown that eq. (3.13) is approximated well by

$$\Delta\mathbf{\Gamma} \approx \widetilde{\Delta\mathbf{\Gamma}} = \frac{\Delta\mathbf{\Gamma}_0}{e_{10}e_{01}} \ , \tag{3.15}$$

which means that the calculation of $\Delta\mathbf{\Gamma}$ is indeed de facto independent from the state of the carrier cancellation.

In order to get an estimation of the error this approximation can cause, the expressions in square brackets of eq. (3.13) can be stated in terms of $\mathbf{\Gamma}^{(a,b)}$, the reflection coefficients for the reference planes as defined in section 2.2. This leads to

$$\Delta\mathbf{\Gamma} = \frac{\Delta\mathbf{\Gamma}_0}{e_{10}e_{01}} \left[\left(1 - e_{11}\mathbf{\Gamma}^{(a)}\right) \left(1 - e_{11}\mathbf{\Gamma}^{(b)}\right) \right] \ , \tag{3.16}$$

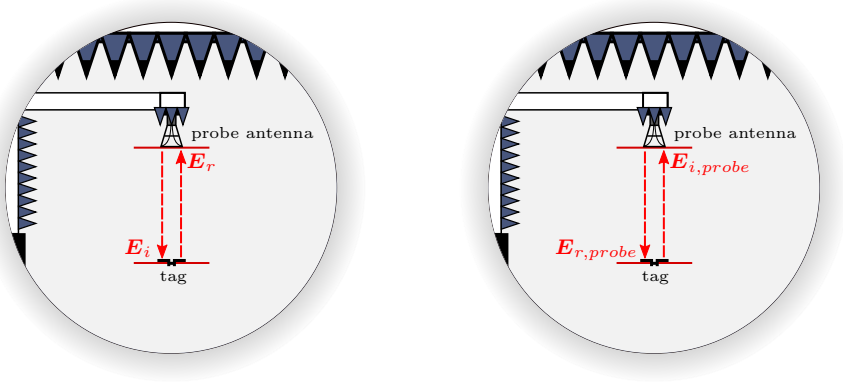
where besides $\mathbf{\Gamma}^{(a,b)}$ only $e_{10}e_{01}$ and e_{11} remain. The former only as linear factor, representing the cable losses and the free space path loss. However, the term e_{11} denotes the component of the wave reflected by the tag, which is scattered back towards the tag again. Assuming the environment of an anechoic chamber, the main component of this term stems from reflections at the probe antenna itself.
Recalling Fig. 2.2 makes clear that whatever is reflected at the probe antenna back towards the tag has to travel the distance between the probe antenna and the tag antenna in order to contribute to the term $e_{11}\mathbf{\Gamma}$. Besides that, also the parameter $\mathbf{\Gamma}$ contains this distance. Due to the propagation through free space, the waves thereby experience a loss of about 30 dB per direction[24]. Although this already indicates rather small values for the term $e_{11}\mathbf{\Gamma}$, a better assessment can be reached when applying the already introduced idea of RCS.
Fig. 3.18 shows the concept of the RCS calculation of eq. (2.15) applied to both the tag and the probe antenna as

$$\sigma_{tag} = 4\pi R^2 \left| \frac{\boldsymbol{E}_r}{\boldsymbol{E}_i} \right|^2 \ , \qquad \sigma_{probe} = 4\pi R^2 \left| \frac{\boldsymbol{E}_{r,probe}}{\boldsymbol{E}_{i,probe}} \right|^2 \ . \tag{3.17}$$

[22] The normalized power wave is defined as $a := \frac{V}{\sqrt{Z_w}}$, with the characteristic impedance Z_w of the cable and the complex-valued voltage amplitude V of the wave. It has a unit of $\sqrt{\mathrm{W}}$ and is related to the power of the wave as $P = \frac{1}{2}|a|^2$.

[23] e_{00}, e_{01}, e_{10}, e_{11}, and all wave quantities are complex-valued in general. Nevertheless, due to readability they are not denoted in bold letters here.

[24] Estimated using the concept of FSPL.



(a) Calculation of σ_{tag}. **(b)** Calculation of σ_{probe}.

Figure 3.18: Concept of RCS calculation for probe and tag.

Applying $\mathbf{\Gamma} = \frac{\boldsymbol{E}_r}{\boldsymbol{E}_i}$ and $\mathbf{\Gamma}_{probe} = \frac{\boldsymbol{E}_{r,probe}}{\boldsymbol{E}_{i,probe}}$, eq. (3.17) can be rewritten as

$$|\mathbf{\Gamma}| = \sqrt{\frac{\sigma_{tag}}{4\pi R^2}}\ , \qquad |\mathbf{\Gamma}_{probe}| = \sqrt{\frac{\sigma_{probe}}{4\pi R^2}}\ , \tag{3.18}$$

respectively. Assuming, that all sources of reflections except the probe antenna can be neglected and σ_{probe} describes all effects regarding this antenna, the error term is $|e_{11}| = |\mathbf{\Gamma}_{probe}|$. Finally this leads to

$$|e_{11}\mathbf{\Gamma}| = \frac{\sqrt{\sigma_{tag}\sigma_{probe}}}{4\pi R^2}\ . \tag{3.19}$$

Measurements in the UHF band yield for example a maximum RCS of RFID tags in the order of $\sigma_{tag} \approx -20\,\mathrm{dBsm}$. As for the probe antenna, in this band the RCS, including the structural mode as described in [17], as well as the antenna mode for an antenna load better 20 dB, takes on values in the order of $\sigma_{probe} \approx -20\,\mathrm{dBsm}$. With $R = 1.31\,\mathrm{m}$ this leads to $|e_{11}\mathbf{\Gamma}| \approx -33\,\mathrm{dB}$.
Following all the previous considerations, a relative error for can be defined as

$$\gamma = \left| \frac{\widetilde{\Delta\mathbf{\Gamma}} - \Delta\mathbf{\Gamma}}{\Delta\mathbf{\Gamma}} \right|\ . \tag{3.20}$$

With the maximum values measured in the UHF band this becomes $\gamma \approx -60\,\mathrm{dB}$. This is sufficiently small, given that this is even a worst case assumption.

Finally, another, very intuitive point of view shall be stated, regarding the influence of the carrier cancellation on the calibration. Assuming that e_{11} can be neglected, the value of e_{00} for a given carrier cancellation setting remains constant no matter what backscatter state the tag is currently in. This means that the wave denoted by b_0 in Fig. 3.17 has a constant part $e_{00}a_0$ in both cases. When calculating the difference between those two

values in order to get $\Delta\mathbf{\Gamma}_0$, this constant part disappears shown in eq. (3.21).

$$\begin{aligned}\Delta\mathbf{\Gamma}_0 &= \mathbf{\Gamma}_0^{(a)} - \mathbf{\Gamma}_0^{(b)} \\ &= \frac{b_0^{(a)}}{a_0} - \frac{b_0^{(b)}}{a_0} \\ &\approx \frac{e_{10}e_{10}\mathbf{\Gamma}^{(a)}a_0 + e_{00}a_0}{a_0} - \frac{e_{10}e_{10}\mathbf{\Gamma}^{(b)}a_0 + e_{00}a_0}{a_0} \\ &\approx \left(e_{10}e_{10}\mathbf{\Gamma}^{(a)} + e_{00}\right) - \left(e_{10}e_{10}\mathbf{\Gamma}^{(b)} + e_{00}\right) \\ &\approx e_{10}e_{10}\,\Delta\mathbf{\Gamma}\ . \end{aligned} \tag{3.21}$$

Apparently, this is equivalent to eq. (3.15).

By using the approximation eq. (3.15), the calibration only has to provide the tracking parameter $e_{10}e_{01}$, in order to calculate $\Delta\mathbf{\Gamma}$ and subsequently the ΔRCS.
Besides that, the two normalized power wave quantities a_0 and b_0 must be known to allow for the correct calculation of $\Delta\mathbf{\Gamma}_0$.

While b_0 can be simply derived from the signal V_{pk} measured by the VSA by

$$b_0 = \frac{V_{pk}}{\sqrt{Z_w}}\ , \tag{3.22}$$

with a reference impedance of $Z_w = 50\,\Omega$, the case is more complicated for a_0. A source calibration is necessary prior to all further steps.

3.4.2 Source Calibration

The complex-valued a_0 can only be measured directly by using a measurement device with fixed phase relation to the VSA. Since this is not feasible with the available measurement equipment, a different way of determining this value has to be chosen. Magnitude and phase are determined separately.

Magnitude

The magnitude of a_0 can simply be calculated from the power of the incident wave measured by the power sensor introduced in section 3.2.6. The influence of the directional coupler, necessary to split off a part of the incident wave, has to be removed by using its pre-measured S-parameters. This leads to the corrected power P_{a_0} of the wave at the reference plane of a_0. The magnitude can be calculated by

$$|a_0| = \sqrt{2P_{a_0}}\ . \tag{3.23}$$

Phase

As the phase of a_0 cannot be measured directly, it is necessary to determine it differently. Fortunately, due to the principle of the source signal generation as introduced in section 3.2.2, the phase of this signal measured by the VSA is always the same for a certain center frequency setting, except for the phase offset stemming from the random phase locking of the VSA. However, this offset can be measured upon initialization as it remains constant thereafter. Hence, even though the phase of a_0 is not known beforehand, it still has a deterministic dependence on the respective setting of the source power level and the center frequency.
During the source calibration procedure, the source port is connected to the RF IN connector of the VSA using a known cable[25]. Sweeping through the entire possible frequency and source power range allows to record all respective phase states of a_0. Coherence is ensured because the VSA is used for this measurement. As for the necessary frequency resolution, a linear phase response of the system is assumed. With an overall length of the source system not greater than 3 m, phase unambiguity is avoided using frequency steps of $\Delta f < 75\,\mathrm{MHz}$[26]. For frequency points not measured during the calibration, an interpolation of the phase response is applied. In this way, $arg(a_0)$ is known at any time. Together with the already known wave b_0, $\Delta\boldsymbol{\Gamma}_0$ can be calculated as

$$\Delta\boldsymbol{\Gamma}_0 = \frac{b_0}{|a_0|\, e^{j \arg(a_0)}} \ . \tag{3.24}$$

3.4.3 Forward Path Calibration

The forward path calibration has to provide the information about the relationship between the source wave a_0 and the incident electric field strength $\boldsymbol{E}_i$ at the position of the tag.

Fig. 3.19 shows the principle of this calibration step. A reference antenna identical to the probe antenna is mounted at the position of the tag. This allows to capture the electric field strength at this position. In order to obtain a coherent measurement result, the port of the antenna has to be connected to the VSA. This is done using the *phi*-stage connection of the anechoic chamber. All the cables used to establish this connection have to be known and their influence has to be removed from the measured results. In this way, the parameter $\boldsymbol{A}$ can be determined which is defined as the relation between the wave at the source port a_0 and the wave at the port of the reference antenna a_1 as

$$\boldsymbol{A} := \frac{a_1}{a_0} \ , \tag{3.25}$$

for a selection of frequencies similar to the one explained in section 3.4.2. Introducing further the complex-valued parameter

$$\boldsymbol{S}_{ant,ref} := \frac{a_1}{\boldsymbol{E}_i} \ , \tag{3.26}$$

[25] This connection actually comprises an attenuator in addition to a simple cable, since power levels up to 40 dBm occur.
[26] This is the case for a group delay $\tau_{gr} < \frac{1}{\Delta f}$. The actual calibration uses $\Delta f = 1\,\mathrm{MHz}$.

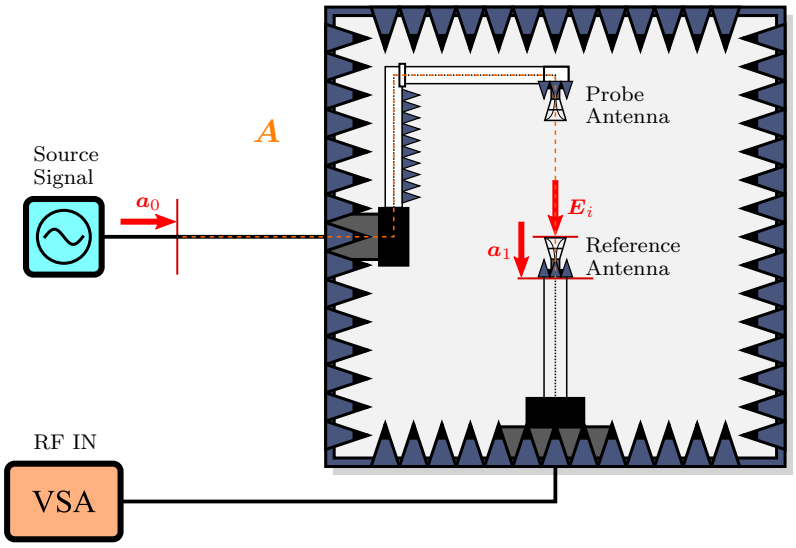


Figure 3.19: Schematic of the forward path calibration.

to represent the relation between the normalized power wave a_1 at the antenna port and the electric field strength $\boldsymbol{E}_i$ at the position of the reference antenna allows to express $\boldsymbol{E}_i$ in terms of a_0 as

$$\boldsymbol{E}_i = \frac{\boldsymbol{A}}{\boldsymbol{S}_{ant,ref}}\, a_0 \ . \tag{3.27}$$

3.4.4 Backward Path Calibration

Analogous to the forward path calibration, the backward path calibration provides an expression for the relation between the wave b_0 measured by the VSA and the electric field strength $\boldsymbol{E}_r$ at the position of the probe antenna.

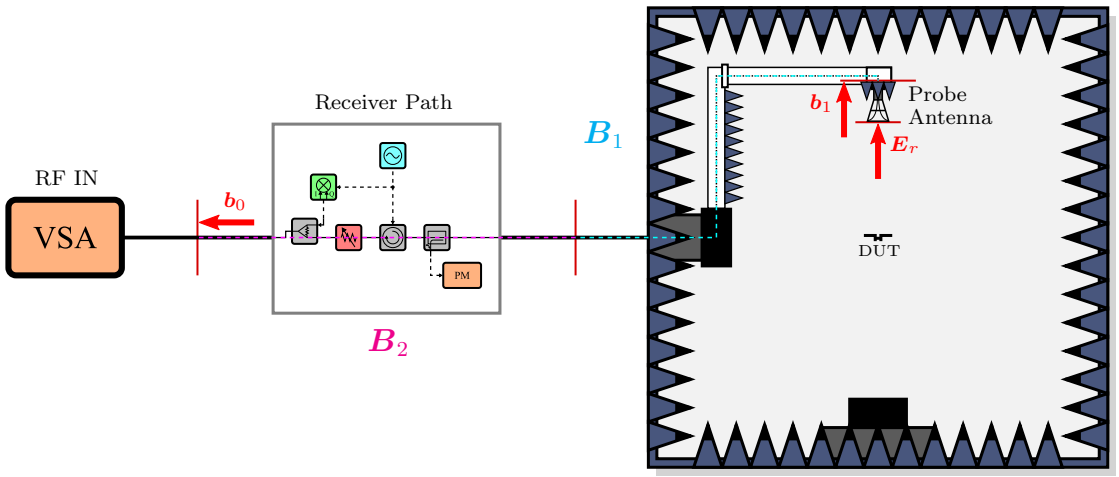


Figure 3.20: Schematic of the backward path calibration.

An overview of the situation can be seen in Fig. 3.20. In contrast to the forward path calibration, no air path is involved here. Nevertheless, the probe antenna still has to be

considered. Again, by defining parameters similar to eq. (3.25) to eq. (3.27), the relation between the measured wave b_0 and the wave at the probe antenna port b_1 can be expressed as

$$\boldsymbol{B} := \frac{b_0}{b_1} \ . \tag{3.28}$$

This parameter can be split into two parts. One for the connection from the probe antenna to the measurement port denoted as $\boldsymbol{B}_1$ and one for the path through the measurement system up to the VSA RF IN connector denoted by $\boldsymbol{B}_2$ with the relation

$$\boldsymbol{B} = \boldsymbol{B}_1 \boldsymbol{B}_2 \ . \tag{3.29}$$

A slight difference to eq. (3.25) is that the direction of the path is reversed. This is important, because the two-port represented by $\boldsymbol{B}_2$ is not reciprocal because of the circulators involved.
By introducing again a parameter

$$\boldsymbol{S}_{ant,probe} := \frac{b_1}{\boldsymbol{E}_r} \ , \tag{3.30}$$

the electric field strength $\boldsymbol{E}_r$ can be expressed in terms of b_0 as

$$\boldsymbol{E}_r = \frac{1}{\boldsymbol{B}\boldsymbol{S}_{ant,probe}} \, b_0 \ . \tag{3.31}$$

It turns out to be problematic to use the measurement system as a source and a measurement device at the same time for this calibration in this case, since the entire receiver path through the measurement system is part of the calibration and cannot be simply skipped like it is done in the forward path calibration. Thus, all necessary values have to be determined by an external two-port vector network analyzer. This does not pose a problem in the case of $\boldsymbol{B}_1$, but gets slightly more complicated for $\boldsymbol{B}_2$. Although the influence of the carrier cancellation can be neglected as demonstrated in section 3.4.1, there are still various different possible settings that have influence on $\boldsymbol{B}_2$. For this, the parameter has to be measured for all possible settings of the attenuator which performs the leveling of the receive signal for the carrier cancellation and for a selection of possible frequencies, considering also the different paths for the three frequency bands.

Summary

Using the expressions for $\boldsymbol{E}_i$ and $\boldsymbol{E}_r$ stated in eq. (3.27) and eq. (3.31), $\boldsymbol{\Gamma}$ can be rewritten as

$$\boldsymbol{\Gamma} = \frac{\boldsymbol{E}_r}{\boldsymbol{E}_i} = \frac{1}{\boldsymbol{A}\boldsymbol{B}} \frac{\boldsymbol{S}_{ant,ref}}{\boldsymbol{S}_{ant,probe}} \boldsymbol{\Gamma}_0 \ . \tag{3.32}$$

Recalling the assumption that the probe and the reference antenna have the exact same magnitude and phase behavior, this expression becomes

$$\boldsymbol{\Gamma} = \frac{1}{\boldsymbol{A}\boldsymbol{B}} \boldsymbol{\Gamma}_0 \ . \tag{3.33}$$

Interestingly, the dependence on the antenna disappears. Comparing this with eq. (3.15), identifies the tracking parameter

$$e_{10}e_{01} = \boldsymbol{A}\boldsymbol{B} \ . \tag{3.34}$$

3.4.5 Surface Power Density Calibration

With a working calibration, the measurement setup is capable of measuring the complex-valued ΔRCS correctly. Namely, for any frequency set as center frequency of the VSA as well as any power level set via the programmable attenuator in the carrier signal generation part of the system. However, the power density level at the tag position remains unknown. Not only does the power of the RF/LO signal available from the VSA vary considerably over frequency, but also the losses along the path towards the tag show a strong frequency dependence. Besides the frequency responses of the different components, this is mainly due to the long cable length into the anechoic chamber, where non-negligible reflections and hence, notches in its frequency response occur. As a consequence, the setting of the programmable attenuator does not represent the actual surface power density and the magnitude of the electric field strength at the position of the tag. In order to obtain the correct levels of electric field strength at the tag position, belonging to the current $\boldsymbol{\Gamma}$, eq. (3.27) may be used. Since the phase is not of importance here, the phase information may be disregarded. This leads to

$$E_i = |\boldsymbol{E}_i| = \frac{|\boldsymbol{A}|}{|\boldsymbol{S}_{ant,ref}|}\,|a_0| \ . \tag{3.35}$$

With $\boldsymbol{A}$ and a_0 already known, it remains to take a closer look at $\boldsymbol{S}_{ant,ref}$, since this term does not disappear like in the previous calibration. The absolute value of the parameter is related to the known gain G_{ref} of the reference antenna via the relations eq. (2.10) and eq. (2.12) as

$$|\boldsymbol{S}_{ant,ref}| = \sqrt{\frac{\lambda^2}{4\pi}\frac{G_{ref}}{Z_0}} \ , \tag{3.36}$$

while the phase remains unknown. Fortunately, it is not needed here. The magnitude of the electric field strength of the incident wave can be calculated as

$$E_i = \sqrt{\frac{4\pi}{\lambda^2}\frac{Z_0}{G_{ref}}}\,|\boldsymbol{A}|\ |a_0| \ . \tag{3.37}$$

With the source power belonging to a_0 of $P_0 = \frac{|a_0|^2}{2}$, the surface power density of the incident wave at the tag position becomes

$$S_i = \frac{4\pi}{\lambda^2}\frac{|\boldsymbol{A}|^2}{G_{ref}}\,P_0 \ . \tag{3.38}$$

3.5 Parameters & Postprocessing

With the measurement system up and running, as well as a functional correction, all that remains are the necessary settings and an extraction algorithm to obtain the ΔRCS from the captured traces.
The essential parameters to be set determine the behavior of the tag itself, the bandwidth, and the spacing of the measured frequency points.

3.5.1 Parameters

Tag Settings

As already indicated in section 2.3, it is beneficial to have a tag response consisting of a continuous modulation as long as possible. For EPC compliant tags, this can be influenced by the choice of the Miller sequence. It becomes clear from Fig. 2.5, that M = 8 provides the longest continuously modulated preamble and is therefore chosen here.

The EPC communication is reduced to the minimum necessary amount to receive a reply from the tag. This is a so called *query*-command, which activates the tag and triggers a response. In the case of the REFLEX tag, the response in the ISM band around 2.45 GHz is also triggered when powering up the tag.

Another important point is the BLF. It can also be chosen for EPC compliant tags within the *query*-command. Thereby, two edge cases have to be considered. A low BLF in the order of some tens of kHz means that the spectral lines of the tag answer are close to the carrier. Since a certain amount of phase noise remains despite all taken measures, it is the limiting factor here and the tag response might be 'drowned' in noise. On the one hand, due to the rather steep decrease of the phase noise when moving away from the carrier, a higher BLF avoids this problem. On the other hand, this means that a wider analysis bandwidth of the VSA is necessary to capture the same amount of energy belonging to the tag response. However, also a higher amount of noise is received using a higher bandwidth. A BLF of about 40 kHz is used in the measurements[27]. Although this is in the lower range of possible frequencies, it turns out to be the solution yielding best results, since a considerable phase noise contribution can be avoided in that way.

For the battery-assisted backscatter circuit in the ESL, the BLF is determined by the oscillator used to drive the modulation. A wide choice of oscillators is available at a frequency of 32.768 kHz. Since this is similar to the BLF in the other measurements, it is therefore used in this circuit.

Measurement Bandwidth

An important point when using a VSA is the appropriate sampling rate. Here a trade-off is necessary. On the one hand, the bandwidth has to be wide enough to include a major part of the backscatter signals spectrum coming form the tag. In time domain, this is equivalent to a sampling rate high enough to have a sufficient amount of samples during each state of modulation. Fig. 3.21 shows a typical tag response in time and frequency domain with a bandwidth of $BW_{meas} = 1.5\,\text{MHz}$, like it is actually recorded by the measurement system.
On the other hand, a wider spectrum means a higher amount of noise captured. A bandwidth of 1.5 MHz turns out to be a suitable solution. A major portion of about 98 % of the spectral energy of a typical 40 kHz square wave signal as it is produced by the backscatter circuit of a tag is covered.

[27] Due to the limited stability of the LO of the tag, the actual modulation frequency varies around the nominal BLF.

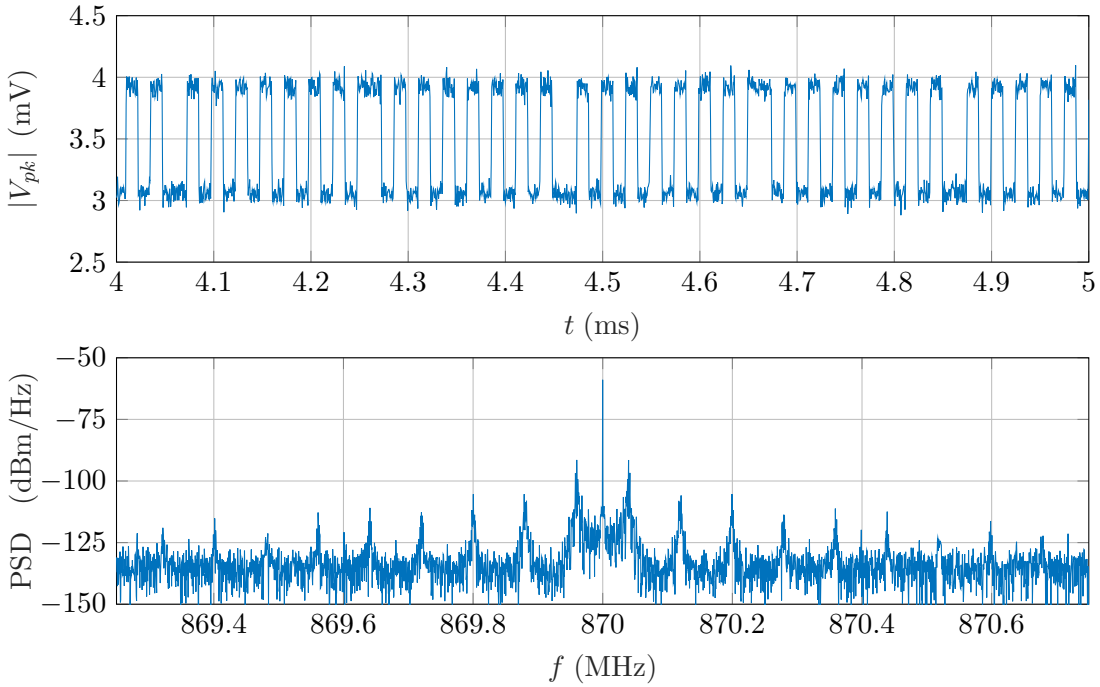


Figure 3.21: Example of a typical EPC tag response with $f_{RF} = 870\,\text{MHz}$ in base-band time domain and as power spectral density (PSD). The high noise floor stems from amplified phase noise.

Frequency Grid

Similar to the calibration described in section 3.4, the spacing of the measured frequency points has to fulfill the condition

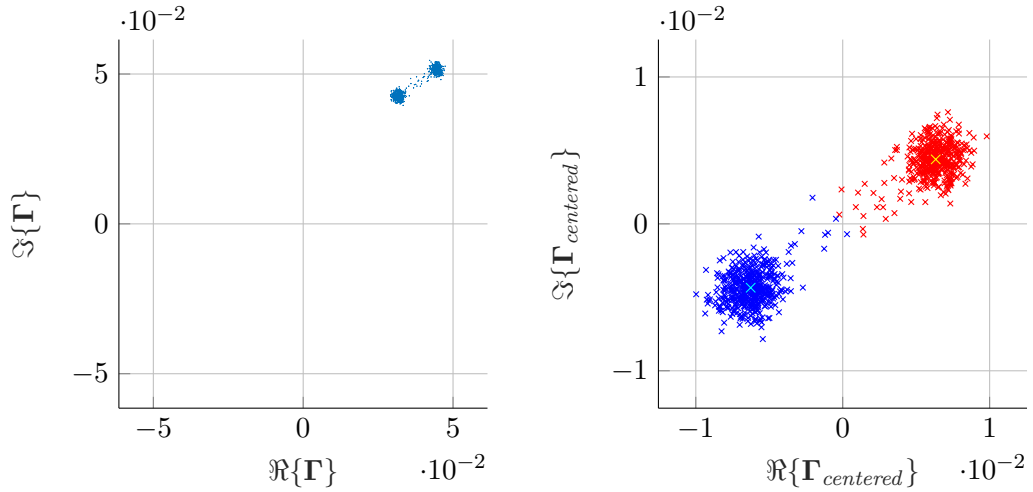
$$\Delta f < \frac{1}{\tau_{gr}} \,, \tag{3.39}$$

with the group delay τ_{gr} of the system, in order to avoid phase ambiguity. This does not pose a severe problem at this point, since the entire signal runtime through the setting is already removed by the calibration. Recalling from section 2.2.3, the runtime that counts is only from the reference plane of the tag to the receiving probe antenna. A frequency grid of $\Delta f = 10\,\text{MHz}$ allows a group delay of $\tau_{gr} = 100\,\text{ns}$ which can be assumed to be much larger than the actual group delay, given the involved dimensions.

3.5.2 Postprocessing

As it can be seen in Fig. 3.21, the time domain response consists of an alternating sequence of the two possible modulation states of the tag. In the case of an EPC compliant communication, the response contains the coded RN16 sequence, preceded by a preamble, in other cases it is simply a continuous square wave.
After applying the necessary correction to the recorded trace, the two states of $\mathbf{\Gamma}$ have to be separated and the ΔRCS can be calculated. For this, the two states have to be identified and separated. Since the signal corresponds to two point clouds in the IQ diagram as seen in Fig. 3.22a. A convenient way of separating these points to obtain the two modulation

states is to use Lloyd's algorithm, which is also known under the term *k-means* clustering [18]. The points can further be corrected by their mean since it represents the remainder of the unwanted carrier reflection that has not been removed by the carrier cancellation. It can be seen as a spectral line at the center frequency in Fig. 3.21 and disappears when calculating the difference of the two states, anyway. The centered and separated points can be seen in Fig. 3.22b. The respective means correspond to the estimations for the two states $\mathbf{\Gamma}^{(a)}$ and $\mathbf{\Gamma}^{(b)}$, shifted by their common mean. They can be used to calculate $\Delta\mathbf{\Gamma}$ and further the ΔRCS according to eq. (2.25).



(a) Trace seen in Fig. 3.21 in the IQ diagram.

(b) Centered and separated traces with their respective means.

Figure 3.22: Exemplary IQ diagrams.

4 Results

In this chapter, measurement results produced by the introduced measurement system are presented. All the results belong to measurements performed in co-polarization of the probe and the tag antenna. Since the measurement chamber comprises a single probe antenna, only monostatic measurement results are available.

Section 4.1 describes test measurements performed to verify the functionality of the measurement setup. The results are compared with theoretical as well as simulated results. Section 4.2 contains an overview of the measurement results for EPC compliant tags at UHF frequencies. Although several different tags have been examined, only the NXP SL3S1204 Ucode7 on TEFLON and the REFLEX tag are presented in detail here. Section 4.3 outlines the results obtained in the ISM frequency range around 2.45 GHz. The REFLEX tag in terms of its 2.45 GHz interface and the modified electronic shelf label (ESL) introduced in section 2.3 are presented.

4.1 System Verification Measurement

As a confirmation of the correctness of the applied system calibration, the analysis of an object with a known RCS is suitable. Since the RCS of objects is a property which is very difficult to access analytically, the selection is limited.

Spherical Reference Target

The best choice would be a perfectly conducting (metallic) sphere. Due to its advantageous properties, it is therefore often used as a standard target for calibrating radar sets. Not only can the RCS be approximated well with simple means, it also approaches a constant value of $\mathrm{RCS}_{sphere} = r^2\pi$ in the high frequency region, with r being the radius of the sphere. According to [19, Sec. 3.2.2], this means $k_0 r > 20$, where $k_0 = 2\pi/\lambda_0$ denotes the free space wave number. In order to apply this constant value RCS_{sphere}, this means for the necessary sphere radius

$$r \overset{!}{>} r_{min} = \frac{20}{k_0} \ . \tag{4.1}$$

The prerequisite to get these results is to perform the measurements under far-field conditions, that is measurement distance $R \gg r$ or equivalently

$$R/r \gg 1 \ . \tag{4.2}$$

Table 4.1 shows an overview of this conditions in the three bands of interest. Obviously, the limitations on R/r arising from eq. (4.1) do not go together at all with the condition stated in eq. (4.2) for the lower two bands. Therefore, to allow for a simple testing, another reference target had to be chosen.

Description	UHF	ISM 2.45	ISM 5.8
f_{center}	900 MHz	2.45 GHz	5.8 GHz
$\lambda_{0,center}$	33 cm	12 cm	5 cm
r_{min}	1 m	40 cm	16 cm
R/r	< 1.2	< 3.3	< 8

Table 4.1: Prerequisites for a spherical reference target in the three bands of interest. Measurement radius $R = 1.31$ m, see section 3.2.5.

Planar Reference Target

Another target with an approximately known RCS, which has also the advantage of easy availability, is a planar metallic object with a rectangular shape. Information to describe such a body can be found for example in [19, Sec. 7.5.2]. There, an RCS approximation is given by

$$\mathrm{RCS}_{calculated} \approx 4\pi \frac{A^2}{\lambda_0^2} \ , \tag{4.3}$$

where A is the area of the plate. This formula is independent of the polarization of the incident wave, as long as the plate is large compared with the wavelength. As a consequence, the concept tends to break down for lower frequencies with $k_0 a/\pi < 1$, where a is the edge length in the case of a square plate.
This approximation can be applied for example to a rectangular aluminum board with edge lengths of $w = 11.8$ cm and $h = 16.7$ cm. In order to get an approximate cut-off frequency f_{co} for the valid range of the calculations, a is chosen as the smallest involved dimension $a = \min(w, h) = 11.8$ cm. This leads to $f_{co} \approx 1.3$ GHz and shows, that the model may be utilized for the ISM bands, whereas this is not the case for UHF frequencies.
This theoretical values are complemented with simulation results produced in the course of the REFLEX project[1]. The simulation settings represent the situation of the measurements described in this work. That is a monostatic measurement scenario with no reflections at the bounding box.
These theoretical results can be compared with the values measured using the built measurement system. Since this system is only capable of measuring the ΔRCS of targets, the empty anechoic chamber is premeasured as a reference. Subtracting this reference values from the values obtained with the plate mounted inside the chamber leads to the

[1] Simulations conducted using the 3D electromagnetic simulation software *CST – Computer Simulation Technology* by DASSAULT SYSTÈMES.

actual RCS. The setup is shown in Fig. 4.1. Fig. 4.2 shows that the measured values are in accordance with the simulation results and the theoretical values, respectively. The involved parameters and the exact results are summarized in table 4.2.

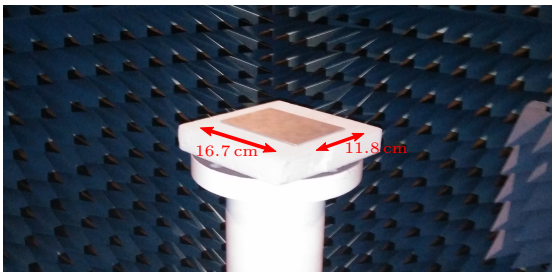


Figure 4.1: Planar reference target in the anechoic chamber.

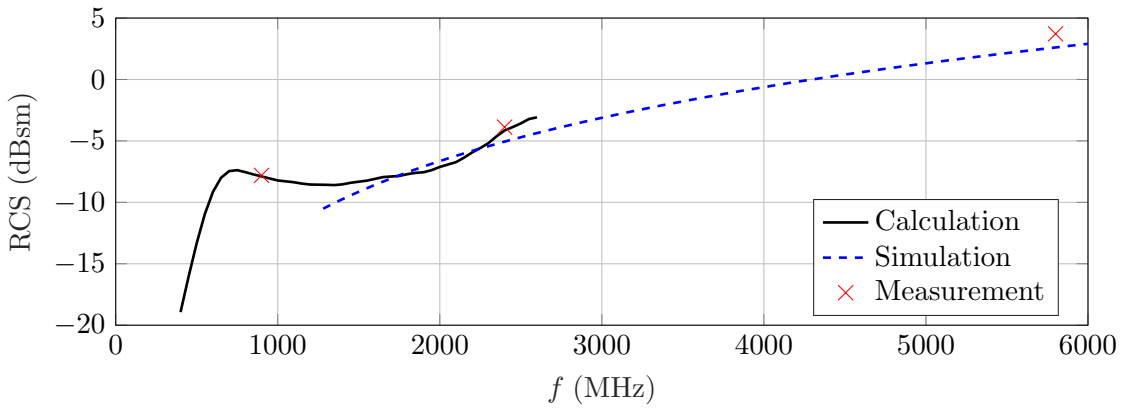


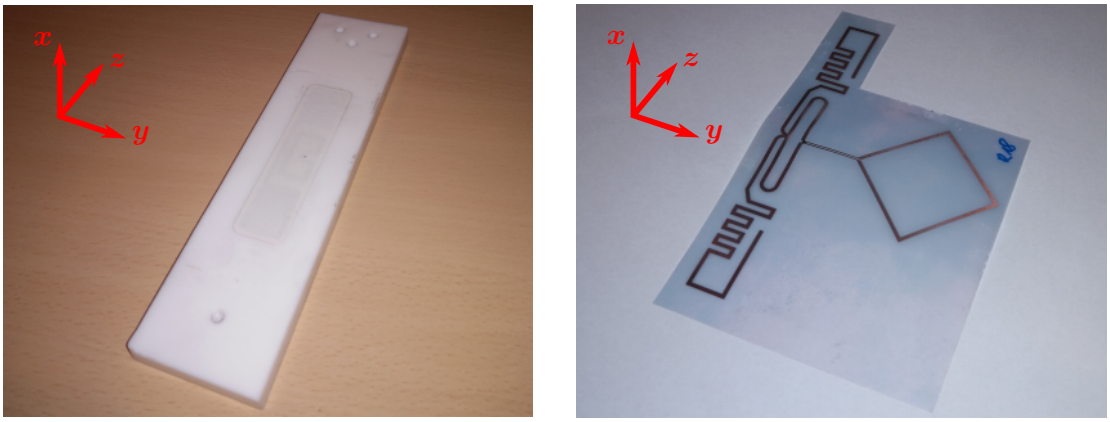
Figure 4.2: The RCS of an aluminum board as planar reference target. Measurement results are shown for the center frequencies of the three bands.

Description	UHF	ISM 2.45	ISM 5.8
f_{center}	900 MHz	2.45 GHz	5.8 GHz
$\lambda_{0,center}$	33 cm	12 cm	5 cm
$k_0 a/\pi$	≈ 0.7	≈ 1.9	≈ 4.6
$\mathrm{RCS}_{calculated}$	n/a	−5.0 dBsm	2.6 dBsm
$\mathrm{RCS}_{simulated}$	−7.9 dBsm	−4.1 dBsm	n/a
$\mathrm{RCS}_{measured}$	−7.8 dBsm	−3.9 dBsm	3.7 dBsm

Table 4.2: Parameters of an aluminum plate as a planar, rectangular reference target. Also, the calculated, simulated and measured RCS values are listed. Measurement radius $R = 1.31$ m, board dimensions $w = 11.8$ cm and $h = 16.7$ cm; $a = \min(w, h) = 11.8$ cm.

4.2 UHF-Measurements

Two different EPC Class-1 Generation-2 tags were measured in the course of this work: One is a NXP Ucode7 type on a TEFLON substrate (Fig. 4.3a). It is referred to simply as Ucode7 in what follows. The other is a REFLEX tag in strong modulation mode, which is also presented regarding its behavior in the 2.45 GHz range later in section 4.3 (Fig. 4.3b). It is noteworthy that this tag comprises two antennas: a meandered dipole antenna for the UHF frequency range and an additional one for the ISM band.



(a) NXP Ucode7 on a TEFLON substrate. **(b)** REFLEX tag.

Figure 4.3: The two DUTs presented in this section.

4.2.1 Power Dependency – Minimum Surface Power Density

The first question to be asked in the context of passive EPC tags is the minimum surface power density S_{min} necessary to power up the tag. The reason is the non-linear behavior of the tags as it can be seen in Fig. 4.4. Furthermore, a frequency and angle dependence of the ΔRCS of the tags has to be expected. This is why the value S_{min} is the best reference in terms of power and hence, serves for all further considerations regarding the UHF band measurement results.
Fig. 4.5 shows the frequency dependence of S_{min}, measured in positive x-direction, for the two tags depicted in Fig. 4.3 at a frequency of 870 MHz, which is in the range of the typical frequencies used to operate such tags. In dependence of the incident angle of the wave, S_{min} reflects the inverse pattern of the tag antenna. In order to emphasize this, the radial axes of Fig. 4.6 are plotted in reverse direction. This means that the maximum value of S is in the center, the minimum at the outer circle. Apparently, the patterns are similar to a dipole pattern for both tags, as it has been assumed earlier.

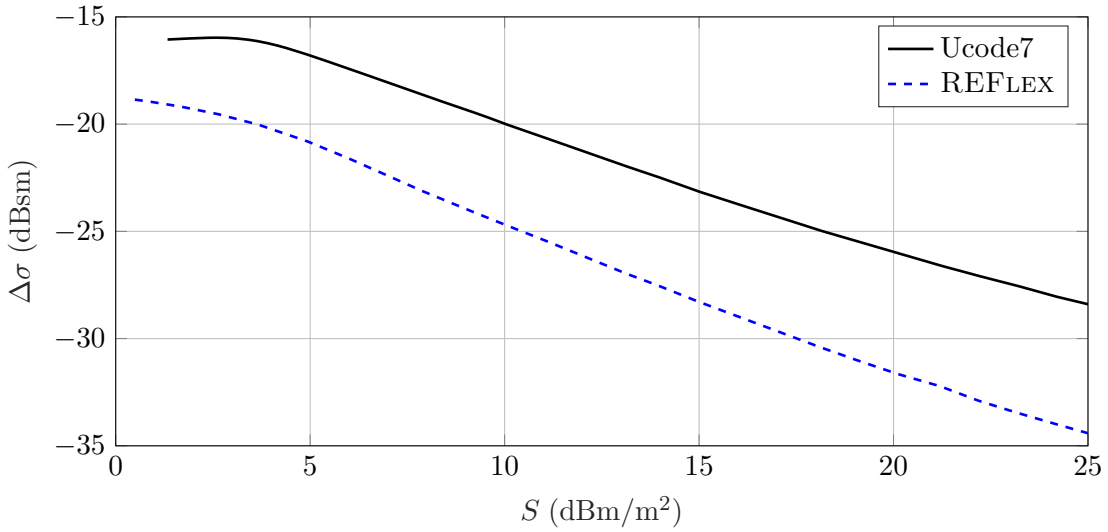


Figure 4.4: The non-linear behavior of tags in the UHF range (870 MHz). Both tags cease to respond below a certain power level S_{min}.

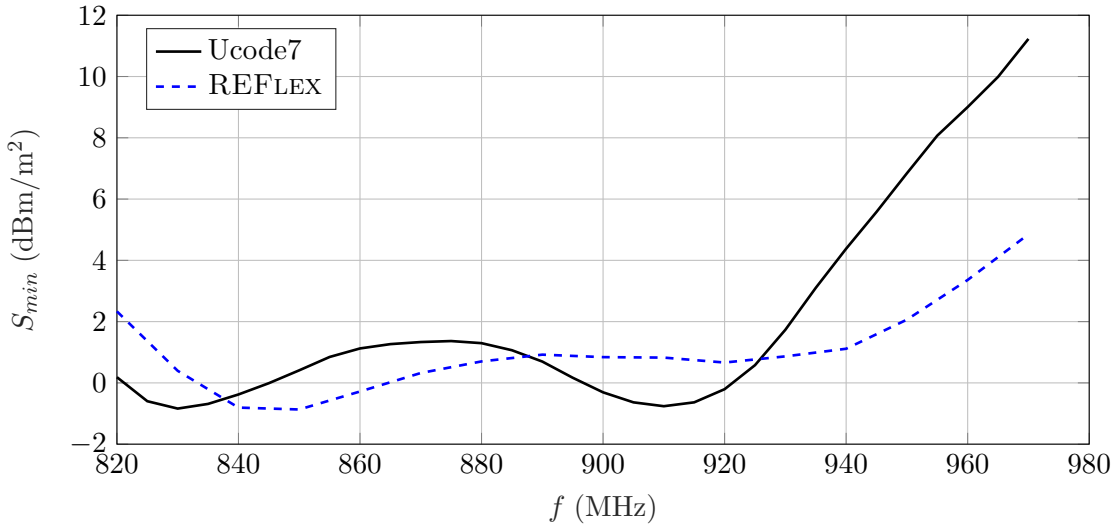
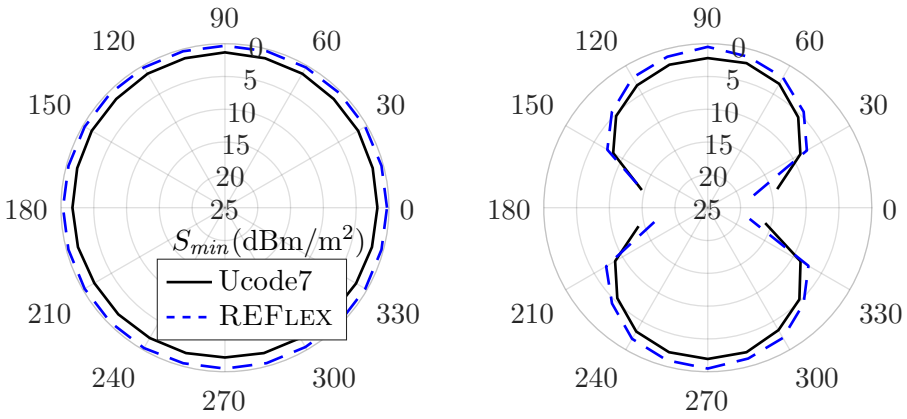


Figure 4.5: The minimum necessary surface power density S_{min} at the position of the tag in order for the tag to be activated.

4.2.2 Scalar ΔRCS

Having defined a reference for the power the tag receives, a meaningful presentation of the ΔRCS can be given. That is as function of frequency for S_{min} and higher powers in constant offset steps of 3 dB, respectively. This is shown in Fig. 4.7.
In spatial domain, for the fixed frequency value, ΔRCS patterns can be plotted as seen in Fig. 4.8.



(a) S_{min} φ-cut. $\varphi = 0$ corresponds to the positive x-direction.

(b) S_{min} ϑ-cut. $\vartheta = 0$ corresponds to the positive z-direction.

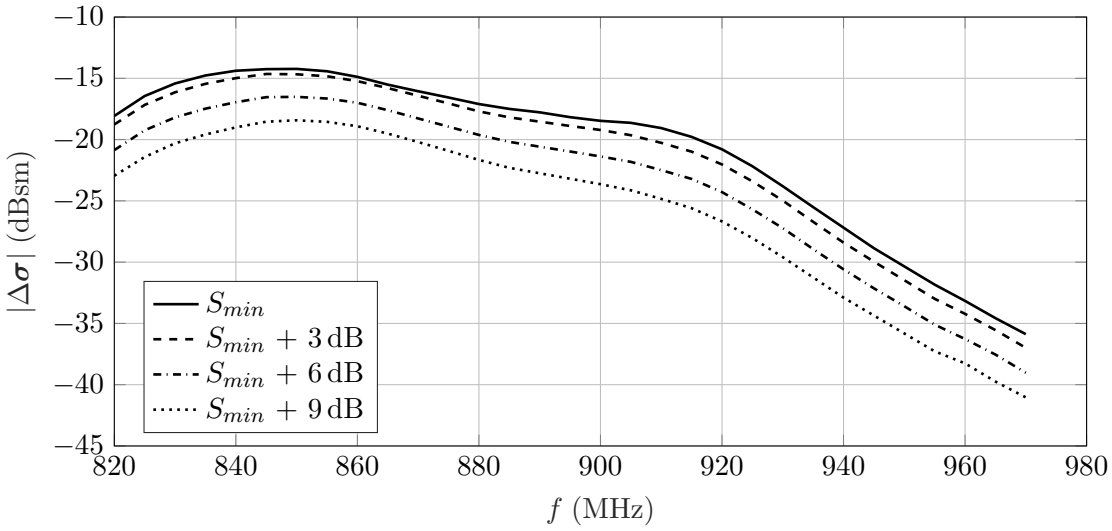
Figure 4.6: Cuts through the patterns of S_{min}. To achieve a representation of the tag antenna pattern, S_{min} is plotted in radial direction in a reverse manner.

4.2.3 Group Delay

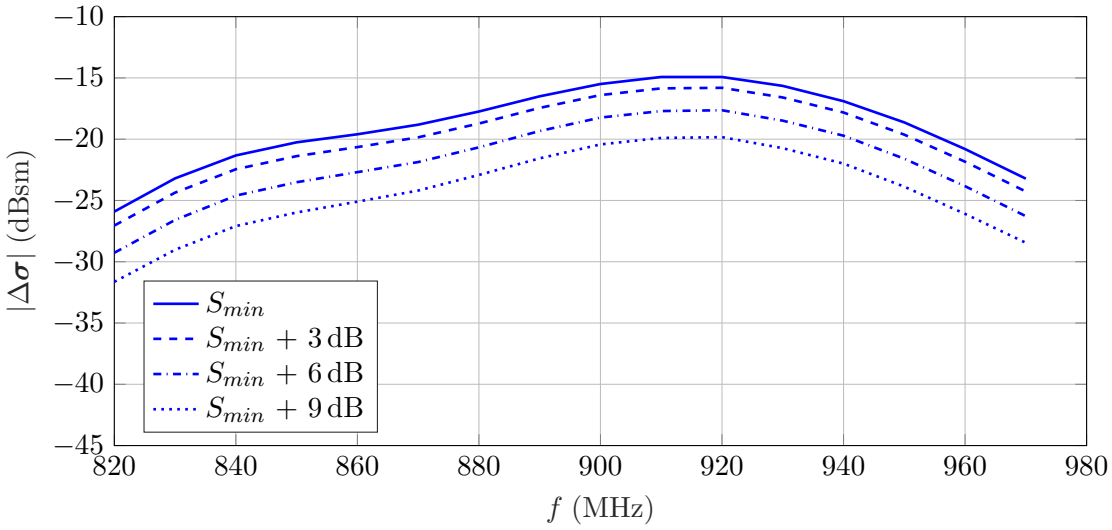
Besides the scalar ΔRCS, the phase information of the measured values provides another essential parameter of the tag, the group delay τ_{gr}. It can be directly derived from the relation between the phase ϕ of the square-root ΔRCS ($\left[\sqrt{\Delta\boldsymbol{\sigma}}\right]$) and the angular frequency ω by

$$\tau_{gr} = -\frac{d\phi}{d\omega} \ . \tag{4.4}$$

Similar to Fig. 4.7, Fig. 4.9 shows τ_{gr} over frequency for different power levels in positive x-direction. The original phase information of the square-root ΔRCS over frequency for the two tags can be seen in Fig. 4.10.

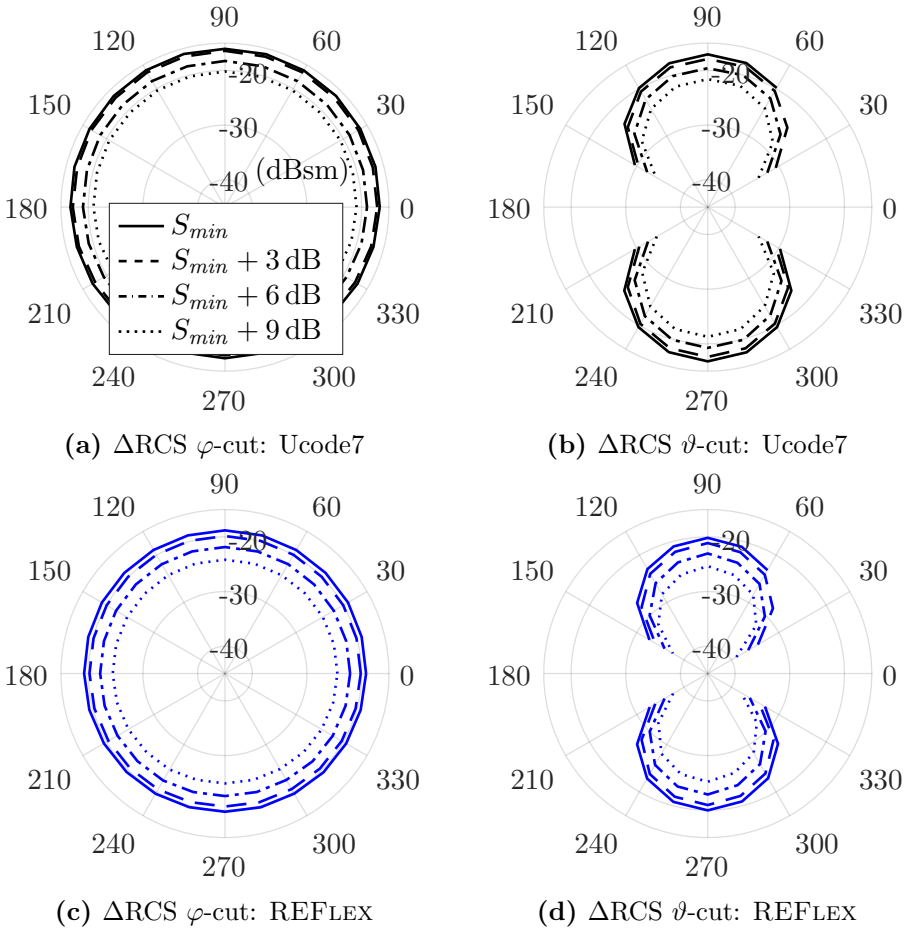


(a) Ucode7 on TEFLON.



(b) REFLEX in strong modulation mode.

Figure 4.7: ΔRCS over frequency for the two different tags and different levels of S.



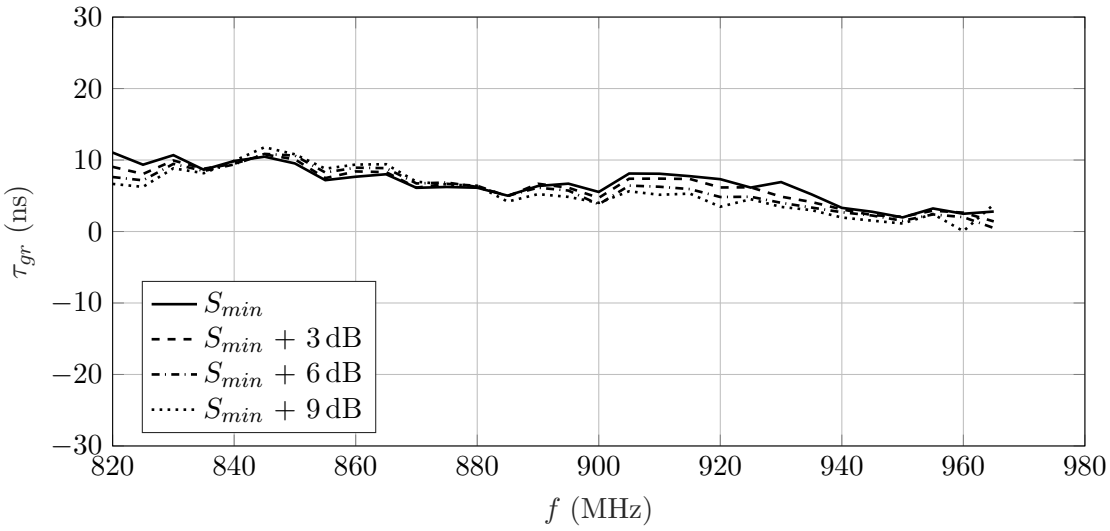
(a) ΔRCS φ-cut: Ucode7

(b) ΔRCS ϑ-cut: Ucode7

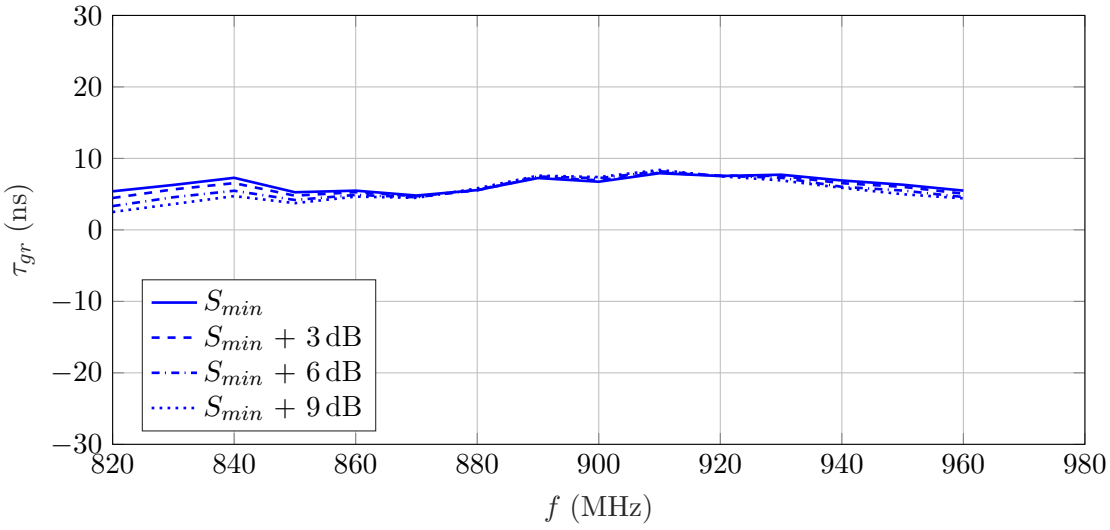
(c) ΔRCS φ-cut: REFLEX

(d) ΔRCS ϑ-cut: REFLEX

Figure 4.8: Cuts through the ΔRCS patterns of the NXP Ucode7 and the REFLEX tag at 870 MHz over φ and ϑ, respectively. The radial axes correspond to the ΔRCS in dBsm.

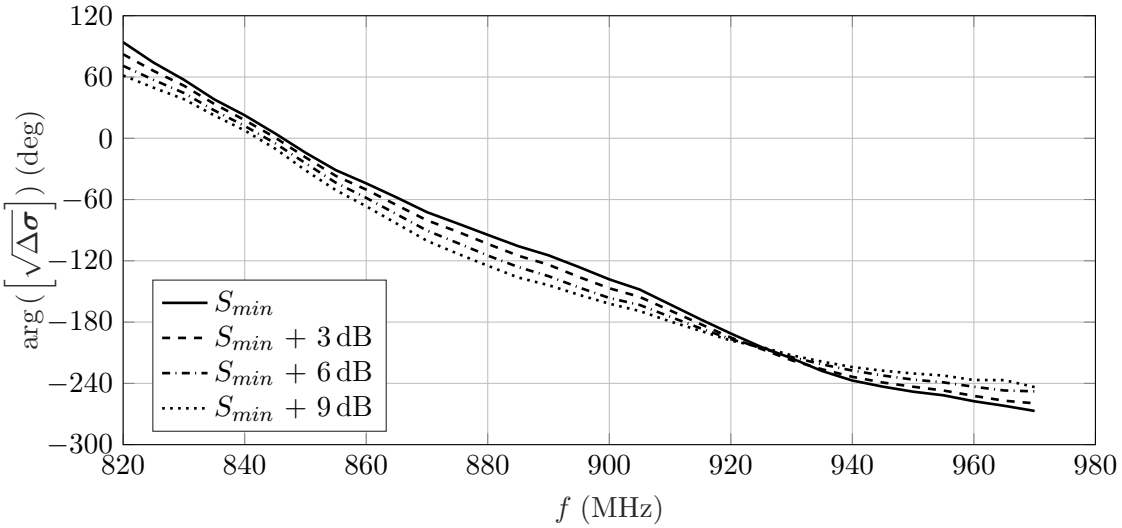


(a) Ucode7 on TEFLON.

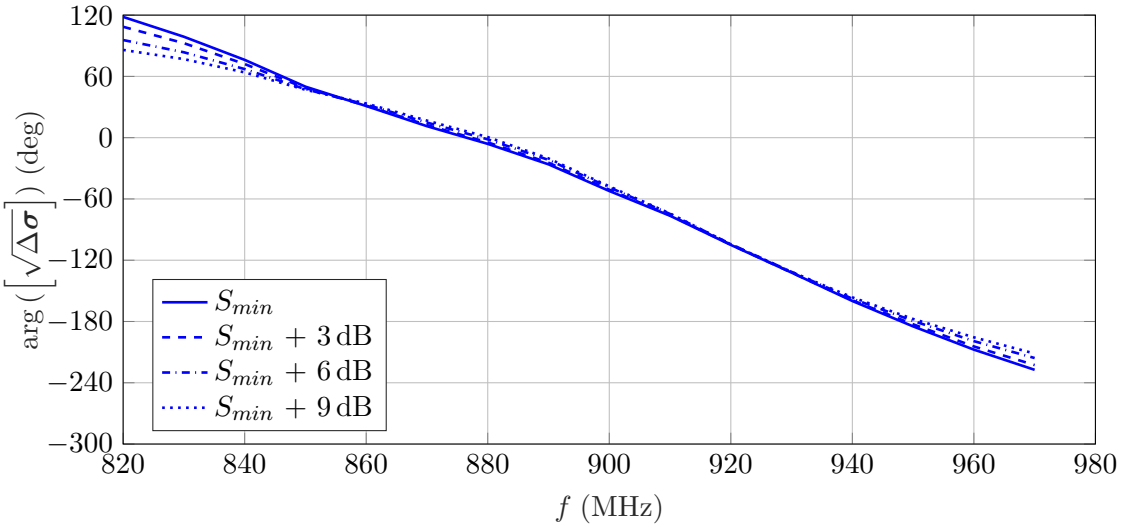


(b) REFLEX in strong modulation mode.

Figure 4.9: Group delay τ_{gr} over frequency for the two different tags and different levels of S.



(a) Ucode7 on TEFLON.



(b) REFLEX in strong modulation mode.

Figure 4.10: Phase of the square-root ΔRCS $\left[\sqrt{\Delta\boldsymbol{\sigma}}\right]$ over frequency for the two different tags and different levels of S.

4.3 DUTs at 2.45 GHz ISM Band

The main focus of the measurements in the ISM bands lies on the one hand on the REFLEX tag seen in Fig. 4.3b, which has already been examined in the UHF range. Although the high frequency interface is examined in this section, the tag is still powered via the UHF interface, as explained in section 2.3.
On the other hand, the modified electronic shelf label is considered. It is depicted in Fig. 4.11 together with the corresponding coordinate system and the position of its internal inverted-F antenna. It serves as an example for a device that uses the ISM 2.45 frequency band for its default application and that might be improved in the future by implementing the DSSS localization technique. Unlike the REFLEX tag it is not powered externally but uses an internal battery. The details of the modifications can be found in appendix B.

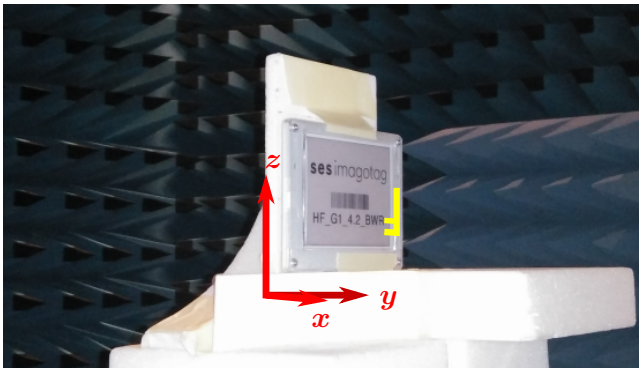


Figure 4.11: ESL as DUT mounted in the chamber. The position of the inverted-F antenna within the ESL is also indicated.

4.3.1 Power Dependency

In contrast to the EPC tags at UHF frequencies, it turns out that both tags do not show much of a non-linear behavior. Also, both tags are not supplied by the actual measurement signal at these frequencies around 2.45 GHz. Hence, there is no such parameter as S_{min} as defined for the tags presented in section 4.2. This can be seen in Fig. 4.12, where the ΔRCS in positive x-direction of the two tags is plotted against the surface power density at the position of the tag at the center frequency of the ISM 2.45 band.

4.3.2 Scalar ΔRCS

Without the reference value S_{min}, the ΔRCS of the tags has to be considered at fixed surface power density levels. Fig. 4.13 shows the full ISM frequency range for several different levels.
Similar to Fig. 4.8, Fig. 4.14 shows the ΔRCS patterns. The patterns of the ESL based tag are approximately omni-directional in the y-plane, however, the patterns are distorted. This is to be expected since the structure of the ESL has an influence on the pattern of the printed antenna.

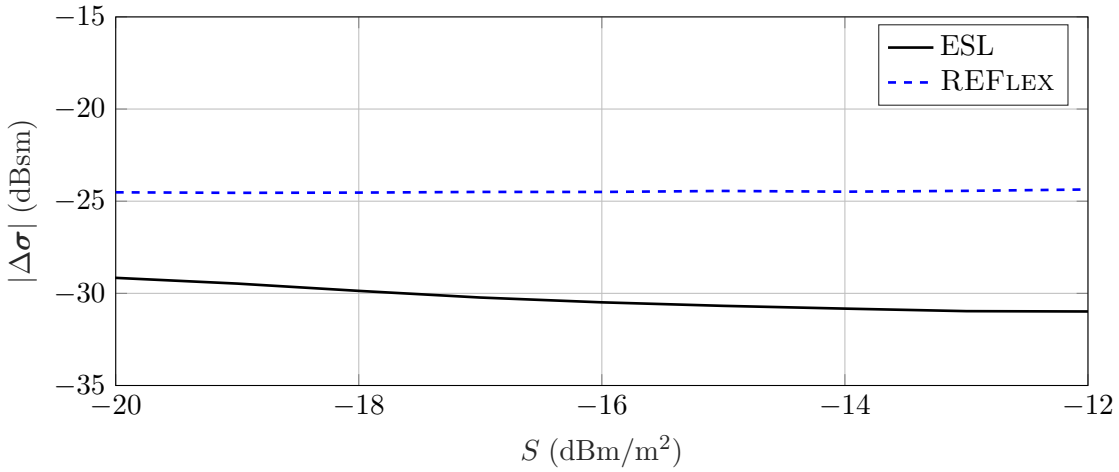
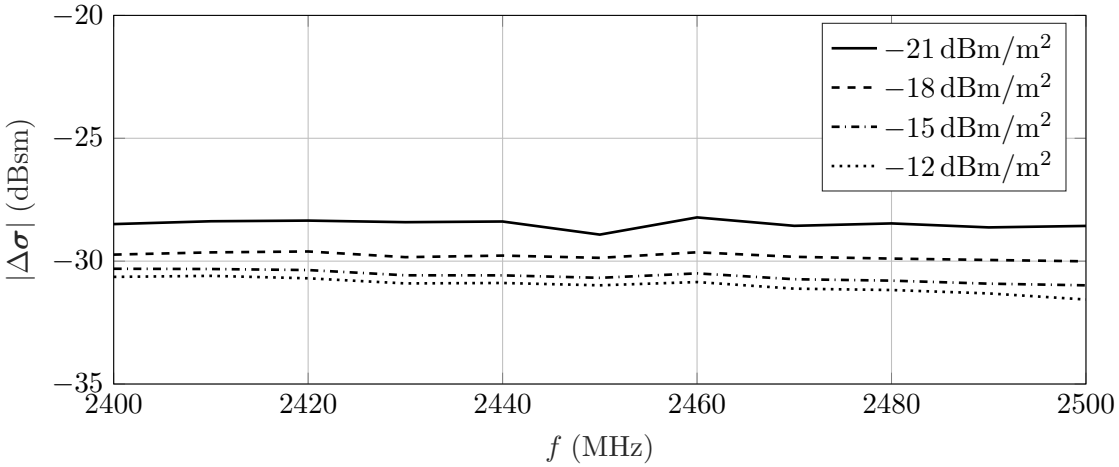


Figure 4.12: The REFLEX tag and the modified ESL exhibit an almost linear behavior at a frequency of 2.45 GHz.

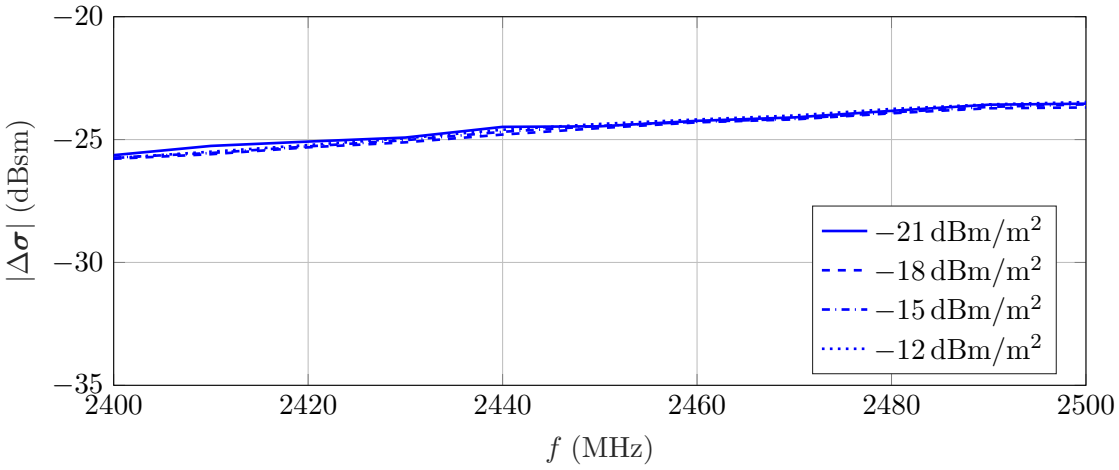
Apparently, also the pattern of the REFLEX tag exhibits a slight deviation from a dipole-like pattern. The difference to the UHF patterns shown in Fig. 4.8 is due to the different antenna used in this frequency band. However, although the antennas are of different shape, the outlines of the ΔRCS patterns are quite similar. Moreover, even though the pattern at a fixed frequency may vary over angle, the ΔRCS frequency responses for different angles of the incident wave almost only differ in a fixed offset as seen in Fig. 4.15.

4.3.3 Group Delay

Similar to section 4.2.3, the group delay of the tag and the phase of $\left[\sqrt{\Delta\boldsymbol{\sigma}}\right]$ are shown in Fig. 4.16 and Fig. 4.17, respectively.

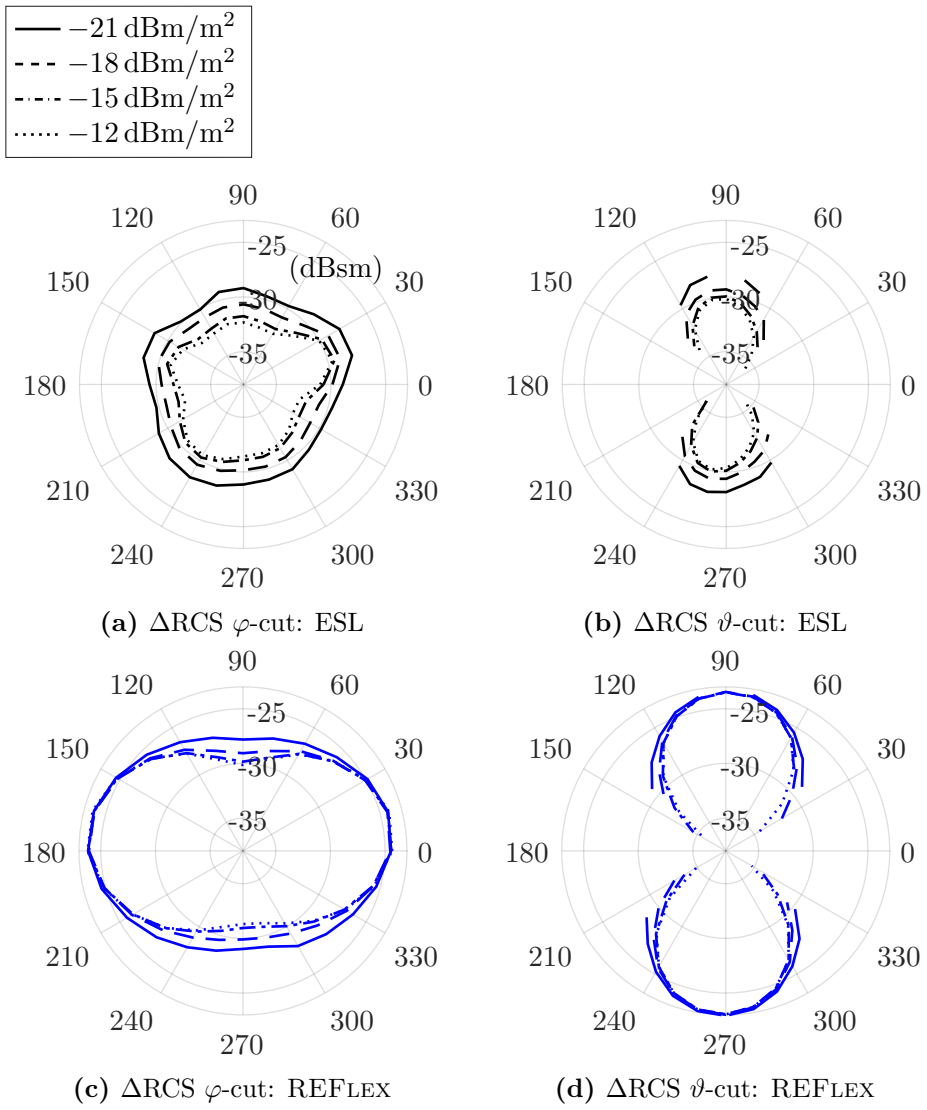


(a) Modified ESL.



(b) REFLEX high frequency interface in strong modulation mode.

Figure 4.13: ΔRCS over frequency for the two different tags and different levels of S in the ISM 2.45 frequency range.



(a) ΔRCS φ-cut: ESL

(b) ΔRCS ϑ-cut: ESL

(c) ΔRCS φ-cut: REFLEX

(d) ΔRCS ϑ-cut: REFLEX

Figure 4.14: Cuts through the ΔRCS patterns of the ESL based and the REFLEX tag at 2.45 GHz. Over φ and ϑ, respectively. The radial axes correspond to the ΔRCS in dBsm. Missing points are due to the weak SNR at low power levels.

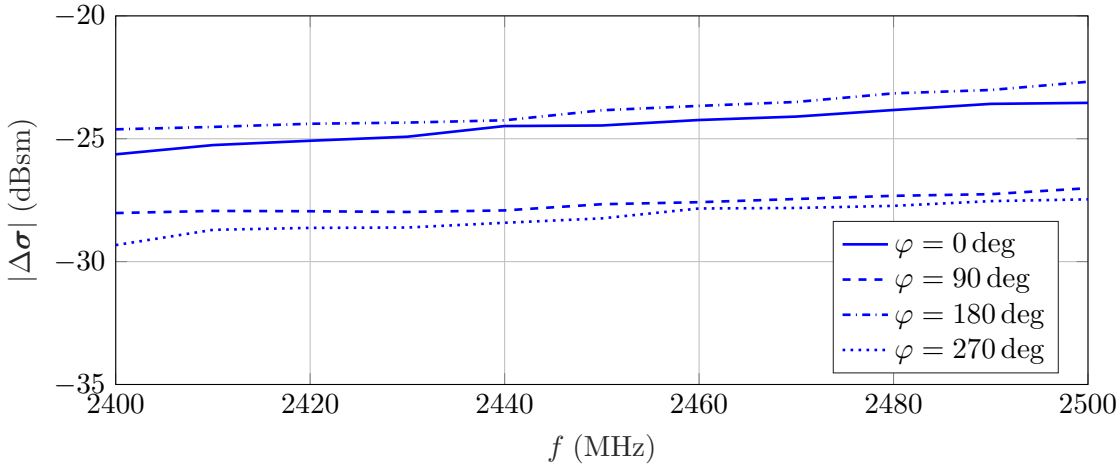
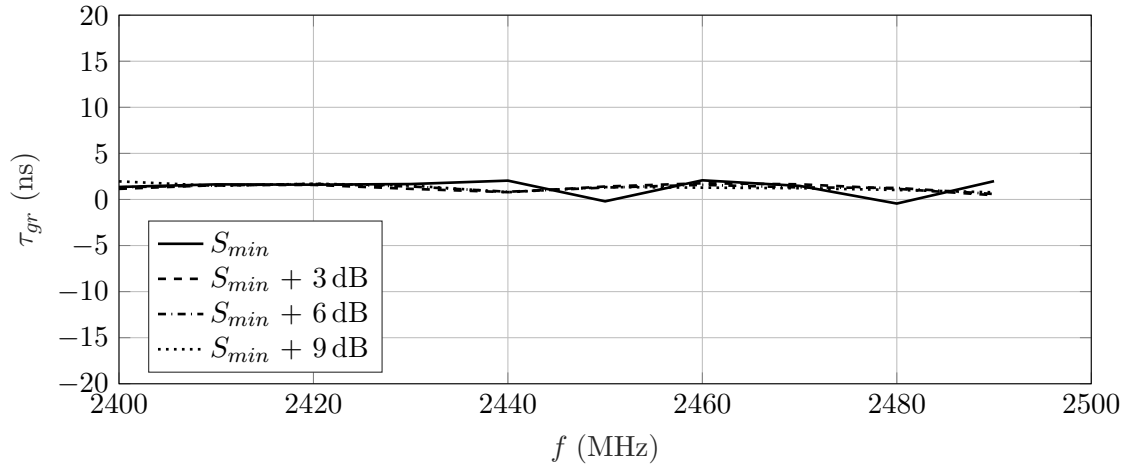
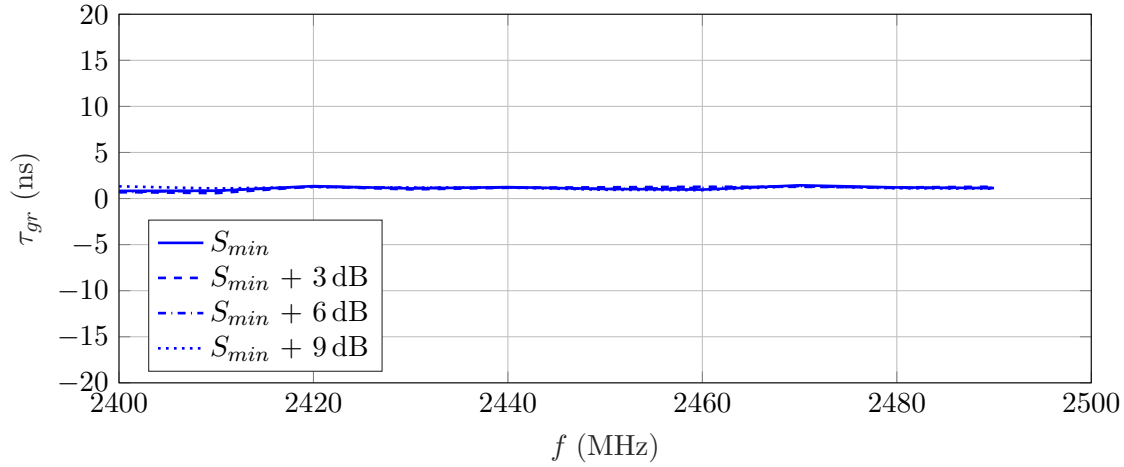


Figure 4.15: ISM band frequency behavior of the REFLEX tag ΔRCS for different φ values.

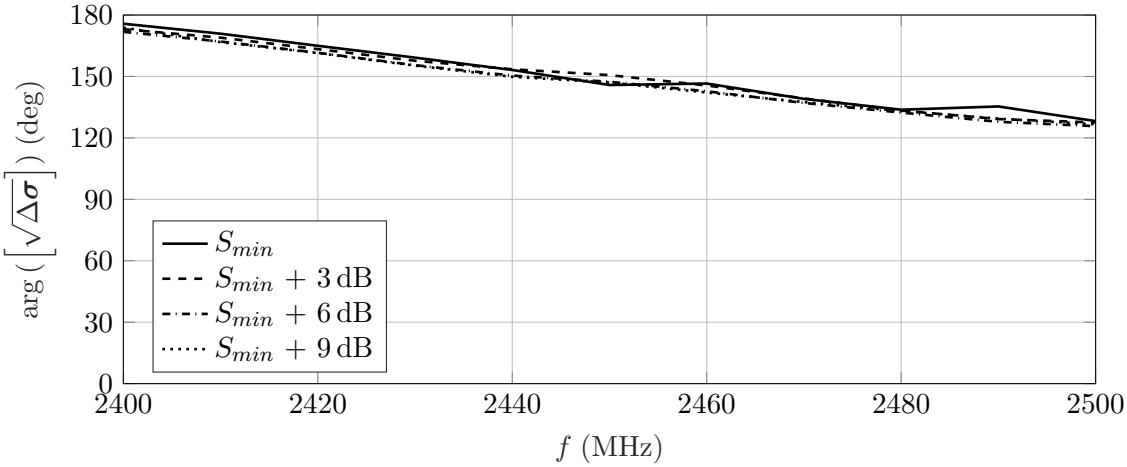


(a) ESL based tag.

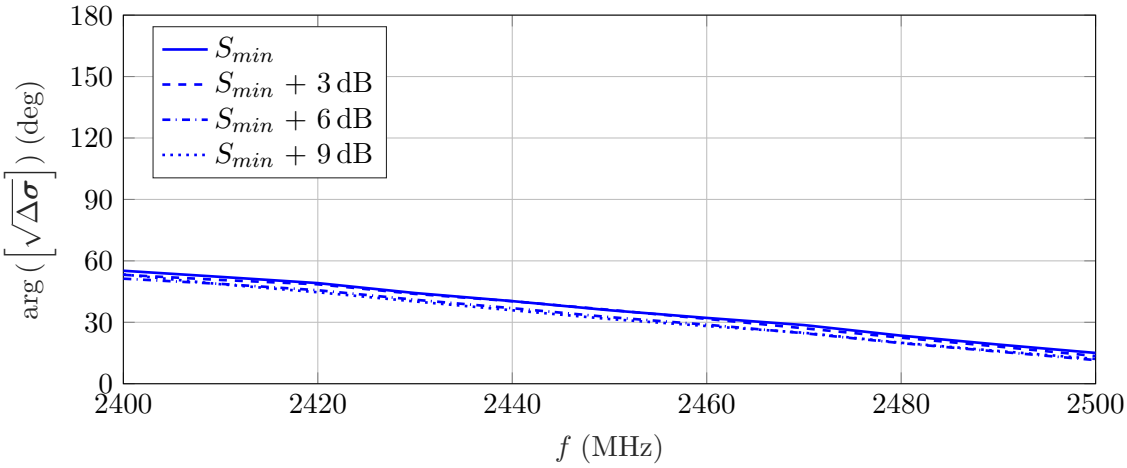


(b) REFLEX high frequency interface in strong modulation mode.

Figure 4.16: Group delay τ_{gr} over frequency for the two different tags and different levels of S. The weak SNR leads to noisy results for low power levels.



(a) ESL based tag.



(b) REFlex high frequency interface in strong modulation mode.

Figure 4.17: Phase of the square-root ΔRCS $\left[\sqrt{\Delta\sigma}\right]$ over frequency for the two different tags and different levels of S.

5 Noise Level Measurement

As explained in section 2.4, it is necessary to assess the noise situation of the environment in the frequency ranges of the ISM bands in order to allow for a statement, whether they may be usable for localization or not. Typical environments for the use of the DSSS localization technique in the context of the SES-IMAGOTAG ESL introduced in section 2.3, might be retail stores, especially consumer electronic markets. This is why such a market has been chosen for noise level measurements[1].

In this environment, spectrograms are recorded in the two ISM bands around 2.45 GHz and 5.8 GHz, respectively. To also get an impression how the noise situation evolves over the coarse of a working day, the measurements are repeated multiple times in the course of an afternoon of a regular working day. This is to be seen mainly in regards to the decreasing number of customers towards and after the shop closing time. The use of the public wireless LAN services available in the store are expected to be the main noise source.

5.1 Measurement Setup

The basic measurement setup used for this purpose is a simple broadband antenna with a frequency flat antenna gain and omni-directional pattern[2]. The obtained signal is sampled in time domain using a VSA[3]. From the sampled signals, the spectrum over time is calculated in the post-processing.
Since the VSA has an internal noise floor somewhat higher than the thermal one, the signal coming from the antenna has to be amplified while adding as little additional noise as possible, using an LNA[4]. In this way, the ambient noise floor can be captured down to the noise figure of this LNA.
In order to use one and the same LNA for both ISM bands, its bandwidth has to be sufficiently large. However, all this means that also signals outside the respective band of interest are captured by the antenna and amplified by the LNA. This might cause an overload and hence, non-linear behavior of the amplifier. To avoid this, bandpass filters fitted to the band which is measured are used for pre-selection of the signal after the

[1] MEDIAMARKT store in the vicinity of Graz, Austria.
[2] HUBER+SUHNER 1399.17.0224, Omni-S broad band WiFi antenna
[3] KEYSIGHT M9391A PXIe; the same as introduced in section 3.2.1.
[4] MINI-CIRCUITS ZX60-83LN-S+, LNA

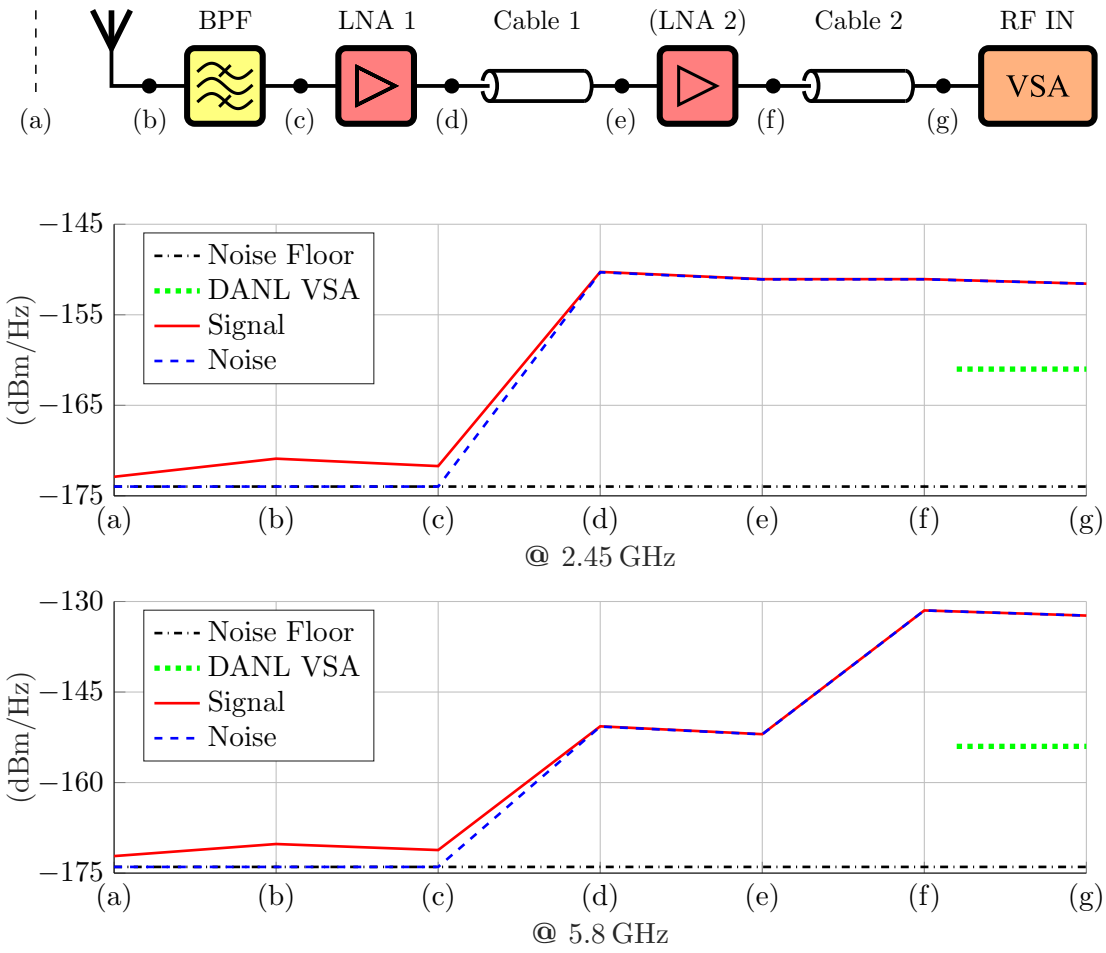


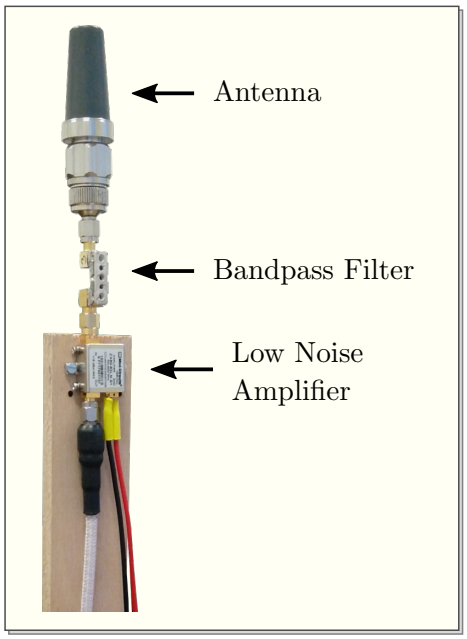
Figure 5.1: Evolvement of the thermal noise level and the minimum detectable signal strength through the measurement setup. LNA 2 is only used for the 5.8 GHz band.

antenna. Customized filters identical to the ones mentioned in section 3.2.2 are used for this purpose.

Fig. 5.1 shows the block diagram of the measurement setup. The amplifiers are necessary to raise the measured low level signals above the internal DANL of the measurement device. Naturally, due to the attenuation of the filter and the noise figure of the LNA, this means that the minimum detectable signal lies above the ambient thermal noise floor. Therefore, Fig. 5.1 also shows the behavior of the setup with regard to the evolvement of the spectral noise density[5] at the different nodes (a) to (g), as well as the spectral density of a signal that results in a SNR of 0 dB at the VSA. It comprises the gain of the used antenna, the insertion losses of the BPF and the cables, as well as the gain and the noise figure of the amplifiers. Using the thereby calculated overall gain, the measured results can be corrected in order to obtain the true power levels.

Fig. 5.2 shows the setup during the measurement. The antenna is mounted in a hight of about $h = 1.7\,\mathrm{m}$, as it is indicated in Fig. 5.2b. It has an approximate dipole-like pattern which is aligned in the horizontal plane in this setting.

[5] At room temperature $T_0 = 290\,\mathrm{K}$.



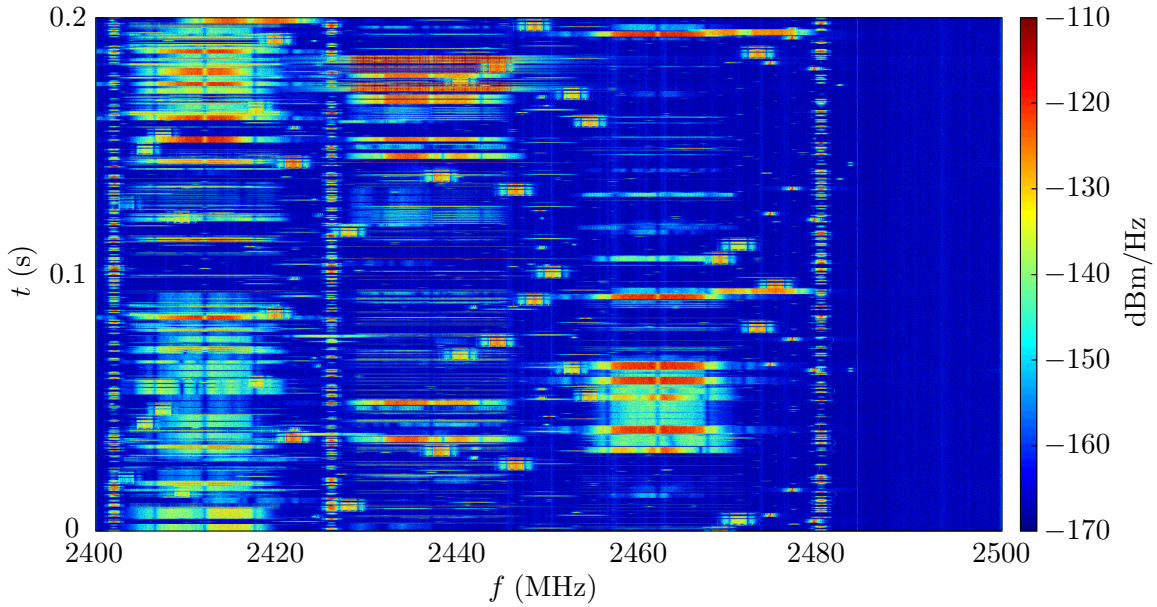
(a) Closeup of the measurement setup front-end.

(b) Full measurement setup assembled in a consumer electronic market.

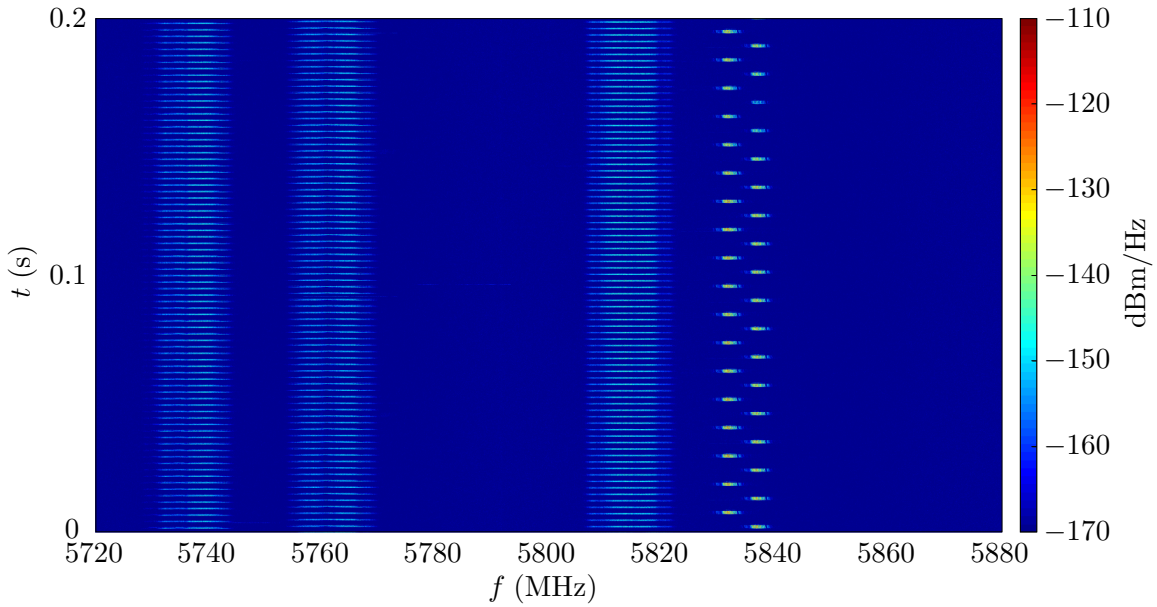
Figure 5.2: Noise level measurement setup.

5.2 Results

Fig. 5.3 shows a representative section of the resulting spectrogram in the two measured bands. While the ISM band around 2.45 GHz is densely crowded with services like wireless LAN or BLUETOOTH®, the ISM band around 5.8 GHz is not much used in this scenario. Introducing a usage threshold of −160 dBm/Hz allows to separate the power spectral density over the time-frequency plane into occupied and free parts. In this way it is possible to evaluate the measured data for percent of occupied time over frequency. As it can be seen in Fig. 5.4, the ISM band around 2.45 GHz is highly occupied especially in the frequency ranges of the typical wireless LAN channels.
Several measurements over periods of ten minutes each at different times of the day reveal a rather steady use of these two bands. Only a slight reduction of traffic in the ISM band around 2.45 GHz is experienced after shop closing time.

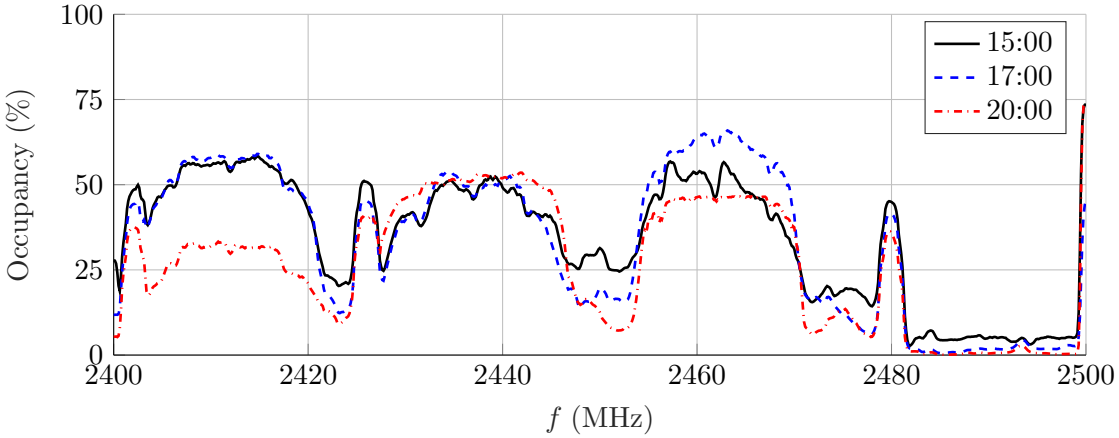


(a) Spectrogram of the 2.45 GHz ISM band. Due to wireless LAN, BLUETOOTH® and other traffic, this band is relatively crowded.

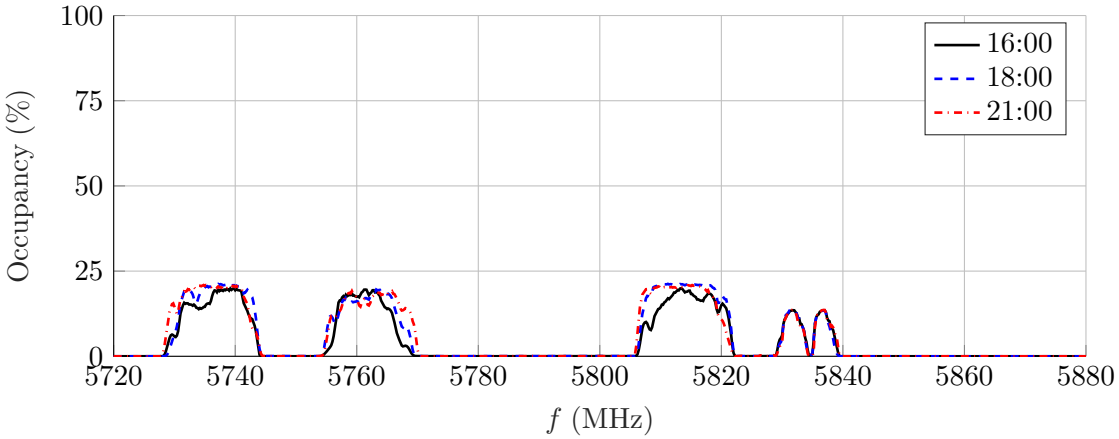


(b) Spectrogram of the 5.8 GHz ISM band. Compared to Fig. 5.3a, it is almost empty.

Figure 5.3: Spectrograms of the two ISM bands over a period of 200 ms.



(a) The 2.45 GHz ISM band shows a relatively high occupancy.



(b) The 5.8 GHz ISM band has large regions with almost zero occupancy.

Figure 5.4: Percent of time when the threshold power spectral density of −160 dBm/Hz is exceeded. The measurements are taken at different times of the day over a period of 10 min, each.

6 Implications for Localization Accuracy

This chapter gives some concluding considerations regarding the relevance and meaning of the results obtained in this work on the DSSS based localization technique.

6.1 ΔRCS of Tags

UHF Band Tags

As it has been shown in section 4.2.1, the tags in the UHF range, which are also powered by the interrogating continuous wave signal, are not operating in a linear range. This is problematic in the context of DSSS localization. Since the signal used to obtain this results is narrow-band, it remains unclear, whether the ΔRCS measured in this way at a certain frequency is also valid in the case of a small signal at this frequency in the presence of second, stronger signal at another frequency. However, this is the relevant information for DSSS ranging, where a wide-band small signal is superimposed on a strong carrier signal.
From this it follows that the obtained results for EPC compliant tags in the UHF range are most likely not usable to improve the localization accuracy of this technique. This severity of the non-linearity was not expected previously and could be shown using the built measurement setup.
As the measurement results in UHF range turned out to be not sufficient to allow a direct usage for DSSS localization, an extension of the measurement setup could be contemplated. It may comprise a ΔRCS measurement using low level signals while supplying the tag with a stronger signal at a UHF frequency different from the measurement frequency. This would resemble the actual situation of the DSSS localization in a better way. From this, better statements regarding the implications of the ΔRCS of tags on the localization may be expected.

ISM Band Tags

In contrast to the tags in the UHF range, the tags have a linear behavior over power in the ISM frequency range. This means that the ΔRCS is the same for small and large scale signals. As shown in section 4.3, the frequency response of the tags is almost flat, which means that a baseband impulse response similar to a Dirac delta function is expected.

Further, it could also be shown that the frequency responses of the REFLEX tag for different angles of the incident wave only differ in an offset that is constant over frequency. This is especially interesting in the context of the discussed DSSS based localization technique. However, a dependence on the power of the supplying UHF carrier signal of these tags has not been investigated so far. This might also be subject to further work on this topic.

6.2 Noise Level

The results presented in section 5.2 show, that the use of the ISM 2.45 band for additional services like localization techniques based on broadband sequences comes with severe interferences. Since the ISM 5.8 band appears still far less populated with services at the time of the measurements, an extension in this direction may be beneficial. Of course, the situation is likely to get worse in the future, as many services based on the use of the open ISM bands suffer from the limitations of the highly popular band around 2.45 GHz and future developments are likely to go into higher frequency bands, too.

7 Conclusion & Outlook

Within this thesis the ΔRCS of RFID tags was in the main focus. A measurement setup was developed and successfully realized that is capable of determining this complex-valued parameter in three frequency bands as well as for different power levels and incident spatial angles on the tags. These requirements have not been met to this extent so far by any commercially available solution.
The major challenges were the inevitable phase noise sensitivity of such a backscatter modulation based system as well as the spurious reflections of the continuous wave source signal. The latter are mainly due to not perfectly matched components such as the cables leading into the anechoic chamber and the probe antenna.
In order to overcome this obstacles, the carrier signal used to determine the ΔRCS was derived from the internal source of the used signal analyzer. A carrier cancellation was implemented to reduce the unwanted reflections and make better use of the admissible input range of the analyzer. All this is to be seen with regard to the achieved flexibility of the setup, since the carrier cancellation can be dynamically adapted to any given frequency and power level as well as changing reflections coming from the anechoic chamber.
The measurement results show a non-linear behavior of passive EPC compliant tags in the UHF range. The ΔRCS also varies over frequency. Tags backscattering in the ISM 2.45 frequency band, which are not supplied via the measurement carrier, behave linearly over the applied power level as well as the investigated frequency range. In spatial domain, the results reflect the tag antenna patterns, as it is to be expected.
In addition to the ΔRCS measurements, the interference situation in a typical electronics retail shop was analyzed. In view of the localization applications based on DSSS backscatter systems in ISM bands, the measurements reveal a quite densely used ISM band around 2.45 GHz, while the ISM band around 5.8 GHz is still mostly unused.
Although the system provides the desired results, improvement is always possible. A major drawback is the rather long duration of several hours of one measurement cycle. A speedup might be achieved by improving the carrier cancellation. It is the most time consuming step of the measurement procedure besides the movement of the axes inside the anechoic chamber, which cannot be reduced easily. It turned out that the bottleneck is the data transfer between the VSA and the controlling PC based on SCPI commands.
For relatively low values of ΔRCS, the SNR limits the measurable range. As already indicated in section 3.5.2, much can be done by applying a suitable averaging of the tag response. Up to this point, this has been implemented in a very intuitive, straight forward clustering of the measured traces and could be improved using an actual decoding of the tag answer.

A Modifications of the Anechoic Chamber

It should be said first, that the anechoic chamber used in this work must be seen as a highly sensitive piece of equipment. It is good practice to never trust any single part of it and to check their individual behavior time and again. This is especially true for the rotary joints, the *theta*-stage as a whole, any connection that may be opened, and any cable that may be moved. Furthermore, it is advisable to re-measure known DUTs on a regular basis as a cross-check.
Many hours had to be spent in vain to reach this level of caution and the author would be delighted if these lines could contribute to spare someone some time in the future.

This chapter is meant to be a short introduction to the modifications made to the anechoic chamber to improve its behavior in terms of ground reflections. It should also be understood as a guidance to assemble the necessary additional equipment. A.2 gives a step by step tutorial.

A.1 Additional Absorbers

Previous measurements in the anechoic chamber have shown unexpected magnitude ripples in frequency as well as in spatial domain when characterizing patterns of antennas. The periodicity of these ripples suggests that this phenomenon stems from multipath propagation with an additional non-line of sight path over the exposed metallic components in the *phi*-stage as seen in Fig. A.1.
As expected from this assumption, the phenomenon tends to disappear in the case of highly directive antennas mounted in a way that their principle beam is pointing in positive z-direction (upwards). However, this also means that when characterizing omni-directional antennas like dipoles mounted in a way that a significant part of energy is radiated towards the ground, the results are questionable. Obviously, these observations suggest, that additional absorbers covering the metallic parts on the base of the chamber may improve this situation. Therefore, a platform with a circular cutout for the rotary *phi*-stage to carry pyramids of radiation-absorbent material was constructed.To take care of the remaining metallic rotary part, a circularly shaped absorber with feed throughs for the cable connecting the antenna under test (AUT) as well as for screws and threaded rods for mounting

purposes was added. Using spacers to avoid direct pressure on the absorbing material, a tower of ROHACELL® is placed on top of it to reach the center of the chamber.
In order to limit the range of the *theta*-arm and thereby keeping it from hitting the newly installed absorbers on the ground, additional end stops are necessary. They are realized using light barriers mounted close to the center of rotation of the *theta*-arm. A dial gauge[1] is used to achieve accurate centric positioning of the mounting plate for the end stop indicators. The end stop sensors can be seen in Fig. A.2.

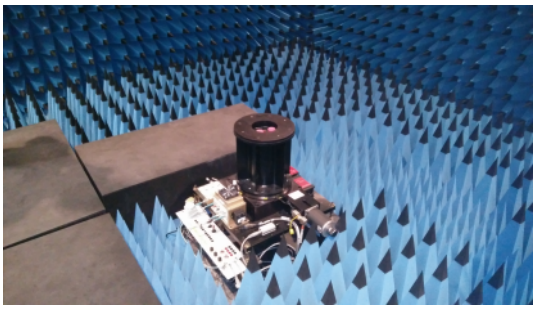


Figure A.1: The uncovered *phi*-stage, causing multipath effects.

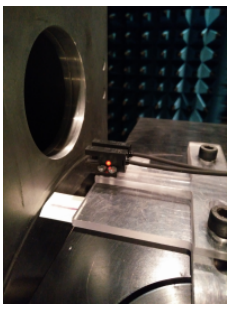


Figure A.2: The new end stop sensors while being active.

A.2 Installation Tutorial

WARNING: Do not place the absorber table without having plugged in the additional end stops!

Initialization of the *theta*-Arm

1. Make sure that the new end stops are plugged in. (Fig. A.3)
2. Initialize the *theta*-stage (or all axes) in the NSI software or the DOS interface. The new end stops are set in a way that the *theta*-arm will go to exactly 20.0 deg after the this step.
3. Manually move the *theta*-arm to −20 deg using the appropriate software command. The *theta*-arm will now actually be exactly at 0 deg, i.e. at the intended new zero position.
4. Use the command 'set position' to tell the software that this is the new zero position.

Installation of the Additional Absorbers

1. Remove the *phi*-pillar. (Fig. A.1)
2. Add the absorber table. The correct orientation is marked on the table as "**X→**" and "**Y→**", corresponding to the coordinate system of the chamber. **The orientation is not arbitrary.** In the correction orientation, the feet exactly fit onto the four studs at the corners of the *phi*-stage. (Fig. A.4)

[1] German: *Messuhr*

Figure A.3: The end stop sensor connection in unplugged and plugged state.

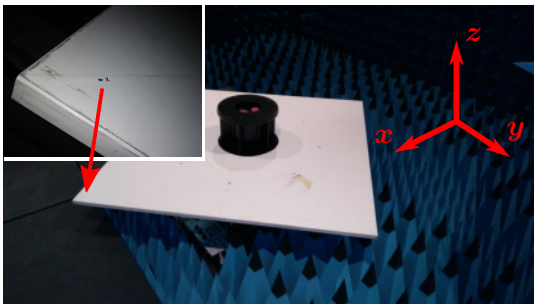


Figure A.4: The absorber table mounted on the *phi*-stage and close-up of the positive x-corner. Labels at the corners of the table indicate the positive x and y-direction in accordance with the coordinate system of the chamber.

3. Add the cylindrical *phi*-pillar ground absorber **including the supporting spacers** for the structure to be added on top later. The spacers are crucial, since the absorber is highly sensitive to pressure.
   If necessary, the hole in the center can be used to feed through a cable connecting the DUT. (Fig. A.5)

4. Add spacers to keep space for a possible auxiliary antenna. This might be necessary for RFID tags as DUTs. (Fig. A.6)

5. Add the ROHACELL® pillar to reach the nominal height of 1.37 m. (Fig. A.7)

6. Add the absorbers onto the absorber table. (Fig. A.8)

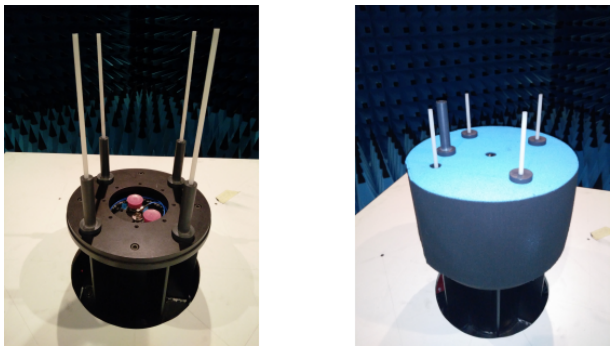


Figure A.5: The cylindrical absorber covering the rotating part of the *phi*-stage. **Do not forget the spacers** – the absorber is sensitive to pressure!

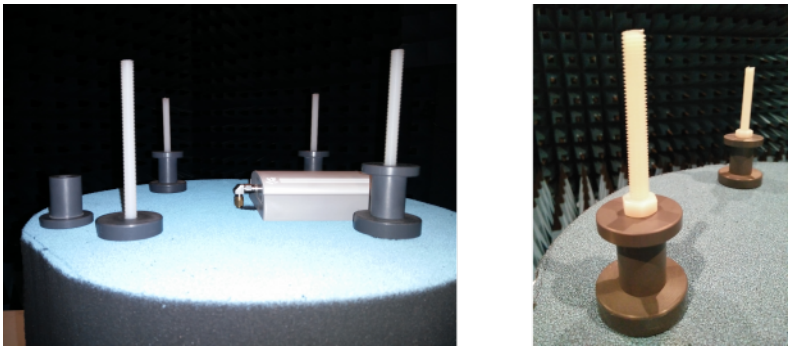


Figure A.6: Spacers that can be used to place an auxiliary antenna.

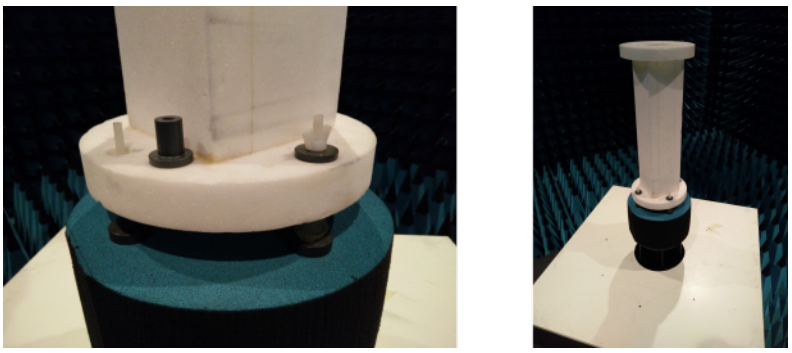


Figure A.7: ROHACELL® pillar placed hold in place by additional spacers and plastic wing nuts.

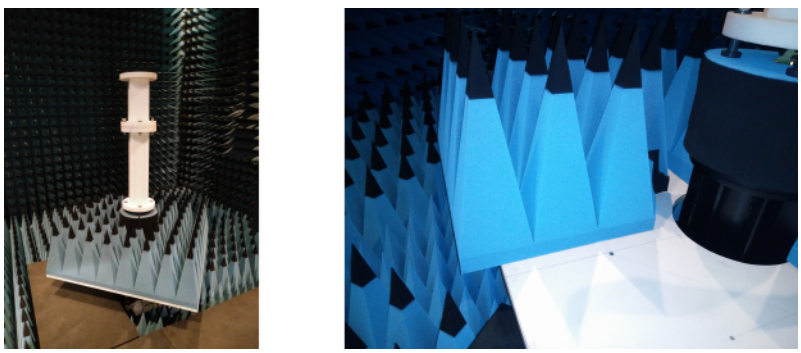


Figure A.8: The four clipped quadratic absorbers allow the pillar to rotate freely.

B Active Backscatter Modulation Circuit

This chapter refers to the modified ESL as introduced in section 2.3. The according ΔRCS measurement results can be found in section 4.3.

The circuit is necessary to modulate the impedance connected to the original inverted-F antenna used for the default communication of the ESL. Fig. B.1 shows the according schematic as well as a photograph of the circuit. The respective parameters are listed in table B.2.
The circuit is based on a PIN diode which is continuously switched between conducting and off-state. As a result, the impedance connected to the antenna changes between approximate open and short. An inductor is used to block RF signals, a blocking capacitor is necessary to avoid a DC short circuit over the printed inverted-F antenna on the printed circuit board (PCB). An oscillator provides a frequency f_0 similar to the BLF of regular RFID tags. To provide the required current, a logic gate is used as a driver.
The original circuitry is disconnected from the antenna and all unnecessary parts are removed from the PCB. The necessary RF components are placed close to the antenna instead of the original components. While only the antenna and the battery connector of the original board are used, all other components used for the modulation are placed on an additional board, connected to the original one by enameled copper wire. The used components are listed in table B.1.
The two boards are fitted into the original housing seen in Fig. 2.6.

Battery	Panasonic	CR2450-3P (3x100 mAh)
Voltage Regulator	Texas Instruments	TPS75225Q
Oscillator	Micro Crystal	OV-7604-C7
Driver	Fairchild	NC7SZ32 (OR Gate)
Diode	Philips	BAP70-02

Table B.1: Parameters of the backscatter modulation circuit.

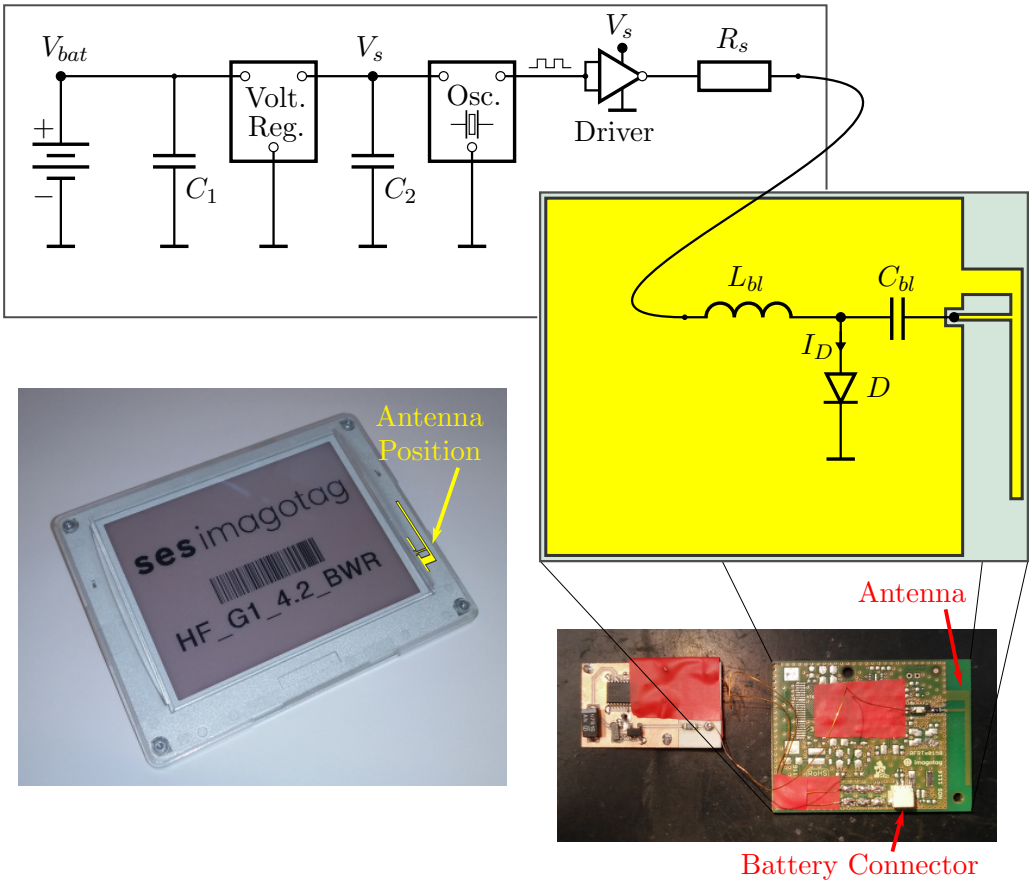


Figure B.1: Schematic and picture of the active backscatter modulation circuit. The battery is also connected via the original PCB. The position of the antenna within the ESL is also indicated.

Battery Voltage	V_{bat}	$= 3\,\mathrm{V}$
Supply Voltage	V_s	$= 2.5\,\mathrm{V}$
Nominal Frequency	f_0	$= 32.768\,\mathrm{kHz}$
RF block	L_{bl}	$= 5800\,\mathrm{nH}$
DC block	C_{bl}	$= 6.8\,\mathrm{nF}$
Series Resistor	R_s	$= 22\,\Omega$
max. forward Current	$I_{D,max}$	$= 43\,\mathrm{mA}$
min. forward Resistance	$r_{D,min}$	$= 2\,\Omega$
Reverse Capacitance	C_D	$= 500\,\mathrm{fF}$

Table B.2: Parameters of the backscatter modulation circuit. C_1 and C_2 are chosen according to the voltage regulator datasheet.

References

[1] Adrian Lobe. Der verchippte Mitarbeiter `http://derstandard.at/2000061803314/Der-verchippte-Mitarbeiter-laengst-kein-Einzelfall-mehr`, July 2017. 1

[2] GS EPCglobal. EPC radio-frequency identity protocols generation-2 UHF RFID; specification for RFID air interface protocol for communications at 860 MHz – 960 MHz. *EPCglobal Inc., November*, 2013. 1, 3, 14, 15

[3] EN ETSI. 302 208-1 Version 1.4. 1, 2015. 1

[4] Holger Arthaber, Thomas Faseth, and Florian Galler. Spread-spectrum based ranging of passive UHF EPC RFID tags. *IEEE Communications Letters*, 19(10):1734–1737, 2015. 2, 5

[5] Florian Galler, Thomas Faseth, and Holger Arthaber. SDR based EPC UHF RFID reader DS-SS localization testbed. In *Wireless and Microwave Technology Conference (WAMICON), 2015 IEEE 16th Annual*, pages 1–4. IEEE, 2015. 2

[6] Alessandra Costanzo, Diego Masotti, Thomas Ussmueller, and Robert Weigel. Tag, you're it: Ranging and finding via RFID technology. *IEEE Microwave Magazine*, 14(5):36–46, 2013. 3

[7] Merrill I. Skolnik. *Introduction to Radar Systems*. McGraw-Hill, 1980. 7

[8] Warren L. Stutzman and Gary A. Thiele. *Antenna Theory and Design*. John Wiley & Sons, 2012. 9

[9] Sebastian Riegger and Werner Wiesbeck. Wide-band polarimetry and complex radar cross section signatures. *Proceedings of the IEEE*, 77(5):649–658, 1989. 9

[10] Pavel V. Nikitin, K. V. S. Rao, and R. D. Martinez. Differential RCS of RFID tag. *Electronics Letters*, 43(8):431–432, 2007. 12

[11] ISO/IEC 18047-6. *Radio frequency identification device conformance test methods – Part 6: Test methods for air interface communications at 860 MHz to 960 MHz*. 2017. 14

[12] REFlex. REFlex - RFID Real-Time Localization for Flexible Production Environments. `https://iktderzukunft.at/de/projekte/reflex.php`. 15

[13] ITU. Radio Regulations, Articles. `http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/1.43.48.en.101.pdf`, 2016. 17

[14] Gregory F. Masters and Stuart F. Gregson. Coordinate system plotting for antenna measurements. In *AMTA Annual Meeting & Symposium*, 2007. 32

[15] Andrea Ferrero and Umberto Pisani. Two-port network analyzer calibration using an unknown 'thru'. *IEEE Microwave and Guided Wave Letters*, 2(12):505–507, 1992. 33

[16] Alien Newell, R. Baird, and P. Wacker. Accurate measurement of antenna gain and polarization at reduced distances by an extrapolation technique. *IEEE Transactions on Antennas and Propagation*, 21(4):418–431, 1973. 33

[17] Sanming Hu, Honghui Chen, Choi Look Law, Zhongxiang Shen, Lei Zhu, Wenxun Zhang, and Wenbin Dou. Backscattering cross section of ultrawideband antennas. *IEEE Antennas and Wireless Propagation Letters*, 6:70–73, 2007. 41

[18] Stuart Lloyd. Least squares quantization in PCM. *IEEE transactions on information theory*, 28(2):129–137, 1982. 49

[19] George T Ruck. *Radar cross section handbook*. Plenum Publishing Corporation, 1970. 50, 51

Hiermit erkläre ich, dass die vorliegende Arbeit gemäß dem Code of Conduct – Regeln zur Sicherung guter wissenschaftlicher Praxis (in der aktuellen Fassung des jeweiligen Mitteilungsblattes der TU Wien), insbesondere ohne unzulässige Hilfe Dritter und ohne Benutzung anderer als der angegebenen Hilfsmittel, angefertigt wurde. Die aus anderen Quellen direkt oder indirekt übernommenen Daten und Konzepte sind unter Angabe der Quelle gekennzeichnet.
Die Arbeit wurde bisher weder im In– noch im Ausland in gleicher oder in ähnlicher Form in anderen Prüfungsverfahren vorgelegt.

Wien, 17. Jänner 2018 *Daniel Neunteufel*