TECHNISCHE UNIVERSITÄT WIEN

Dissertation

Localization of Passive UHF RFID Tags

ausgeführt zum Zwecke der Erlangung des akademischen Grades
eines Doktors der technischen Wissenschaften

unter der Leitung von

Assoc. Prof. Dipl.-Ing. Dr. techn. Holger Arthaber

Institute of Electrodymamics, Microwave and Circuit Engineering

eingereicht an der Technischen Universität Wien
Fakultät für Elektrotechnik und Informationstechnik

von

Dipl.-Ing. Florian Galler, BSc.
Matr.Nr. 0826275
Carl-Appel-Straße 5/1108
1100 Wien

Wien, im Juli 2019

Abstract

Identification of items is one of the key ingredients for automation of work flows and logistics. Ultra high frequency (UHF) radio frequency identification (RFID) systems are a commonly used solution for contactless identification with read ranges of about 10 m. While identification is sufficient for a lot of use-cases, several applications require localization of the tag as well, e.g. sequence detection on conveyor belts or range gating.

This thesis focuses on a broadband ranging method which can be applied to backscatter based RFID systems. As no changes to the tags are required, this localization method can potentially be applied to billions of already deployed commercial-off-the-shelf (COTS) electronic product code (EPC) UHF RFID tags.

A ranging enabled RFID reader testbed, based on a COTS software defined radio (SDR), will be presented. To utilize the full available performance of the SDR, a custom field programmable gate array (FPGA) implementation was developed. The developed ranging testbed was used to conduct measurements in an empty office environment. These measurements showed that multipath propagation is a limiting factor for the application of the broadband ranging method in typical indoor environments.

The influence of the non-ideal delta radar cross section (ΔRCS) of RFID tags onto the ranging method is discussed. Therefore, a systematically approach to derive the ΔRCS from the knowledge of the complex valued gain pattern and the impedance of the RFID chip is presented. By utilization of various simulations, critical environmental factors were identified. The results show that the additional group delay of the resonant RFID antennas has to be considered if precise ranging measurements are required.

A dual frequency tag was developed and built in a close cooperation with *NXP Semiconductor N.V.* to further enhance the ranging performance. With this tag it is possible to separate the identification from the ranging process in frequency domain. Thus, each part can be optimized separately. The sensitivity of the group delay on the dielectric properties of the material surrounding the tag was significantly reduced by using a broadband design.

Kurzfassung

In der automatisierten Industrie und Logistik ist die Identifizierung von Gegenständen ein wichtiger Aspekt. Electronic Product Code Ultra-High Frequency Radio Frequency Identification (EPC UHF RFID) Systeme werden vermehrt für die berührungslose Identifikation eingesetzt. Für eine Vielzahl von Anwendungsfällen ist die Identifizierung ausreichend, jedoch würden einige Anwendungen zusätzlich auch eine Positionsinformation benötigen. Man denke hier zum Beispiel an die Erkennung der Reihenfolge von Gütern auf einem Förderband oder an die Begrenzung von Lesezonen.

Diese Arbeit beschäftigt sich mit dem Thema der Anwendbarkeit eines breitbandigen Entfernungsmessverfahren auf kommerziell erhältliche EPC Standard konforme RFID Tags, welche schon milliardenfach im Einsatz sind.

Ein RFID Lesegerät wurde entwickelt, welches neben der standardkonformen EPC Kommunikation zusätzlich ein breitbandiges Lokalisierungsverfahren unterstützt. Dieser Prototyp wurde auf Basis eines kommerziell erhältlichen Software Defined Radio (SDR) entwickelt. Eine Field Programmable Gate Array Entwicklung wurde durchgeführt, um die Hardware des SDRs optimal zu nutzen. Die Anwendbarkeit des breitbandigen Entfernungsmessverfahrens wurde anschließend in einem Büroraum untersucht. Die Messungen zeigten, dass die Mehrwegeausbreitung einer der limitierenden Faktoren in Innenraumszenarien ist.

Weiters wurde der Einfluss eines nichtidealen Delta Radarquerschnittes des RFID Tags auf die Genauigkeit der Distanzmessung untersucht. Dazu wurde ein Ansatz entwickelt, der ausgehend von einer Antennengewinn Simulation und der Impedanz des RFID Chips die Berechnung des Delta Radarquerschnitt ermöglicht. Unter Zuhilfenahme dieser Methode wurden verschiedene Vergleichssimulationen durchgeführt. Besonders hervorzuheben ist die Änderung der Gruppenlaufzeit wenn die dielektrischen Eigenschaften des Materials geändert werden auf welchem der Tag aufgebracht ist. Die Änderung der Gruppenlaufzeit beeinflusst die Genauigkeit des Entfernungsmessverfahren und sollte daher kompensiert werden.

Außerdem wurde ein Zweifrequenz Tag in Kooperation mit *NXP Semiconductor N.V.* entwickelt. Durch die Verwendung von zwei unterschiedlichen Frequenzbändern für Lokalisierung und Identifikation, kann jeder Teil separat optimiert werden und so zum Beispiel die Sensitivität der Gruppenlaufzeit des Tags auf Änderungen des umgebenden Materials verringert werden.

Acknowledgements

For the past nearly five years, I spent much of my time at the university in a very thriving environment. I would like to thank my colleges in the microwave group for sharing their ideas, knowledge and time in numerous discussions and social events. I would like to express my appreciation to Dr. Holger Arthaber for the supervision of my thesis and for his encouragement.

I also want to express my gratitude to all colleges I worked with during the project Real-time localization for flexible production environments (REFlex). The funding of this project by the Austrian Research Promotion Agency (FFG) is gratefully acknowledged (project number: 845630).

Special thanks go to Cornelia for insisting on activities outside of the academic environment and for proofreading this thesis.

Finally, I want to thank my parents, relatives, and friends for supporting me, especially my mother, who had always fostered my technical interests and thus provided the basis for my studies.

Contents

List of Acronyms

ADC	Analog-to-digital Converter
AoA	Angle of Arrival
ARP	Address Resolution Protocol
AWGN	Additive White Gaussian Noise
BLF	Backlink Frequency
CORDIC	Coordinate Rotation Digital Computer
COTS	Commercial-off-the-shelf
CW	Continuous Wave
DAC	Digital-to-analog Converter
DM	Dense Multipath
ΔRCS	Delta Radar Cross Section
EIRP	Equivalent Isotropic Radiated Power
EM	Electromagnetic
EPC	Electronic Product Code
ERP	Equivalent Radiated Power
ESD	Electrostatic Discharge
ETSI	European Telecommunications Standards Institute
FMCW	Frequency Modulated Continuous Wave
FPGA	Field Programmable Gate Array
FSPL	Free Space Path Loss
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
IC	Integrated Circuit
IoT	Internet of Things
ISM	Industrial, Scientific, and Medical
LAN	Local Area Network
LO	Local Oscillator
LoS	Line of Sight
MIMO	Multiple-input, Multiple-output
MLS	Maximum Length Sequence
PC	Personal Computer

PCB	Printed Circuit Board
PET	Polyethylene Terephthalate
PLL	Phase-locked Loop
PTFE	Polytetrafluoroethylene
RAM	Random-access Memory
RCS	Radar Cross Section
REFlex	Real-time Localization for Flexible Production Environments
RF	Radio Frequency
RFID	Radio Frequency Identification
RRC	Root-raised-cosine
RSSI	Received Signal Strength Indication
RX	Receive
S-parameter	Scattering-parameter
SDR	Software Defined Radio
SISO	Single-input, Single-output
SNR	Signal to Noise Ratio
TCP	Transmission Control Protocol
ToF	Time-of-flight
TRL	Through-reflect-line
TX	Transmit
UDP	User Datagram Protocol
UHF	Ultra High Frequency
UWB	Ultra Wide Band
VHDL	Very High Speed Integrated Circuit Hardware Description Language
VNA	Vector Network Analyzer

List of Symbols

c_0	speed of light in vacuum
$*$	convolution
$\star$	cyclic cross correlation
ϵ_r	relative permittivity
k	wave number
λ	wavelength
μ_r	relative permeability
$(R \Rightarrow T)$	reader to tag communication
$(T \Rightarrow R)$	tag to reader communication

Chapter 1

Motivation, Thesis Outline, and State of the Art

Automatic and reliable identification of objects is an important part of today's automation work flows in industry and logistic. With the raise of the internet of things (IoT), more and more applications demand for an inexpensive, accurate, and ubiquitous identification and localization. One of the promising systems for contactless identification is ultra high frequency (UHF) radio frequency identification (RFID), which is based on low cost, battery free transponders with an interrogation range of about 10 m. For many of these systems an additional localization with cost optimized infrastructure would be very beneficial and would enable more use cases. Systems for identification are already widely deployed in industry, and therefore, research effort is put into development of localization systems based on already deployed tags. The nowadays used approach for localization of RFID tags includes received signal strength indication (RSSI) and angle of arrival (AoA) based systems. Both of these localization methods have in common that the results are strongly distorted by multipath propagation. Unfortunately, RFID systems are commonly used in industrial environments, where strong reflections due to metal parts occur. This results in severe multipath channels, and therefore, the prior mentioned localization methods result in large errors. In some applications mixing up different tagged objects can result in high follow up costs, e.g. sorting baggage on an airport. On typical conveyor belt scenarios constructive methods, such as unwieldy metal shieldings, are used to separate items for the identification process. These constructions could be substituted by reliable localization systems.

To overcome the limitations of the classical localization systems, this thesis focuses on a novel method for ranging of RFID tags which utilizes a much broader

bandwidth and is so less susceptible to multipath environments. The presented method can be applied to almost every RFID system whose tag to reader ($T \Rightarrow R$) communication is backscatter based. A testbed for this localization method which works with electronic product code (EPC) standard conformal RFID tags will be presented.

The thesis is structured as follows: Sections 1.1 and 1.2 present an introduction into RFID systems and an overview over radio frequency (RF) localization methods, respectively. Chapter 2 introduces the time-of-flight (ToF) based ranging method for backscatter based RFID tags and presents regulatory requirements as well as requirements onto a testbed platform. The implementation of this test platform, which is based on a commercial-off-the-shelf (COTS) available software defined radio (SDR), is discussed in chapter 3. Ranging results acquired with the previously mentioned SDR testbed are discussed in chapter 4. Afterwards, the influence of the RFID tag onto the localization accuracy is analyzed in chapter 5. Within that chapter, measurement methods used to characterize the reflection parameters in the different modulation states are discussed. Furthermore, a method for simulation of the complex valued delta radar cross section (ΔRCS) of RFID tags is shown and the results are discussed with regard to the impact onto the ranging performance. Furthermore, a two frequency tag is introduced which enables a separation between identification and ranging in frequency domain. Thereby, the identification is done in the UHF frequency band and ranging is performed in the 2.4 GHz industrial, scientific, and medical (ISM) band. Chapter 6 shows how the testbed was extended to support concurrent ranging with multiple SDRs. This converts the single-input, single-output (SISO) testbed to a multiple-input, multiple-output (MIMO) testbed and enables the use of the two frequency RFID tags. Furthermore, measurement results obtained with the MIMO testbed are shown and discussed. The thesis finishes with a conclusion and an outlook in chapter 7.

1.1 Radio Frequency Identification

RFID systems are a class of auto identification systems for contactless identification of objects with attached transponders, which use RF signals. These systems can be classified by different key parameters [1]:

- Operating frequency
- Operation in the near- or farfield
- Active, passive, or semi-passive tag design
- Strategy to separate a tag population

- Memory capacity
- Encryption capabilities
- Cost of the tag

The RFID system best suited for the application can be chosen by finding a system whose key parameters match the application.

For example, for an access control system in an office building one requirement is that the door only opens if the transponder is in close range to the reader. Overreach is very problematic, since it could open the door to people which are not allowed to enter. Therefore, typically near field systems are used, which operate on a pretty confined range in the order of 10 cm. Furthermore, it would be advisory to choose a system which can assure that tags are genuine and cannot be copied. This can be achieved by using authentication with strong cryptography.

Another example could be a system used to identify items in a warehouse for inventory. Here it is useful if the reading range is large such that an inventory can be made automatically. Therefore, a farfield system would be chosen. Another key aspect would be the cost of the individual tag which must be as cheap as possible, as the tags are needed in high volume. The tags will be probably used only one time as the labor cost for removing it from the items would be in most of the cases higher than buying a new label. Therefore, also a small ecological footprint is important, which makes it necessary that the tags have no batteries. Therefore, they need to be passive, meaning that the individual tag has no long time energy storage and collects the energy needed for operation from the RF field of the RFID reader. For these requirements passive UHF EPC tags are well suited. Billions of EPC tags are already deployed worldwide in a variety of applications, e.g. in the apparel industry, in logistic warehouses, for safety critical documentation of aircraft maintenance.

In this thesis, the main focus lies on RFID systems complying to the the EPC UHF Gen 2 Air Interface Protocol [2]. This protocol was first published in 2004 as a successor of the Gen 1 protocol [3] and it is commonly used for logistic applications.

1.2 Ranging Methods

Estimating the distance between a transmitter and receiver is a common task in RF systems. The method used depends on the required accuracy and on the resources available on the transmitter and receiver. The simplest method, which normally comes at almost no additionally hardware cost, is the utilization of the RSSI. If the receiver hardware allows coherent processing of multiple RF signals,

spatial information can be derived from the measured RF phases. Systems utilizing this information are for example AoA or frequency modulated continuous wave (FMCW) radar systems. Finally, ranging information can also be derived from the ToF of the radio signal. In the following subsections, these three localization methods are introduced and their applicability for RFID systems is discussed.

1.2.1 Received Signal Strength Indication

The RSSI of a received RF signal can be used to calculate the distance between the transmitter and the receiver. This is accomplished for line of sight (LoS) RF links by reformulating the well known Friis transmission equation

$$\hat{d} = \sqrt{\frac{P_t A_t A_r}{P_r \lambda^2}}, \tag{1.1}$$

where P_r and P_t are the received and transmitted power, A_t and A_r are the effective areas of the transmit (TX) and receive (RX) antenna, λ is the wavelength of the RF signal, and $\hat{d}$ is the estimated distance between the TX and RX antenna. This formula is only valid for LoS scenarios. In multipath environment different signal paths sum up coherently at the receiver. Molisch shows in [4, chapter 5] how the superposition of planar waves with different incident directions results in so called small scale fading. Due to this apparently random fading, the relationship between RSSI and the distance between TX and RX is not unique in multipath channels.

Furthermore, subtle pitfalls other than fading due to multipath can occur as well. For example, the effective area of the antennas depends on the incident direction and on the polarization of the wave. Therefore, even in a pure LoS scenario, antenna orientation affects the RSSI measurement value. This distorts the ranging results if the orientation of the antennas is not known and corrected.

All the previous discussed effects make ranging based on the RSSI hard to be used in practice if accurate ranging is needed. However, since the evaluation of the RSSI is rather easy, many researchers try to find ways to make use of this data. Developed systems show that by using multiple access points it is possible to get an approximate location information of mobile devices. One method is called fingerprinting, which means that the RSSI values at different locations are pre-measured and stored in a database. During this learning process the location of the mobile device must be known by other sources, e.g. by global navigation satellite systems (GNSSs) or manual measurement. As soon as the fingerprint database is filled, the position of a mobile device is estimated by measuring the RSSI of all access points within communication distance. By comparing the

measured data with the previously recorded database the location of the mobile can be determined. This method works very well, and can be observed, for example, on smart phones. In urban areas with plenty of wireless local area network (LAN) access points, a localization of the mobile device is performed by evaluating the RSSI of these access points. Therefore, localization is possible even in scenarios where GNSSs do not work properly, e.g. indoors.

Deriving spatial information based on the RSSI for RFID systems is somehow problematic in practical applications. First of all, RFID systems are typically deployed in industrial environments where inherently large metal objects form a dense multipath (DM) channel. Furthermore, RFID tags change their ΔRCS depending on the incident signal power [5], [6]. They typically reduce the ΔRCS if more power is applied, since tags close to the reader do not need a large ΔRCS to be read by the reader. Therefore, the RSSI nonlinearly depends on the power received by the tag. Another problem is that the orientation of the tag with respect to the reader is typically unknown, which leads to not correctable errors due to the gain patterns of the antennas.

Despite all the difficulties mentioned before, there are scenarios where RSSI based localization can be applied to RFID systems. Some researchers showed that fingerprinting with RSSI measurements can be used for grouping RFID tags spatially [7], [8]. Furthermore, the RSSI data can be combined with phase measurement data to get a better accuracy [9].

1.2.2 RF Phase Based Localization

Time delays of sinusoidal signals can be represented as phase shifts. A delay τ relates to a frequency dependent phase shift of $-2\pi f\tau$ radian. This delay can be used to calculate spatial information by utilizing the constant speed of propagation

$$c_{medium} = \frac{c_0}{\sqrt{\epsilon_r \mu_r}}, \tag{1.2}$$

where c_0, ϵ_r, and μ_r are the speed of light in vacuum (299 792 458 m/s), the relative permittivity, and the relative permeability, respectively.

However, measuring the phase of an RF link consisting of spatial separated TX and RX systems is not as straightforward as determining the RSSI. The main problem is that the TX and the RX need to have coherent local oscillators (LOs) in order to measure the phase difference. This problem can be solved if the phase is measured only at one side of the RF link. Thus, the two way delay can be derived. This is accomplished if station one sends out an RF signal which is received by station two. Station two now synchronizes its own oscillator to the received waveform and transmits it back to station one. Now, station one can compare the phase of its own oscillator with the phase of the received

signal and, thereby, measures the overall phase shift introduced by the two-way channel. From a practical point of view, the synchronization due to the temporal stability of the used oscillator is critical. Nonetheless, a chipset implementing this ranging technique is already commercially available (AT86RF233) from *Atmel®*. An ranging error in the order of 60 cm can be achieved, which was demonstrated in an indoor experiment in a large university hall [10].

Another possibility is to measure the phase difference between two signals, as it is done in spatial domain phase difference of arrival measurements described in section 1.2.2.3.

In backscatter scenarios, phase measurements can be done at the interrogator by evaluating the phase between the two modulation states. No synchronization between multiple oscillators is needed since in typical RFID readers one oscillator is used to drive the RX demodulator and the TX modulator. Phase information is available at most of the commercial RFID reader systems since it comes at practically no additional hardware costs if phase coherent processing is utilized.

In the following, three configurations for deriving spatial information from phase measurements will be discussed.

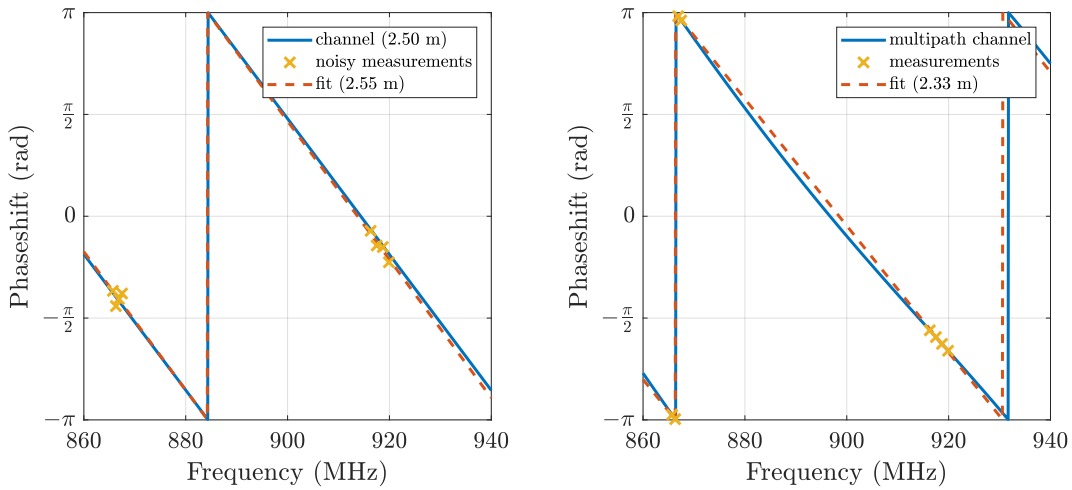
1.2.2.1 Direct Relationship between RF Phase and Distance

One possibility is to derive the distance between transmitter and receiver directly from the phase of the received signal. Phase measurements have an ambiguity at every wavelength. Therefore, the measured two-way link distance has an ambiguity every 16.5 cm, as the freespace wavelength is about 33 cm for UHF frequencies used in RFID systems. While this seems obstructive for practical application, it can be used for example to detect small movements in the long term, for example providing an alert system for landslides and volcanoes. For this applications it is necessary to correct for phase offset drifts which can be caused by meteorological conditions or long time drifts [11].

Another possiblity is to combine these measurements with a physical model. In [12], a system to track an object in a 3×3 m space by using phase measurements of four reader antennas and a nonlinear Kalman filter with smoothing is shown.

1.2.2.2 Frequency Domain Phase Difference of Arrival

The second method utilizes the frequency dependence of phase measurements to calculate the distance from the phase difference between two phase measurements at different frequencies. Thereby the small ambiguity free range of a single frequency measurement can be resolved. The phase difference must be measured



(a) Phase measurements are distorted by a normal distribution with zero mean and $\sigma = \frac{\pi}{30}$. The results are linearly fitted to get a distance estimate.

(b) Phase measurements are taken from a two-way two-tap multipath channel (ground reflection). The results are linearly fitted to get a distance estimate.

Figure 1.1: RF phase based distance measurement by using only the ETSI high power channels in the lower and upper band. The LoS distance was simulated with 2.5 m. Two results are depicted, where (a) shows a simulation of a linear fit using noisy phase measurements and (b) simulates a two-way two-tap multipath channel.

and the two way delay can then be calculated by

$$\hat{\tau} = \frac{\varphi_1 - \varphi_2}{2\pi(f_2 - f_1)} \ . \tag{1.3}$$

The ambiguity is removed if the difference between the phases is smaller than 2π. This means that the ambiguity free range for $\hat{\tau}$ in free space is $\frac{c_0}{\Delta f}$, with the frequency spacing $\Delta f = f_2 - f_1$. By choosing too closely spaced frequencies in real world applications the temporal resolution is decreased due to measurement noise. In practice, one would use more than two frequencies to reduce measurement noise and to obtain more accurate ranging results.

In RFID systems, frequency dependent measurements can be acquired by interrogation of the tags at different frequencies. However, this strategy is problematic since the allowed frequency band of RFID systems is rather narrow due to regulation. In Europe the spacing between the lowest high power channel of the lower band to the highest high power channel of the lower band is 1.8 MHz while the spacing in the upper band is 3.6 MHz [13]. Nevertheless, the upper

band is currently not deployed in all countries of Europe. An overview of all allocated frequency bands for RFID world wide can be found on the webpage of GS1 [14]. With this relatively small spacing between the channels the measurement is free of ambiguities up to several hundredths of meters which is not problematic since passive backscatter based RFID systems have typical operation ranges below 20 m. However, the sensitivity to measurement errors of the phase is rather high due to narrow frequency spacing, e.g. 4.3 °/m for 1.8 MHz spacing and 8.6 °/m for 3.6 MHz spacing. The problem with the high sensitivity can be resolved if measurements are made at the outermost high and low band channels. The spacing is 54.2 MHz, and therefore the resolution is 130.1 °/m. It is also possible to combine the measurements on multiple channels.

Figure 1.1a shows the results of such a combined measurement on all available channels allowed by European Telecommunications Standards Institute (ETSI). The simulation was conducted with the assumption that the error of phase measurements is normally distributed with zero mean and a standard deviation of $\frac{\pi}{30}$rad. To derive a distance measurement from the eight unequally spaced measurement points, a fit onto a linear phase model according to

$$(\hat{d}, \hat{\varphi}_0) = \underset{d\in[d_{min},d_{max}],\varphi_0\in[-\pi,\pi]}{\arg\min} \sqrt{\sum_{i=1}^{N_{meas}} \left(\varphi_{meas,i} - \left(\varphi_0 - \frac{4\pi d f_i}{c_0}\right)\right)^2} \tag{1.4}$$

was performed, where $\hat{d}$ is the estimated distance, $\hat{\varphi}_0$ is a nuisance parameter to account for an arbitrary phase shift, d_{min} and d_{max} specify the search space, N_{meas} is the number of measurements, and $\varphi_{meas,i}$ the i-th measurement result at frequency f_i. The distance search space was limited to −1 m to 16 m[1] for the simulation results shown in fig. 1.1, which reflects the typical read ranges of EPC tags. Within this search space, several local minima distributed over the whole parameter space exist. Therefore, it is likely to get a wrong distance estimation if the phase measurements are too noisy.

This method can only be applied in quasi static scenarios, where the tag is assumed to be at the same position during multiple interrogations. The time between two consecutive EPC readouts is at least 3.8 ms[2] if the tag is interrogated on two distinct frequencies. This value is calculated with highest possible data rate according to the EPC standard [2] including the time for a proper power off

[1]The search space was chosen larger than the expected read range of passive EPC RFID tags to provide reasonable margin for practical uncertainties, for example stemming from wrong calibration of cables or additional group delay of the tag (see chapter 5).

[2]This minimum duration is calculated assuming the fastest interrogation settings allowed by [2] (Backlink frequency = 640 kHz, T_{ari} = 6.25 µs) and a 96 bit long EPC. It includes the RF carrier power up and power down time as well as the communication time (Select, Query, and RN16 command).

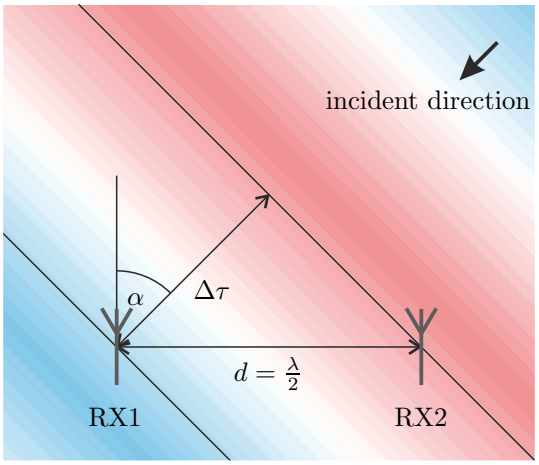


Figure 1.2: Measurement of the AoA by using two antennas

and power on and also the time for selecting a single tag based on its 96 bit EPC. This means that in a dynamic environment, where for example the tag is moved with a speed of 1 m/s, the phase will be altered by about 8° due to the change of the distance during the interrogation (3.8 mm).

Another problem is that the method is vulnerable to multipath propagation. To get an impression of the effects of multipath onto the measurements results, a simulation was set up, including the LoS propagation and the ground reflection. However, in practice not only the ground reflection will occur and the measurements will be much more distorted. The simulation was done with a two-tap model, where the LoS path was simulated with a distance of 2.5 m and the ground reflection with a distance of 4.4 m. The multipath was attenuated by 10 dB with respect to the LoS path to account for the lower gain of the antenna due to the different spatial direction, the loss at the ground reflection, and also the higher free space path loss (FSPL) resulting from the longer path length. The result can be observed in fig. 1.1b where it can be clearly seen that the fit with a single LoS component fails and predicts in this case a lower distance between reader and tag even though no measurement noise was added. This shows that the method is not robust against multipath propagation, which is also explained in detail in [15]. One could argue that a fit with multipath data to a LoS scenario is not the optimal solution. However, a fit to the multipath scenario would be practically not possible due to the limited number of available supporting points. Furthermore, the simulation results shown in fig. 1.1b are performed without any uncertainty of the phase measurements, which also would limit the accuracy in practice.

In chapter 5, the influence of the tag design onto the ranging performance will be discussed. RFID tags are commonly based on dipole antennas which are

resonant structures, and therefore strongly frequency dependent. Simulations and measurements [6], [16] showed that both, the magnitude of the ΔRCS and the phase are strongly frequency dependent. This imposes additional problems onto the ranging method as the influence has to be compensated to get accurate measurements. This calibration could be specific to every individual tag design. However, the calibration could also depend on the material the tag is attached to, which would pose a problem for practical scenarios. Furthermore, the tested tags also showed a dependency of the group delay on the actual received power, which further introduces ranging inaccuracy, hard to compensate.

1.2.2.3 Spatial Domain Phase Difference of Arrival

The incident angle of a wave front can be measured by calculating the difference between the RF phase of two closely spaced antennas. In literature, this is also sometimes called the AoA. Figure 1.2 shows two antennas and an arriving wave front. Depending on the incident direction, the plane wave arrives at one antenna earlier than on the other which leads to different delays, and therefore different RF phases. Thus, the incident angle of the received RF wave front $\hat{\alpha}$ can be calculated by

$$\hat{\alpha} = \arcsin\left(\frac{(\varphi_{RX2} - \varphi_{RX1})\lambda}{2\pi d}\right), \tag{1.5}$$

where φ_{RX2} and φ_{RX1} are the measured phases of the received RF signal, λ is the wavelength of the received signal, and d is the distance between the antennas. If the distance d is larger than $\frac{\lambda}{2}$, the arcsin() function introduces ambiguities, which can be avoided by a closely spacing of the antennas. On the other hand, the antennas should be spaced as far apart as possible to achieve a high resolution. Consequently, an antenna spacing of $\frac{\lambda}{2}$ should be used.

With two antennas it is not possible to identify if the wave front is coming from behind the antenna array or from the front. By using a third antenna, this ambiguity could be resolved. For example three antennas arranged in a triangle configuration can be used to determine the angle of reception around 360°.

As already explained, the phase information of the RFID tag response is obtained by most of the COTS RFID readers. Many of these readers also allow to connect several antennas. However, most of the readers only use one antenna at a time. Therefore, the tag must be interrogated multiple times for an AoA estimation. This results in the same problems regarding dynamic environments as stated in section 1.2.2.2. However, this shortcoming can be resolved by using more demodulators parallel as can be seen in the hardware setup of [17], where a COTS reader is used in conjunction with a custom switch and demodulation board.

Also a spatial antenna array can be used to perform beam forming of the TX signal [18]. With the ability to steer the RF beam, an angle of activation and deactivation can be measured. The spatial information of the tag is afterwards derived by assuming that the tag is between the two measured activation angles.

Some manufacturers already use this techniques in their products [19]–[21]. However, they do not exactly specify how the localization is performed and they also might not allow the user to access the raw data. Thereby one can only evaluate the results and check if the accuracy is good enough for the desired application.

Nikitin et al. [15] performed measurements with a COTS RFID reader in an experimental warehouse portal. The results of these measurements showed that spatial domain phase difference of arrival is one of the robustest methods for phase based RFID localization for this setup.

1.2.2.4 Time Domain Phase Difference of Arrival

Phase measurement can also be used to measure the speed of objects. One method is the so called Doppler radar where a continuous wave (CW) wave is transmitted and the reflection on an object is analysed. An object which moves in direction from the transmitter or to the transmitter produces a continuous phase change in the observed reflection signal at the transceiver. This phase change is directly proportional to the velocity of the object with respect to the transceiver and the relative speed $\hat{v}$ can be calculated by

$$\hat{v} = -\frac{c_0}{2\pi f}\frac{d\varphi}{dt}, \tag{1.6}$$

where negative $\hat{v}$ indicate that the object is coming closer and positive $\hat{v}$ that the object is moving away from the antenna.

Therefore, multiple phase measurements can be used to measure the speed of a tag relative to the reader. This can be utilized for example to measure the direction of movement which can be an indicator to know if a tag is leaving or entering a particular area. It also can be used to distinguish between moving and static tags [22].

1.2.3 Time of Flight Based Localization

ToF based methods measure the time a signal takes to travel from the TX to the RX. Since the propagation speed of the RF signal is normally known, the delay can be used to measure the distance. The temporal resolution of ToF systems depends on how accurate the time can be measured. There are multiple methods

available to measure the time of reception, all of which having different temporal resolutions, accuracies, and implementation efforts.

To measure the ToF the time of transmission and the time of reception has to be known. The receiver can detect the start of reception for example if the RX signal strength rises above a certain threshold. The resolution of this approach depends on the clock rate from which the time stamps are derived. Furthermore, the accuracy is also dependent on how accurate the start of the RF reception can be determined. For example, RF frames with a slowly rising envelope make the system more prone to errors.

Another possibility is to compute the cross-correlation between the received signal and a copy of the transmitted signal. Therefore, the receiver evaluates the result of the correlation and determines the ToF by searching for a peak in the output of the correlation function. Since this method does not only use the rising edge of the envelope, it is typically much more accurate. However, the downside of this approach is that specifically designed transmit signals with good autocorrelation properties should be used. This means that the signals should only have a strong peak at zero offset and few other maxima with a high relative attenuation to the peak at zero, so that the detection in noise is less prone to errors. Furthermore, to compute the cross-correlation of the signals the complexity of the receiver has to be increased. This method is used for example in GNSS systems [23] where a high accuracy is demanded. In section 2.2 the requirements onto the ranging signal will be discussed. Section 2.3 will show the relation between the bandwidth of the ranging signal and the measurement errors due to multipath propagation.

All presented methods need precisely synchronized clock sources of the TX and RX. Since this is problematic for mobile stations, some approaches have been developed which do not need this synchronization.

One of them is to measure the two way round trip time. Thereby, station one sends out a message which is received by station two. Station two must now send a message back to station one, indicating how much time has passed between reception and transmission or having a fixed time offset. The master can now determine the two way ToF is by calculating the time difference between transmission and reception minus the processing time at station two.

Another method does not even need a two way communication, which is for example not feasible for GNSS applications. However, multiple coherent base stations or satellites at known places are needed. All stations send out a unique ranging signal simultaneously, and therefore, the ΔToF between the multiple propagation paths can be calculated[3]. By using this ΔToF measurements and knowing exactly the positions of the transmitters, the receiver can calculate its

[3] At least four transmitters are necessary for 3-D localization and time synchronization

own position and also synchronize its clock to the common clock of the transmitters.

For RFID systems, ToF based methods are hard to implement due to the low data rate of the communication, the imprecise oscillator of the tag, and due to stringent power constrains on the tag side. Therefore, ToF RFID localization systems are mainly based on a two way ToF measurement where no processing on the tag is required. For example, in [24]–[26] a system is shown where ToF based measurements are collected with specialized tags which have an UHF part to wake up the tag and provide coarse synchronization and an additional ultra wide band (UWB) switch, which is utilized for backscatter modulation of UWB pulses transmitted by the interrogator. The receiver performs non-coherent cross-correlation with the transmitted pulses and is so able to detect the tag response and the two-way ToF.

A method which enables ToF based ranging measurements for standard EPC RFID tags was reported and evaluated by Arthaber and Faseth [27]–[29]. An additional broadband ranging signal is superimposed during the $(T \Rightarrow R)$ communication. The received signal at the interrogator consists of reflections of the environment, the leakage from TX to the RX, and the reflection of the tag. By using a coherent adding method, the static reflections are suppressed while the part of the reflections which is modulated by the tag is amplified. Therefore, a correlation based broadband ranging is made possible with EPC COTS tags. This ranging method will be presented in chapter 2 in detail since it forms the basis of the further investigations within this thesis.

Chapter 2

Time of Flight based Ranging for RFID Tags

RFID systems are mainly used in multipath scenarios. Hence, localization results obtained with RSSI and RF phase based methods are unreliable due to fading and phase distortions as already discussed in section 2.1. For accurate ranging results in multipath environments, the bandwidth of the ranging system is of major importance. UHF RFID systems are narrowband due to regulation [13] and also due to the tag design, which is normally optimized for a high sensitivity in the frequency range of 865 MHz to 928 MHz. Therefore, broadband RSSI and RF phase measurements seem to be not applicable at the first glance. Nevertheless, a new method [27]–[29] which overlays a broadband low power ranging sequence on top of the normal EPC communication shows that broadband ranging is possible with standard conformal EPC RFID tags.

The following sections will discuss the ToF based ranging method for backscatter RFID tags. Section 2.1 introduces the coherent averaging method used to separate the reflected ranging signal of the tag from the static reflections. Section 2.2 shows how cross-correlation is used to calculate the ToF of a signal. In section 2.3 the influence of multipath channels onto the cross-correlation based ranging is discussed. Finally, the regulatory situation in Europe and the requirements onto the ranging hardware are discussed in section 2.4 and section 2.5, respectively.

2.1 Ranging with an Overlaid Signal

As discussed in section 1.1, the communication between the interrogator and an EPC RFID tag is half duplex, meaning that it consists of a downlink phase

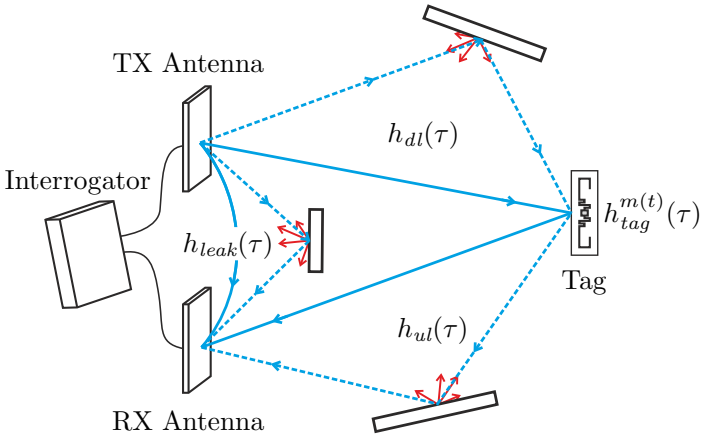


Figure 2.1: RFID channel in a bistatic environment with a single interrogator

($R \Rightarrow T$) where information is transmitted by the reader to the tag and an uplink phase ($T \Rightarrow R$) in the other direction. The discussed ranging method operates in the uplink phase, where the interrogator sends out a CW signal to supply the tags within the interrogation area with energy while the currently active tag transfers data by switching its modulation transistor according to a modulation scheme standardized by GS1 [2].

Figure 2.1 shows the typical RFID channel model for backscatter modulation in a bistatic environment with a single RFID reader, also called interrogator. The leakage between the TX and RX antenna is characterized by its impulse response $h_{leak}(\tau)$. It includes all paths which are not modulated by the active RFID tag (e.g., coupling between the antennas, reflections on the static environment, and reflections on inactive RFID tags[1]) and is sometimes also called static clutter. The downlink and uplink impulse responses $h_{dl}(\tau)$ and $h_{ul}(\tau)$ describe the channel between the reader and the tag. In typical RFID scenarios they consist of a strong LoS component and diverse other so called multipath components, e.g., reflections on the ground, walls, and other reflective items like metal structures. Another important component of the backscatter channel is the impulse response of the tag itself $h_{tag}^{m(t)}(\tau)$. It can be modeled as an impulse response which depends on the actual modulation state $m(t) \in \{0, 1\}$. For EPC tags, this means that the impulse response of the tag is modeled by its two independent impulse responses $h_{tag}^{0}(\tau)$ and $h_{tag}^{1}(\tau)$ of the tag in tits absorbing state and its reflecting state, respectively. This model is not valid during the transitions between the states, nevertheless, this simplification is made since the coherent adding method only uses signals

[1] Inactive RFID tags do not change their reflection coefficient, therefore, they contribute only to the static clutter of the environment.

during the time when the tag response has settled already. Please note that the impulse response of the interrogator antennas depend on the spatial direction of the paths. For simplification it is included in $h_{leak}(\tau)$, $h_{dl}(\tau)$, and $h_{ul}(\tau)$.

The signal received by the interrogator $s_{rx}(t)$ can thus be derived from the transmitted signal $s_{tx}(t)$ by

$$s_{rx}(t) = \left(\left[h_{leak} + h_{dl} * h_{tag}^{m(t)} * h_{dl}\right] * s_{tx}\right)(t) + n(t), \tag{2.1}$$

where $n(t)$ is the received noise and the symbol "$*$" denotes the convolution of two signals.

For the ToF based ranging, the interrogator superimposes a low power spectral density broadband signal onto the CW carrier. Therefore, the transmit signal of the reader during $(T \Rightarrow R)$ communication in equivalent baseband reads

$$s_{tx}(t) = 1 + a s_{ranging}(t \bmod T_{ranging}), \tag{2.2}$$

where $s_{ranging}$ is the cyclically transmitted ranging signal with period length of $T_{ranging}$ and complex valued amplitude a. $T_{ranging}$ is chosen such that it is shorter than the shortest possible modulation bit[2].

During $(T \Rightarrow R)$ communication, the received signal $s_{rx}(t)$ at the reader consists of static clutter and the backscatter modulated signal from the responding tag. For the measurement of the ToF, the modulated signal must be isolated from the static reflection and leakage.

Figure 2.2 shows an illustration of the coherent averaging method used to record the tag response for the broadband ranging method. As this figure shows a symbolic representation, arbitrary signal levels and offsets are used. The colored squares indicate the ranging sequence which is transmitted cyclically. Each colored block is exactly one cycle of the ranging sequence, regardless of its color.

The modulation of the tag can clearly be seen as the square wave in the received signal $s_{rx}(t)$. A segment with length $T_{ranging}$ is recorded of every received modulation bit, where a guard time T_{guard} is used to account for the imprecise recovery of the modulation edge at the interrogator and for the settling time of the modulation transition. The modulation of the tag is not synchronous to the broadband ranging signal. Therefore, the recorded segment is cyclically shifted such that the actual code phase of the ranging signal $s_{ranging}(t)$ is compensated, and thereby the signal $s'_{rx,k}(\tau)$ is extracted. This process is done for each modulation bit.

Assuming that the channel impulse responses h_{cpl}, h_{ul}, and h_{dl} are time invariant and that the impulse responses of the tag in the two modulation states

[2]In EPC systems this is ensured if $T_{ranging} < 1/(2\mathrm{BLF}(1+\mathrm{FT}))$, where BLF and FT are the backlink frequency and frequency tolerance according to the EPC standard [2], respectively.

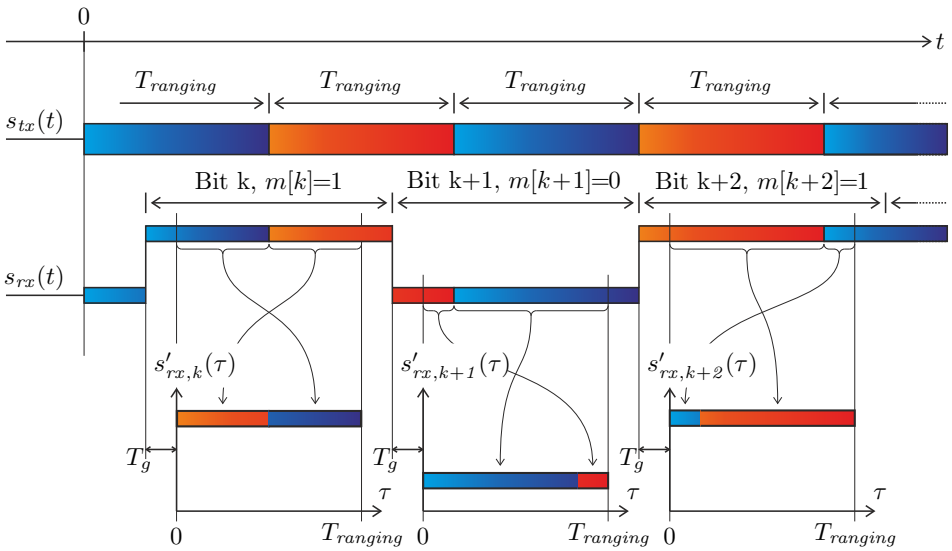


Figure 2.2: Illustration of the coherent averaging process showing how the ranging signal is extracted from the received signal.

$h^0_{tag}(\tau)$ and $h^1_{tag}(\tau)$ are also time invariant during the recordings, the recorded snapshots can be written as

$$s'_{rx,k}(\tau) = \left(\left[h_{leak} + h_{dl} * h^{m[k]}_{tag} * h_{ul}\right] * (1 + a s_{ranging})\right)(\tau) + n_k(\tau) \tag{2.3}$$

Now, a special form of coherent averaging can be performed according to

$$s'_{avg}(\tau) = \frac{1}{K_0}\sum_{k=1}^{K_0} s'_{rx,m_0[k]}(\tau) - \frac{1}{K_1}\sum_{k=1}^{K_1} s'_{rx,m_1[k]}(\tau) \tag{2.4}$$

where $m_0[k]$ and $m_1[k]$ are lists which provide the modulation bit indices of the modulation bits in state "0" and "1", respectively. Equations (2.3) and (2.4) can be combined to

$$\begin{aligned} s'_{avg}(\tau) = \frac{1}{K_0}\sum_{k=1}^{K_0} \left(\left(\left(h_{leak} + h_{dl} * h^0_{tag} * h_{ul}\right) * (1 + a s_{ranging})\right)(\tau) + n_{m_0[k]}(\tau)\right) - \\ \frac{1}{K_1}\sum_{k=1}^{K_1} \left(\left(\left(h_{leak} + h_{dl} * h^1_{tag} * h_{ul}\right) * (1 + a s_{ranging})\right)(\tau) + n_{m_1[k]}(\tau)\right) \end{aligned} \tag{2.5}$$

which can be reformulated to

$$s'_{avg}(\tau) = \left(\left(\frac{1}{K_0}\sum_{k=1}^{K_0} h_{leak} - \frac{1}{K_1}\sum_{k=1}^{K_1} h_{leak}\right) * (1 + as_{ranging})\right)(\tau) +$$
$$\left(\left(\frac{1}{K_0}\sum_{k=1}^{K_0}\left(h_{dl} * h^0_{tag} * h_{ul}\right) - \frac{1}{K_1}\sum_{k=1}^{K_1}\left(h_{dl} * h^1_{tag} * h_{ul}\right)\right) * (1 + as_{ranging})\right)(\tau) +$$
$$\frac{1}{K_0}\sum_{k=1}^{K_0} n_{m_0[k]}(\tau) - \frac{1}{K_1}\sum_{k=1}^{K_1} n_{m_1[k]}(\tau) \quad (2.6)$$

by using the distributive property of the convolution and regrouping of the sum terms. Analyzing the first line of eq. (2.6) shows that static reflections as well as the leakage $h_{leak}(\tau)$ cancel out by the subtraction, as they are assumed to be equal during all measurements K_0+K_1. The signal components modulated by the tag remain in the coherent averaging process. Assuming further additive white Gaussian noise (AWGN) with zero mean and a variance of σ_n^2 at the receiver and using the substitution $h^{\Delta}_{tag}(\tau) = [h^0_{tag}(\tau) - h^1_{tag}(\tau)]$, the equation can be further simplified to

$$s'_{avg}(\tau) = \left(\left(h_{dl} * h^{\Delta}_{tag} * h_{ul}\right) * (1 + as_{ranging})\right)(\tau) + \sqrt{\frac{K_0 + K_1}{K_0 K_1}} n(\tau). \quad (2.7)$$

The signal to noise ratio (SNR) of the received signal improves if coherent averaging is applied during the entire length of the communication. Therefore, low power ranging signals are sufficient for localization. The drawback is that the channel has to be quasi static during the coherent averaging duration. This limits the applicability to static or slowly moving scenarios.

Taking the recordings over the same number of modulation bits in both modulation states $K_0 = K_1 = \frac{K}{2}$ allows to simplify eqs. (2.4) and (2.7) even further

$$s'_{avg}(\tau) = \frac{1}{K}\sum_{k=1}^{K}(1 - 2m[k])s'_{rx,k}(\tau) =$$
$$= \left(\left(h_{ul} * h^{\Delta}_{tag} * h_{dl}\right) * (1 + as_{ranging})\right)(\tau) + \frac{2}{\sqrt{K}} n(\tau). \quad (2.8)$$

For EPC backscatter modulations the number of bits in the two modulation states is balanced anyway. Furthermore, it is also beneficial for practical implementations since memory efficient implementations are possible. Therefore, without loss of generality, in the further part of this thesis all derivations are based on the assumption that an equal number of bits in both states is recorded.

The signal $s'_{avg}(\tau)$ is essentially the convolution of the two way backscatter channel $(h_{ul} * h_{dl})(\tau)$ with the delta impulse response of the tag $h^{\Delta}_{tag}(\tau)$ and the ranging signal $s_{ranging}(\tau)$. While there are multiple methods to derive spatial information from this signal, this thesis will introduce and discuss the cross-correlation based method in detail in the following section.

2.2 Cross-correlation Based ToF Measurement

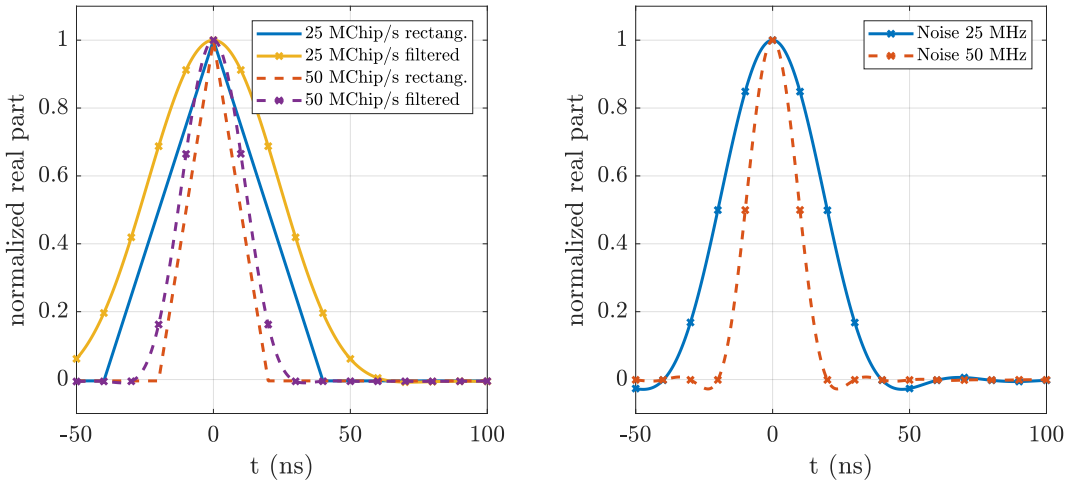
The temporal offset between two signals can be evaluated by computing the cross-correlation between them and searching for the position of the maximum magnitude. The ToF is the time offset between the received and transmitted ranging signal. For the broadband ranging method for RFID tags, the distance between tag and interrogator can be determined by

$$\hat{d} = \frac{c_0}{2} \arg\max_{\tau} \left| \left(s'_{avg} \star s_{ranging} \right)(\tau) \right| \tag{2.9}$$

where ("$\star$") denotes the cyclic cross-correlation defined as

$$(f \star g)(\tau) \stackrel{\text{def}}{=} \int_0^{T_{ranging}} f^*(t) g((t+\tau) \bmod T_{ranging}) dt. \tag{2.10}$$

Particularity well suited ranging signals have good autocorrelation properties, e.g., only a single autocorrelation maximum at $\tau = 0$. An example here for are the maximum length sequences (MLSs). The autocorrelation of these functions is triangular shaped with a base width of two times the chip length T_{chip}. For the triangular shape perfectly rectangular signals are assumed. They have infinite bandwidth, hence unfeasible in practical applications. Due to bandwidth limitations the shape of the autocorrelation function will be slightly distorted. This can be seen in fig. 2.3a, where the autocorrelation function for a 255 bit long MLS with a chip rate of 25 MChip/s and 50 MChip/s is shown. The autocorrelation is depicted without band limitation and also filtered by root-raised-cosine (RRC) filters with a roll-off factor α of 1 and a bandwidth of 25 MHz and 50 MHz for the 25 MChip/s and 50 MChip/s sequence, respectively. The utilized bandwidth was chosen such that the test platform introduced in chapter 3 is capable of transmission and reception. Furthermore, a high roll-off factor was chosen to reduce ringing in the autocorrelation function. It can clearly be seen that the autocorrelation functions of the bandwidth reduced signals have no sharp triangle tip but a rather flat top, which has a negative impact onto the ranging resolution under low SNR conditions. A higher chip rate and bandwidth would be favorable, since it results in a narrower autocorrelation peak. In case of RFID localization the RFID tag limits the usable bandwidth due to its resonant structure discussed in chapter 5.



(a) Autocorrelation function of a 255 bit long MLS sequence with a chip rate of 25 MChip/s and 50 MChips/s. Both results were depicted band limited with a RRC filter and with infinite bandwidth.

(b) Autocorrelation function of a real valued noise like ranging sequence with length of 20.48 µs depicted with different band limitations 25 MHz and 50 MHz.

Figure 2.3: Autocorrelation function of (a)MLS sequences and (b) band limited noise with different bandwidth

In scenarios where multiple readers operate at the same location, one could use multiple sequences in parallel if they have good cross-correlation properties. Hence, the throughput can be improved compared to sequencing of the ranging measurements. Gold sequences [30] are an example for such sequences which are used, e.g., for global positioning system (GPS), a GNSS system with multiple satellites. Kasami sequences are another example of sequences with good cross-correlation properties [31]. Another option is the use of noise like signals. These signals exhibit good autocorrelation and cross-correlation properties. Figure 2.3b shows the autocorrelation of two noise like signals utilizing different bandwidths. The generated signals were filtered by a RRC filter with a roll-off factor α of 1 and a bandwidth of 25 MHz and 50 MHz. The peak of the autocorrelation function is slightly thinner compared to the MLS sequence, but it also shows more ringing. The main disadvantage of these noise like signals is that the crest factor is significantly higher compared to binary sequences like Gold, Kasami, or MLS sequences.

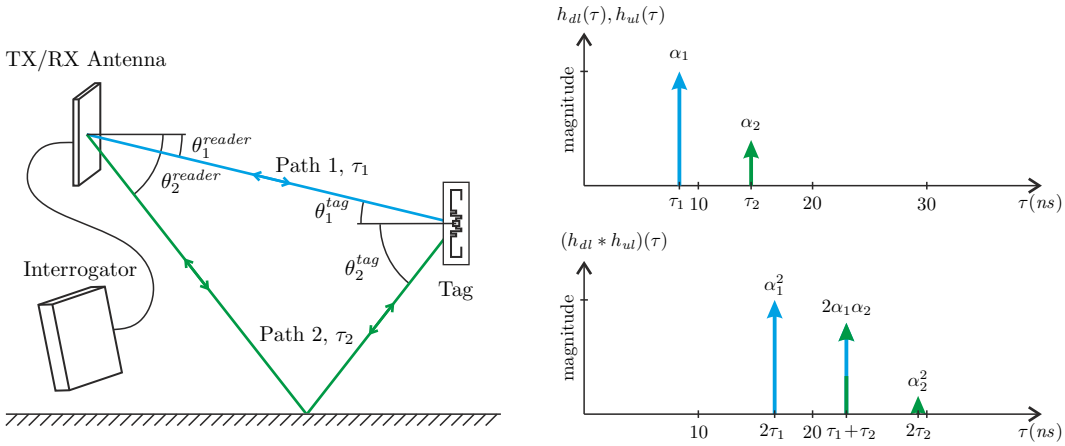
Since the autocorrelation function of band limited signals is no ideal Dirac pulse, a distortion of the result will occur if the spatial distance between several multipaths is so small that their correlation peaks overlap. Section 2.3 will discuss the influence of multipath environments onto the measurement accuracy by means of a simulation, based on a two ray model. Generally speaking, it can be noted that ranging signals with higher bandwidth have smaller auto-correlation peaks. Thus, more available bandwidth allows a better separation of multipath components and the detection of the peak is less prone to errors by noise. The usable bandwidth is limited since the delta tag response $h_{tag}^{\Delta}(\tau)$ distorts the received signal due to its narrowband behavior. Practical measurements and simulations of COTS tags will be discussed in detail in chapter 5.

2.3 Influence of Multipath Environments onto Cross-correlation Based ToF Ranging

In the following section it will be investigated to which extend a multipath channel distorts the ranging results obtained by the cross-correlation based method.

The simplest mathematical model for a multipath channel can be obtained by splitting the channel response into individual transmission paths and model them as time-shifted Dirac delta functions with different complex amplitudes. The channel impulse response of an arbitrary multipath can then be written as

$$h(\tau) = \sum_{k=1}^{K=N} \alpha_k \, \delta(\tau - \tau_k) \tag{2.11}$$



(a) RFID channel model with one ground reflection

(b) Channel impulse response of the one way channel and of the pinhole channel shown in the upper part and in the lower part, respectively.

Figure 2.4: Channel model (a) and the associated impulse responses (b) of an RFID channel with an LoS and one ground reflection component.

where N equals the number of considered paths, α_k is the complex amplitude of the k-th path, and $\delta(\tau - \tau_k)$ is a Dirac delta function time shifted by τ_k. This implies that all individual paths are assumed to be frequency independent within the band of interest. This assumption will not hold true in real scenarios, e.g., due to the frequency dependent tag response and due to diffuse reflections which cannot be separated into individual taps. Nevertheless, this model is sufficient to provide a first overview on the challenges related to localization of RFID tags by means of a superimposed broadband ranging signal in multipath scenarios.

By using this model the two ray ground reflection model is exemplary discussed. This is the simplest multipath scenario present in RFID systems. A monostatic[3] scenario depicted in fig. 2.4a is considered, where a single antenna at the interrogator is used for transmitting and receiving. The channel impulse response of the uplink and the downlink channel can be written as

$$h_{dl}(\tau) = h_{ul}(\tau) = \sum_{k=1}^{2} \alpha_k \ \delta(\tau - \tau_k) \tag{2.12}$$

where α_k is used to account for the gain of the antenna of the interrogator, the ΔRCS of the tag, the free space path loss, and the ground reflection coefficient.

[3]In a monostatic scenario one antenna is used for TX and RX. Typically the TX and RX signals are separated by an directional coupler or a circulator.

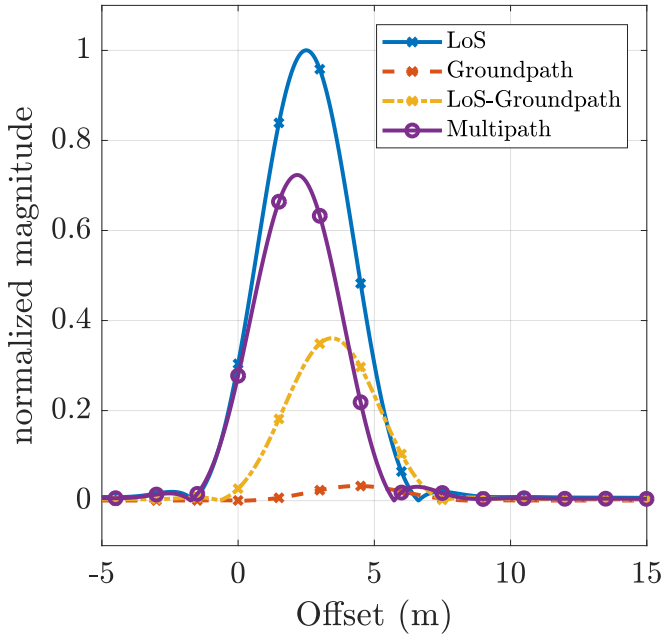


Figure 2.5: Result of the cross-correlation based ToF measurement of a typical two way scenario where tag and reader are mounted 1.8 m above the ground and spaced by 2.5 m

The channel formed by the downlink $h_{dl}(\tau)$ and the uplink path $h_{ul}(\tau)$ will from here on be called pinhole channel and can be evaluated to

$$h_{pinhole}(\tau) = h_{dl}(\tau) * h_{ul}(\tau) = \\ = \alpha_1^2\delta(\tau - 2\tau_1) + 2\alpha_1\alpha_2\delta(\tau - \tau_1 - \tau_2) + \alpha_2^2\delta(\tau - 2\tau_2). \quad (2.13)$$

Please note that the convolution of two n-tap channels results in a channel response with $\frac{(n+1)!}{2(n-1)!}$ taps. For the two ray model this is exemplary depicted in fig. 2.4b. Two important facts can be noticed from the illustration. First, the temporal distance between the LoS tap and the first reflection of the pinhole channel is $\tau_2 - \tau_1$, and therefore the same as in the one way channel. Second, the relative magnitude difference of the first to the second tap is about 6 dB smaller compared to the relative magnitude difference between α_1 and α_2.

The received ranging signal s'_{avg} is the convolution of the pinhole channel with the transmitted ranging signal. In the following it will be shown how the multipath channel distorts the cross-corelation function and thereby the computed ToF.

Figure 2.5 shows a typical cross-correlation result, simulated with a two ray multipath model where the tag and the reader are mounted 1.8 m above the

ground and the distance of the LoS path is 2.5 m. The relative magnitude difference between α_1 and α_2 was choosen to be 15 dB. While the different path lengths account for about 5 dB difference, the remaining 10 dB were assumed for reflection losses and less antenna gain in direction of the ground reflection path compared to the LoS path. The final result is shown as the multipath curve, which is the sum of the LoS path, the paths where the LoS and the ground reflection are combined, and the ground reflection paths. The maximum of the actual multipath result is shifted by approximately 33 cm to a smaller distance. The magnitude of the correlation peak is smaller than the peak of the LoS component, which is due to destructive interference of the individual components. The relative magnitude difference between the LoS path and LoS-groundpath is about 9 dB and the relative magnitude difference between the LoS path and groundpath is about 30 dB. Please note that the distortion of the correlation results mainly stems from the LoS-groundpath which has a temporal distance of only one times the difference between the LoS and ground reflection path. Hence, while the resolution of the ranging process in a two way channel compared to a one way ranging is increased by a factor of two, the temporal distance between multipaths stays equal and the relative magnitude distance decreases. This introduces large ranging errors if the contributions of the different taps are not separable due to overlapping of the cross-correlation of the individual paths.

2.4 Regulatory Considerations

In the previous section, it was shown that a large bandwidth of the ranging signal is beneficial for providing spatial resolution to separate multipath reflections. Though, several regulatory specifications have to be respected if the broadband ranging system is deployed, which limits the available bandwidth. For deployment in Europe, two standards have to be considered for compliance of the transmitted signal. These are the EPC specification of the RFID air interface [2] and the ETSI harmonized European standard EN 302 208 [13].

The EPC standard defines a transmitter spectral mask, such that multiple readers are able to operate on closely spaced channels without while the ETSI standard specifies the available frequencies and allowed power levels for RFID system operation in Europe.

As standards change regularly to adopt to new technologies and requirements, this work can only discuss and review the current situation. The reviewed versions of the standards are V 2.1 and V 3.1.1 for the EPC and ETSI standard, respectively.

Since broadband ranging for RFID tags by means of an overlaid ranging sequence is discussed mostly in an academic context, the standards have not

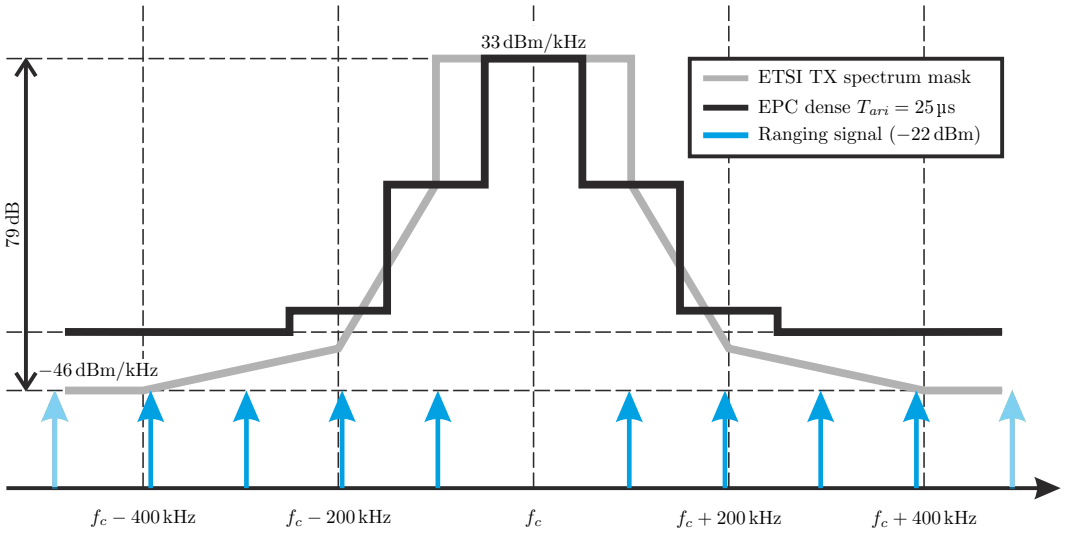


Figure 2.6: Illustration of the ETSI and EPC transmitter spectral mask and the MLS ranging signal.

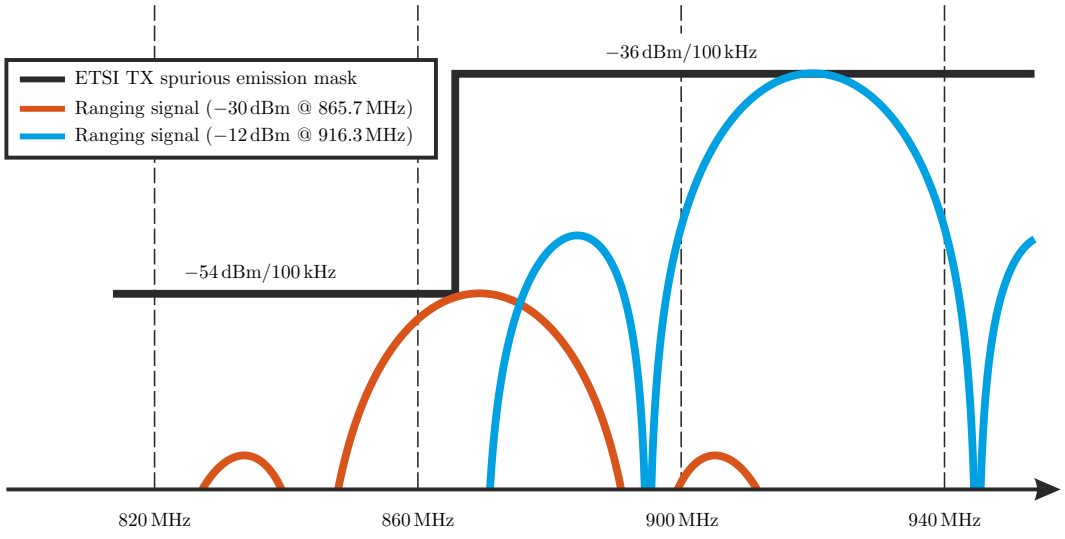


Figure 2.7: Illustration of the ETSI spurious emission mask with two possible ranging signals centered in the ETSI lower and upper band.

adopted yet to this kind of signal. The transmitter spectral masks for narrowband RFID systems are depicted in fig. 2.6 together with an exemplary ranging signal, a 255 bit long MLS sequence with a chiprate of 25 MHz. The ranging signal is depicted with −22 dBm equivalent radiated power (ERP), which ensures that the power density of the signal is below both masks. Since the ranging sequence by the reader is transmitted cyclically, it results in a discrete line spectrum, where the lines are spaced by the inverse of the period time of the cyclic signal. The spectral mask of the EPC standard scales with the used modulation bandwidth (inversely proportional to T_{ari}[4]). In fig. 2.6 the narrowest mask is shown.

The transmitter spectral mask of the EPC standard is specified without limits of the frequency range, but the ETSI mask is only defined ±500 kHz around the carrier frequency. Since the bandwidth of the used ranging signal is much larger than the defined ETSI mask, we also evaluate the maximum power, such that the signal is below the spurious emission mask. Please note that the ranging signal is an intentionally transmitted signal, hence, it is strictly speaking, not considered as a spurious emission [32]. The spurious emission mask in the UHF band of the ETSI standard is depicted in fig. 2.7. Since the mask has a discontinuity at 862 MHz, the maximum power of the ranging signal depends on the center frequency of the ranging signal if it has to be ensured that it is below the mask. For center frequencies in the lower ETSI band the maximum permissible power of the ranging signal is −30 dBm ERP. For ranging signals centered in the upper ETSI band the maximum permissible power to be compliant with the spurious mask is −12 dBm. This is above the permissible power to comply with the ETSI TX mask (−22 dBm), which has to be respected anyway.

2.5 Requirements onto the Test Platform

The presented ranging method cannot be investigated by simply using COTS interrogators. The first demonstrator, built up with COTS laboratory equipment, is shown in the dissertation of T. Faseth [28]. The EPC standard defines stringent timing requirements for the communication, if these are not fulfilled tags will ignore the transmitted commands. For example, to establish an EPC standard compliant communication with an RFID tag it is necessary to reply a random number send by the tag within 0.5 ms. These stringent real-time requirement could not be met by a testbed consisting of COTS laboratory equipment. Hence, reading the unique EPC number was not possible, and the ranging could only be performed on the much shorter RN16 part of the communication [2].

In order to simplify the demonstrator setup and to enable EPC compliant communication without the need for development of a fully custom transmitter

[4] T_{ari} is the duration of a data 0 symbol in the ($R \Rightarrow T$) communication

and receiver hardware, an SDR is used. To choose among the broad range of available SDRs some key requirements have to be fulfilled.

The available bandwidth and sampling rate is of major importance. Since the bandwidth of the tags is limited, a reasonable bandwidth for ranging is in the order of 80 MHz. This is also sufficient for ranging in the 2.4 GHz ISM band.

The dynamic range of the transmit path must be larger than 63 dB, such that the ranging signal and the EPC communication can be generated simultaneously (see section 2.4). For the receive path, the dynamic range is even more important, as the signal to be demodulated is normally small compared to the leakage of the CW carrier. An analog carrier cancellation in front of the demodulator would enhance the performance and is a key component of many COTS RFID readers. Since this is a very application specific requirement, it is unfortunately not available as an out of the box solution with normal SDRs.

Another important factor is the minimum achievable time to start transmission of a signal after a signal is received. This round trip time must be below 31.3 µs to be compliant to the EPC standard for the highest possible backlink frequency (BLF). This requirement is difficult to be met if a personal computer (PC) is used for demodulation and modulation [33]. Therefore, an implementation directly in the hardware of the SDR is preferable, but this requires access to the schematic or the program code of the SDR, which is not available from most vendors.

Furthermore, for an extension to a MIMO system, either the SDR provides multiple transceivers or it allows synchronization among multiple units.

For the presented test platform an *N210* baseband board with an *SBX* RF frontend from *Ettus* ™ is used. This SDR offers a sampling rate of 100 MSamples and a frequency range from 400 MHz to 4400 MHz with one transmit and receive path. The schematics of the printed circuit boards (PCBs) are freely available [34] and multiple units can be synchronized by a so called MIMO connector which will be shown in chapter 6. Thurs, this SDR is apparently a good choice for the demonstrator.

Chapter 3

Test Platform for RFID Ranging

To evaluate the performance of the broadband ranging method (section 2.1) a COTS SDR was used as a test platform. This chapter describes the implementation of this testbed on the chosen SDR. During my diploma thesis [35], I implemented an EPC compliant RFID interrogator, which was already designed in a way that it can be extended by the broadband ranging method.

Section 3.1 presents an overview of the developed software framework and section 3.2 shows the hardware modifications which were performed to improve the overall performance of the SDR for ranging.

3.1 Software Overview

Due to the stringent real-time requirements of the EPC communication protocol and the required high sampling rate and resolution for the ranging process, it was not possible to use the software framework provided by the manufacturer of the SDR (see section 2.5).

During the work on my diploma thesis [35], an RFID reader was developed. This implementation was used as a starting point for the development of the testbed. The implementation offers an EPC modulator, an EPC demodulator, and a software framework for communication between SDR and PC via a serial port. During the work on this thesis the implementation was extended to perform the coherent ranging method described in section 2.1. Furthermore, the serial communication interface was changed to an Ethernet based interface to increase data throughput.

The structure of the final implementation can be split in three closely interacting parts:

FPGA Implementation: A field programmable gate array (FPGA) is a user configurable integrated circuit (IC), consisting of many basic logic blocks which can be connected by a configurable switching matrix. Since the logic blocks operate independently, FPGAs are specially suited for parallel operations. The low-level FPGA implementation handles all tasks where precise timing or a high throughput is necessary. The connection to the embedded softcore microprocessor (*Microblaze™*) for control and configuration is implemented via a set of registers and memories which can be accessed from the FPGA implementation and the softcore processor. The FPGA implementation was developed in very high speed integrated circuit hardware description language (VHDL) and *Xilinx ISE®* was used for synthesis.

***Microblaze™* software:** The *Microblaze™* softcore micro processor is a light-weight 32-bit microprocessor which can be synthesized and implemented within an FPGA. The benefits of using a microprocessor compared to direct implementation in the FPGA is that the design can be easier debugged and that changes in the code of the microprocessor can be done without synthesis of the FPGA implementation, which is a very time consuming process. The *Microblaze™* processor is used as the connecting element between the FPGA implementation and the *Matlab* implementation. In the testbed, software running on the *Microblaze™* performs several tasks, for example handling of the EPC protocol and configuration of the hardware of the SDR. Furthermore, a light-weight user datagram protocol (UDP) and address resolution protocol (ARP) stack for communication with the PC was implemented for this testbed.

***Matlab* class:** A *Matlab* class was implemented which offers an easy to use interface for configuration and operation of the testbed. The main purpose of this class is to abstract the communication to the SDR in a way that the testbed can be easily integrated in *Matlab* scripts.

In the following subsections, all three parts will be explained in detail and the connections between these parts will be highlighted.

3.1.1 FPGA Implementation

The FPGA implementation is structured into four modules which are configured and controlled by the *Microblaze™* processor via registers and dual-ported random-access memorys (RAMs)[1]. Figure 3.1 shows an overview of the user logic and the signals between the modules. The *RFID RX* and *RFID TX* modules

[1]Dual-ported RAMs have two independent interfaces where the data can be accessed and stored. For RAMs, which should be accessed from the *Microblaze™* and the FPGA implemen-

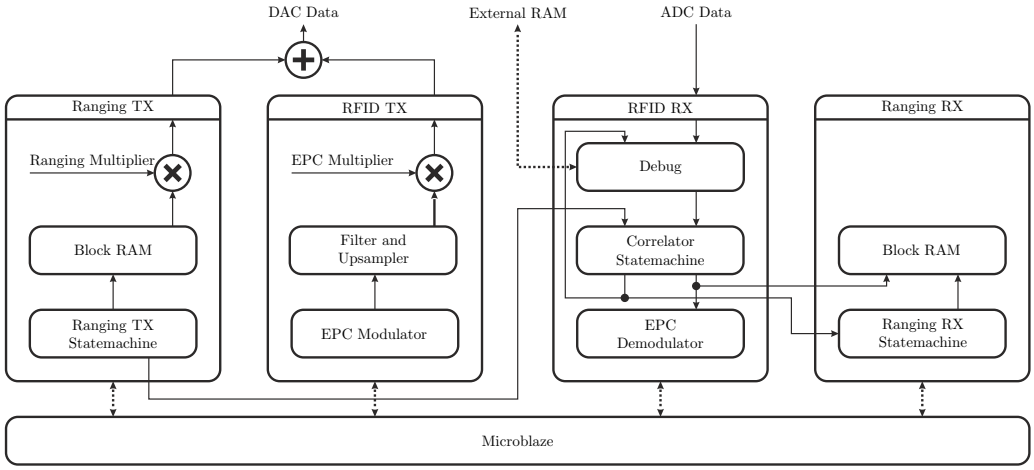


Figure 3.1: FPGA custom user logic overview

perform the decoding and encoding of the EPC communication. The coherent adding module (*ranging RX*) performs the coherent adding method as introduced in section 2.1. The *ranging TX* module is used to superimpose the ranging signal onto the EPC ($R \Rightarrow T$) communication.

3.1.1.1 EPC Modulator

The RFID TX module generates an EPC standard [2] compliant TX signal. A detailed description of it can be found in my diploma thesis [35]. In this work, only a short overview will be presented.

The modulation module consists of an EPC modulator state machine, programmed such that the content of a dual-ported RAM can be transmitted according to the modulation schemes described in [2]. Its output is connected to a pulse shaping filter and an upsampler such that the produced output signal is compliant to the relevant transmit spectral mask. After these filters, the signal can be adjusted in phase and scaled by a complex multiplier prior transmission.

3.1.1.2 EPC Demodulator

The RFID RX module is a light-weight implementation of a demodulator for EPC ($T \Rightarrow R$) communication. A detailed description can be found in [35], [36].

tation, one interface is used for each component. The interface used for the *Microblaze™* is directly memory mapped at the processor memory bus and can so be easily accessed by the *Microblaze™* processor. The other interface remains free for the FPGA implementation.

The module consists of three parts: a debug unit, a simple sub-symbol correlator, and an EPC demodulation state machine.

The debug unit can be used to store the raw data of the analog-to-digital converter (ADC) and some status information of the state machines in the external RAM on the *N210* baseband board. This data can be accessed by the *Microblaze™* and transferred to a PC for further analysis.

For the coherent averaging of the received ranging signal, the exact timings of the edges of the modulation bits have to be known. In order to derive this information in the 100 MHz clock domain, a simple sub-symbol correlator is used. This correlator is implemented by three adders and two ring buffers, each one modulation bit long. This implementation can be realized very efficiently in an FPGA. The magnitude of the output of the correlator is calculated by a coordinate rotation digital computer (CORDIC)[2] block. The output of the CORDIC is used for the demodulation statemachine to decode the $(T \Rightarrow R)$ communication.

Please note, the performance of the overall decoder is worse compared to a matched filter decoder because it relies on the correct decoding of each modulation bit. Nonetheless, this design has been chosen as it can be implemented very efficiently in the FPGA and provides the needed timing information for the coherent adding method. Furthermore, the testbed is designed for experimental research of the broadband ranging method and not for achieving best performance of the EPC decoder.

3.1.1.3 Generation of the Overlaid Ranging Signal

One important feature of the testbed is the possibility to overlay a broadband low power signal during the $(T \Rightarrow R)$ communication. To enable tests with different ranging sequences, an arbitrary signal generator has been implemented in the FPGA logic. The implementation allows transmission of cyclic signals with a maximum length of 20.48 µs, which are stored in a dual-ported RAM. The length of this cyclically transmitted sequence can be chosen from 2 Samples to 2048 Samples in the 100 MHz domain. The resolution of this arbitrary signal generator is 16 bit to match the utilized digital-to-analog converter (DAC) of the *N210* baseband board. Synchronization of the receiver of the ranging signal to the transmitter is necessary for the coherent adding operation. This is achieved by an internal synchronization signal, which indicates the beginning of the cyclic sequence.

Similar to the EPC transmitter, the output of the signal generator can be scaled by a complex constant, which is programmable via the *Microblaze™* pro-

[2]The CORDIC algorithm allows a hardware efficient implementation of many mathematically functions, e.g., trigonometric functions, logarithms, and exponential functions.

cessor. This feature enables to set the magnitude and phase of the ranging signal, without the need to refresh the content of the RAM storing the ranging sequence.

3.1.1.4 Coherent Adding of the Ranging Signal

To reduce the amount of data which has to be transferred from the test platform to the attached PC, the coherent adding of the received ranging signal is processed directly in the user logic of the FPGA.

Two separate dual-ported RAMs are used to store the results of the coherent averaging in the absorbing and the reflecting state of the tag being ranged. It is possible to reduce the memory consumption by storing the final result (absorbing state minus reflecting state) in a single memory if the number of recorded modulation bits in both states is equal (see also section 2.1). Since sufficient amount of free memory was available in the FPGA, the results are stored separately, as it could be helpful for future research.

The *ranging RX statemachine* controls the coherent averaging process. The ranging process starts by resetting the state machine, which is triggered by the *EPC demodulator* at the beginning of the $(T \Rightarrow R)$ decoding process. After reset, the unit waits until the *EPC demodulator* indicates the beginning of a modulation bit. After that, the statemachine waits for th configured guard time and performs the coherent adding for one cycle of the ranging sequence afterwards. The cyclic rotation is performed by using a counter, synchronized to the transmitted sequence as the source of the addressing of the RAMs. During the recording of the first modulation bit, the old content of the RAM is overwritten. For the following modulation bits, the received signal is added to the content already existing in the RAM. The end of the coherent adding process is, again, triggered by the *EPC demodulator*. After the coherent adding process is finished, the content of the RAM can be accessed by the *Microblaze™* and transmitted to the PC.

3.1.2 Microblaze Implementation

The *Microblaze™* is a highly configurable 32 bit softcore microprocessor to be used with *Xilinx Inc.* FPGAs. For the application, several peripherals are configured. They are used by the program running on the processor which is implemented in *C*. Most of the used peripherals are directly from the library of *Xilinx ISE®*. An *SPI* block, a *GPIO* block, and an *I2C* block from *Xilinx Inc.* are used for the communication and configuration of the hardware on the *N210* baseband and *SBX* up- and down-converter board of the SDR. Also, a slightly modified version of the 100 Mbit Ethernet peripheral is used for communication with the PC. Furthermore, the previously discussed FPGA implementation is integrated

as a user created logic block, so that registers and memories used for configuration are memory mapped to the processor.

The *Microblaze™* implementation is the connecting link between the hardware of the SDR and the *Matlab* object running on the PC. On the Ethernet side, only two protocols are implemented, the UDP protocol for command and control and the ARP protocol for discovery of the hardware address of the SDR.

The implemented UDP protocol works on a query and answer basis. This means that the SDR listens on a defined UDP port, waiting for commands sent from a PC. The commands are used, for example, to trigger the EPC communication, to configure the hardware of the SDR, and to transfer data between several memories and the PC. All commands of the PC are acknowledged by the SDR after successful completion. This procedure ensures that all commands are processed by the SDR as the UDP protocol is a best effort service and packets are not guaranteed to be received. UDP was preferred to transmission control protocol (TCP) as the memory resources on the SDR are very limited.

Furthermore, a mode is implemented where the SDR continuously queries an RFID tag population and streams the received data including the result of the ranging process to the PC. With this mode, faster read rates are achievable as the transmission of the data is performed continuously and no confirmations have to be transmitted.

3.1.3 Matlab Implementation

Matlab is used as the programming language for high level data processing. A *Matlab* class was programmed, which abstracts the communication between the SDR and the PC. Furthermore, it provides an easy to use hardware abstraction of the SDR. Therefore, programs using the SDR can be written in a way such that the code is well structured and easy to read. Example scripts are provided along with the class, showing the basic operations of the class and providing a starting point for future implementations.

Most of the methods of the class have default settings such that it is easy to get started using the SDR without detailed knowledge of all subtle parts of the implementation. However, for experiments where the full capabilities of the hardware are subject of interest, it is also possible to override these default values. One example is the configuration of the RF synthesizers used to generate the LOs of the SDR. The synthesizers can easily be configured by specifying the desired frequency. The implementation in the *Matlab* class performs the calculation of the required register settings of the synthesizer, which are specific for the used IC. However, it is also possible to set these register values manually from *Matlab*. This can be used, for example, to find the optimum operation point by performing measurements and tests with different settings.

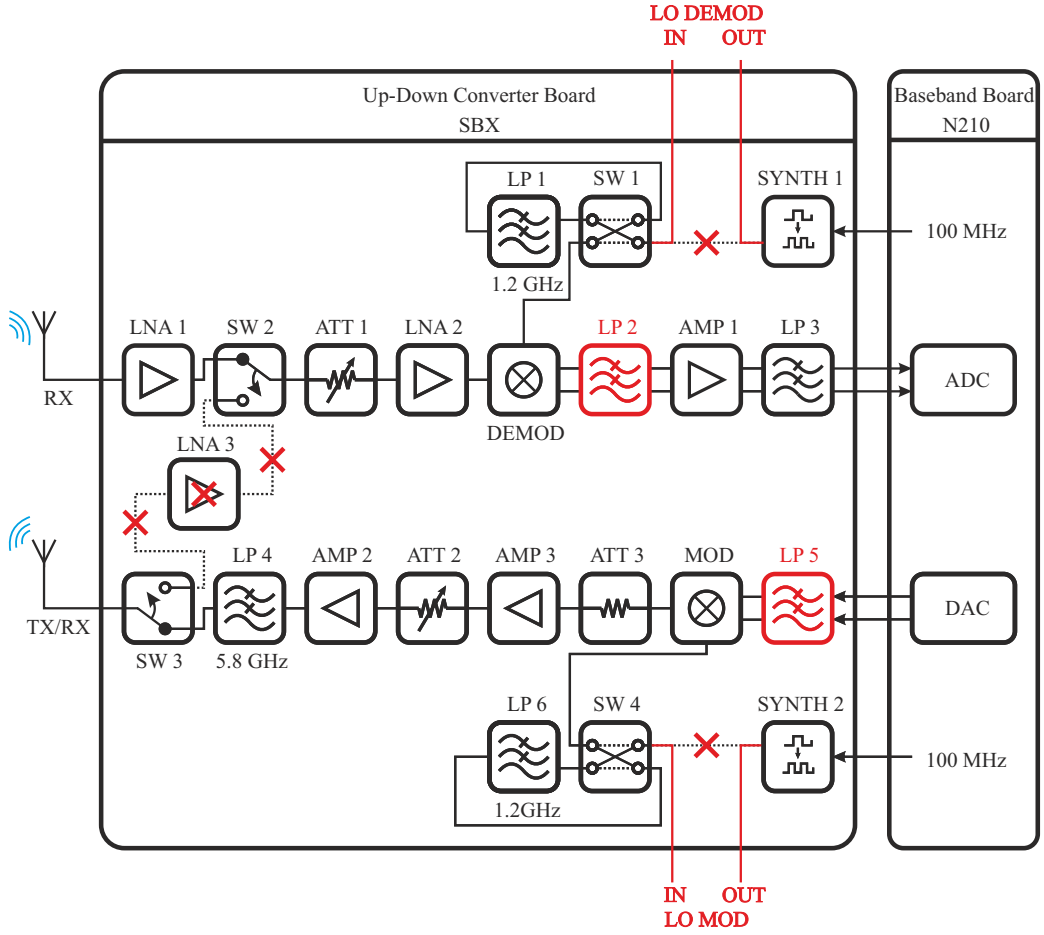


Figure 3.2: Block diagram of the SDR hardware consisting of the up-down converter *SBX* board and the baseband *N210* board. The hardware modifications for the testbed are highlighted in red.

3.2 Hardware of the Software Defined Radio

SDRs provide platforms which can be used for multiple RF standards. This versatility comes at the costs of slightly lower performance compared to dedicated hardware designs. RFID interrogators face specific problems related to backscatter communication. In contrast to other communication standards, where the bidirectional communication is normally separated in frequency or time domain, the RFID interrogator has to decode the backscatter signal of the tag in presence of the CW signal, used to power the tag. Since the used SDR is not optimized for this kind of operation, some hardware modifications were performed to improve the performance of the testbed. The modified parts are highlighted in the block

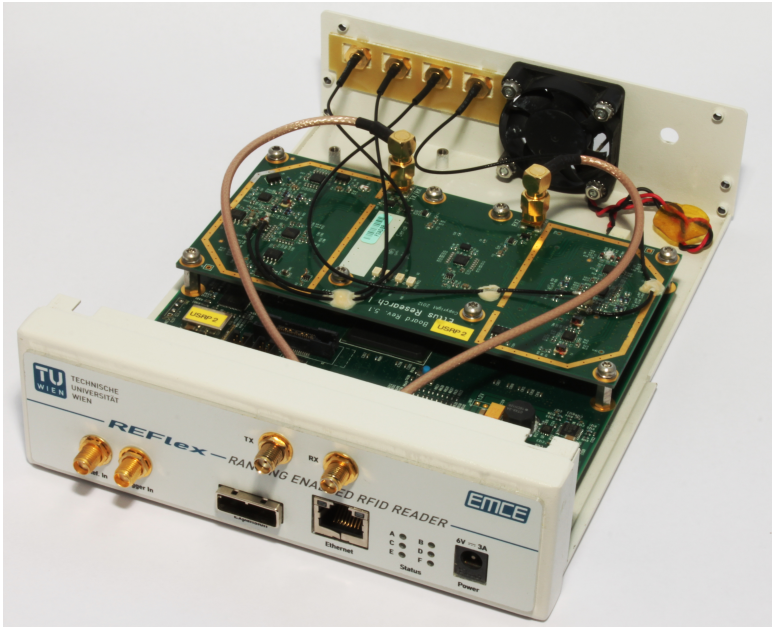


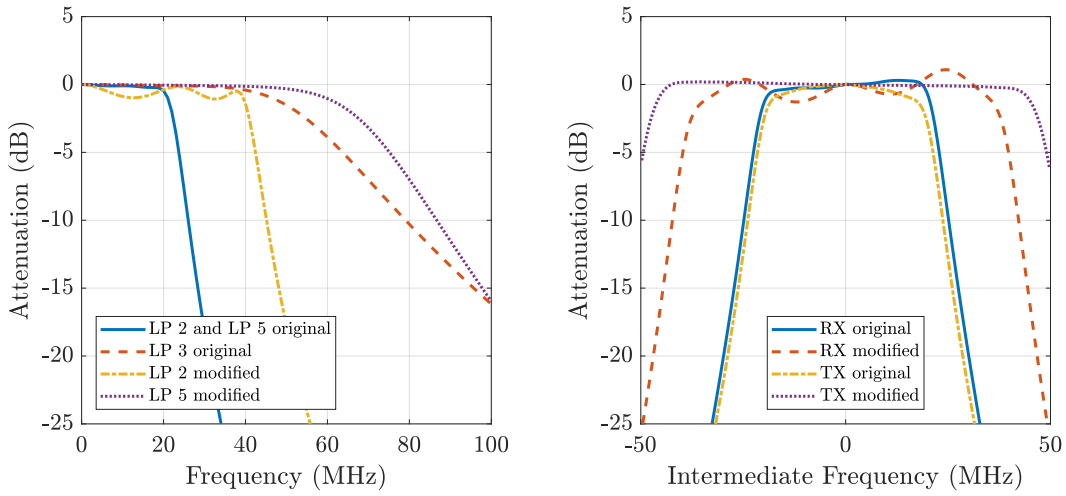
Figure 3.3: Photo of the modified SDR

diagram shown in Figure 3.2. Furthermore, fig. 3.3 shows a photo of the SDR. Section 3.2.1 discusses the hardware modification to share a common LO between TX and RX, such that the phasenoise in the demodulation process can be reduced. Section 3.2.2 shows how the available bandwidth of the SDR was enhanced by modifying the baseband filters in order to support broadband ranging signals. The hardware modifications of the testbed are also discussed in [37].

Another beneficial hardware modification would be an active carrier cancellation. It was omitted as it requires a redesign of the whole RF frontend. In section 6.3 a manual carrier cancellation is shown and the benefits are discussed.

3.2.1 Phase Coherence

One important fact of backscatter communication is that the TX and the RX are operated on the same frequency during ($T \Rightarrow R$) communication. The used SDR uses two separate synthesizers for generation of the LOs for the modulator and demodulator. This hardware design introduces additional phasenoise which leads to a performance degradation, especially for the demodulation of the EPC ($T \Rightarrow R$) communication. This issue was already discovered and discussed during the previously conducted diploma thesis [35] and will only be shortly summarized here.



(a) simulated (b) measured

Figure 3.4: Frequency responses of the baseband filters

The LO signals were made accessible at the backplate of the SDR. Therefore, the circuits between the TX synthesizer and the modulator as well as the connection between the RX synthesizer and the demodulator were separated. To access these signals, RF cables were attached and made accessible at the back of the housing of the SDR. This enables maximum flexibility, as several configurations can be realized. For example, one LO output can be used as the LO input for both modulators by using an RF power splitter. Also, a single LO can be distributed to multiple units, which can be used to build coherent MIMO setups. In chapter 6, applications of this setup will be shown.

3.2.2 Maximizing the Available Bandwidth

The chosen SDR utilizes an ADC with 14 bit resolution and a sampling rate of 100 MSamples/s. The 16 bit DAC is operated with an input data rate of 100 MSamples/s and an internal interpolation filter is used such that the output sampling rate is 400 MSamples/s. Hence, the aliasing free range in the baseband for transmission and reception is 50 MHz and 200 MHz, respectively. For suppression of aliasing products, the baseband filters (*LP 2*, *LP 3*, and *LP 5* (comp. fig. 3.2)) are used.

Simulations of the original lumped elements filters showed that the 3 dB corner frequency of *LP 2* and *LP 5* are 22.7 MHz, and 56.8 MHz for *LP 3*. Therefore, these filters limit the available bandwidth far below the maximum aliasing free bandwidth. If the provided software framework of the SDR is used, the available

sample rate is limited to 50 MHz due to the limited bandwidth of the Ethernet connection. Therefore, the design choice of the manufacturer to limit the analog baseband bandwidth to ≈ 25 MHz makes sense.

In section 2.3 it was shown that more bandwidth enables a better separation of multipath, hence, the goal of the design of the testbed is to utilize the maximum available bandwidth. Apparently *LP 2* and *LP 5* unnecessarily limit the bandwidth, so they were reworked.

For *LP 2* a fifth order lumped element lowpass filter with a Chebyshev response was designed. The filter is designed such that it has a 3 dB cut-off frequency of 40 MHz and 1 dB passband ripple. The large ripple is acceptable as it increases the steepness of the passband to stopband transition of the filter, and it can be compensated in post processing. The requirements on the antialiasing filter of the TX path are not as stringent as for the RX path, since the sampling rate of the DAC is 400 MHz. Hence, for *LP 5* a maximally flat filter with a 3 dB cut-off frequency of 70 MHz was designed. Figure 3.4a shows the simulated responses of the baseband filters prior and after the modification. Figure 3.4b shows the measured baseband filter response of the TX and RX using an LO frequency of 865.7 MHz.

3.2.3 Removal of the Diversity Path

The SDR can be operated with only one antenna in a half duplex mode. For this purpose, the *TX/RX* port of the SDR can be switched between a transmitting and a receiving mode by the switches *SW 2* and *SW 3*. *LNA 3* was removed since the half duplex mode is not needed for the intended application and a negative influence of the coupling between TX and RX via the finite isolation of the used switches could not be ruled out.

Chapter 4

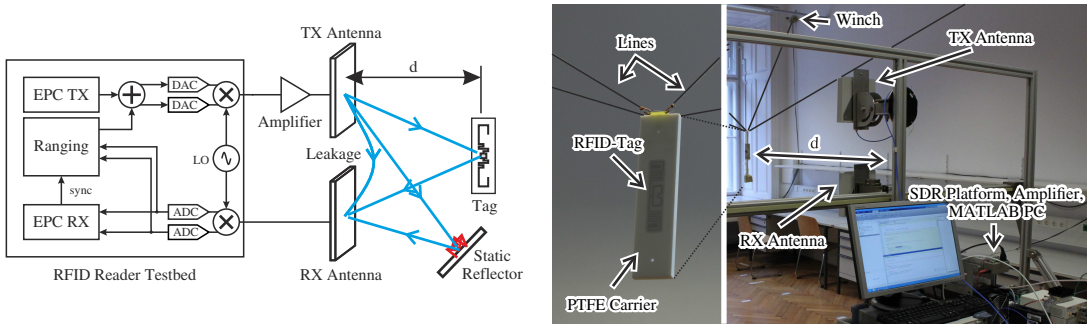
Measurement Setup and Results of the ToF based Ranging

The SDR based localization test platform shown in chapter 3 is used to evaluate the performance of the broadband ranging method (chapter 2). Within this chapter, some of the measurements are discussed which were conducted during the research project Real-time localization for flexible production environments (REFlex). Section 4.1 introduces the measurement setup used and in section 4.2 two exemplary measurements are discussed.

4.1 Measurement Setup

The measurements are conducted in a large empty office environment. A block diagram and a photograph of the measurement system are shown in fig. 4.1a and fig. 4.1b, respectively. The SDR testbed was connected to two *Huber&Suhner SPA-8090/78/8/0/V* patch antennas mounted on a metal frame, hence a bistatic scenario is investigated. The transmit antenna is placed fixed in the middle of the room at a height of 2 m, whereas the receive antenna is placed on a linear axis at a height of 1.45 m.

To provide repeatable measurements with a high spatial resolution, an automatic tag positioning system was built. Reflections of the structure of the positioner are prevented by choosing a setup with four corner mounted stepper-motor winches, high tensile strength lines, and a suspended tag (mounted on a carrier). By coordinated control of the line length between the tag and the winches, the tag can be moved inside a measurement area of 4×4.5 m and at a height up to 2.5 m above the floor.



(a) Block diagram

(b) Photo of the used RFID tag and the reader testbed

Figure 4.1: Measurement system used for evaluation of the broadband ranging system

To allow different RFID tags to be investigated with the tag positioner, the tags are mounted on carriers, which are connected to the lines by little hooks. Since the resonance frequency of an RFID tag depends on the material where the tag is attached to, they are optimized for the intended application. Therefore, to get a reasonable performance the dielectric properties of the carrier have to be similar to the targeted application of the tag design (see also Section 5.4.1).

4.2 Ranging Results in the UHF Band

Several measurement campaigns were conducted of which two are exemplarily presented here. The first measurement is a linear sweep of the tag in boresight of the interrogator with a high spatial resolution, which is also presented in [38]. The second measurement is a 2D spatial sweep across the whole measurement area at a common height.

4.2.1 High Spatial Resolution Linear Sweep

In the following, a high spatial resolution linear sweep is discussed. The tag used for this measurement is a *NXP Semiconductor N.V. UCODE 7* tag optimized for placement on garments. Drawings of this tag and a discussion of its backscattering properties can be found in section 5.4. It was placed onto a 165×40×10 mm sized polytetrafluoroethylene (PTFE) block. This material was chosen as its dielectric properties almost resemble the properties of garments, for which the tag was designed.

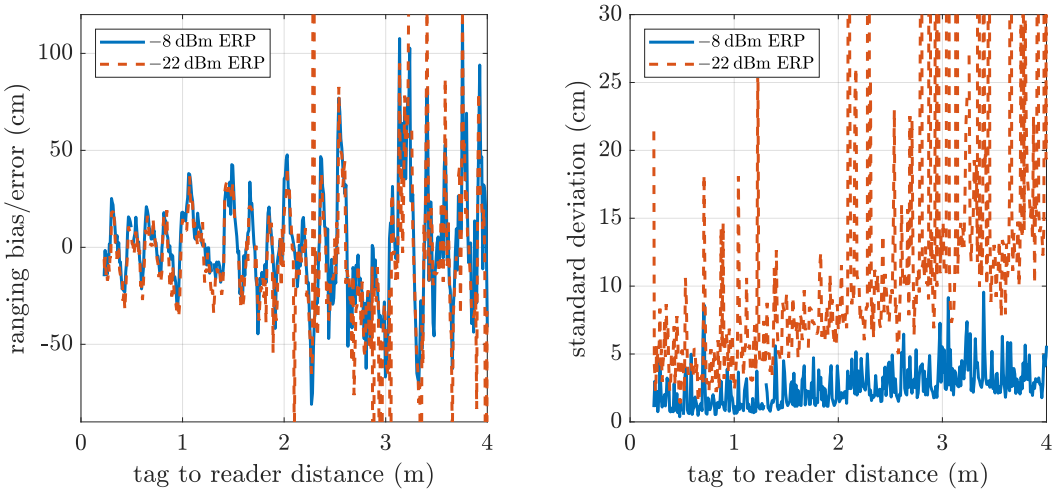


Figure 4.2: Ranging bias and sample standard deviation of the linear sweep measured with −8 dBm and −22 dBm ranging signal power

The tag was positioned in a straight line in front of the interrogator and moved from 0.1 m to 4 m in 1 cm steps. At each position, the tag was queried 200 times and thereby ranged with the method shown in chapter 2. A 255 bit long MLS sequence with a chip rate of 25 MHz is used as the ranging signal. For the ranging, the EPC response of the $(T \Rightarrow R)$ communication is used. To maximize the averaging time, Miller 8 modulation with a BLF of 40 kHz was used. Hence, the coherent averaging process is performed over 2128 subbits and the averaging time is 21.7 ms.

The EPC CW carrier was transmitted with an ERP of 33 dBm which fits the ETSI spectral transmit mask [13]. To show a comparison between ranging with different powerlevels the ranging signal was transmitted with −8 dBm, matching the requirements of the EPC standard [2], and with −22 dBm which complies to the ETSI spectral transmit mask [13].

While the frequency response of the testbed was compensated, the electrical length of the cables between SDR and antennas was not measured, and therefore not compensated. To account for this arbitrary distance shift, the mean distance offset of the measurements in the range 0.1 m to 1 m was subtracted from the ranging results. For the following 2D sweep, the cables were also included into the compensation of the frequency response of the testbed, which resulted in a higher mean offset stemming from the groupdelay of the tag. At the time where the measurement of the linear sweep was conducted, this issue was not considered by me.

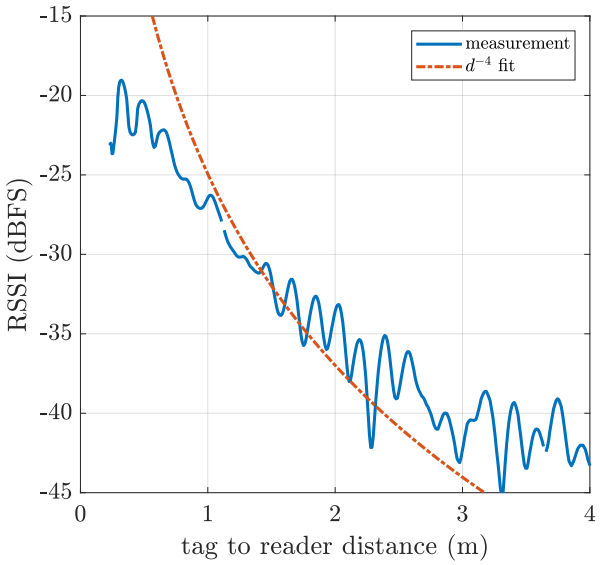


Figure 4.3: RSSI of the linear sweep

Figure 4.2 shows the mean measured ranging offset and the sample standard deviation of the measurements. It can be observed that the ranging bias in the range 0.1 m to 1.8 m is below 40 cm. In the remaining range the error is mostly below ±1 m with a few outliers. The ranging bias most likely stems from inseparable multipath components already discussed in section 2.3. The ranging offset measurements conducted with the two different ranging signal powers match very well, which shows that variation of the bias is not due to noise.

The sample standard deviation of the 200 measurements at each position increases with the distance between reader and tag. While the ranging offset stems mainly from the multipath distortion, the increased standard deviation is due to noise. Comparing the two measurements it can be observed that the standard deviation is higher if a lower ranging signal power is used. The main limiting factor of the SNR of the measurement is the self interference of the CW signal used to power the tag, which is present at the receiver due to the coupling of the transmit to the receive antenna. Therefore, a high input attenuation has to be set so that the SDR is not overloaded, which leads to a high overall noise figure in the order of 23 dB. An active carrier cancellation, as it is used in many COTS RFID readers, can suppress this leakage, and thereby, reduce the effective noise figure. Section 6.3 will present an active carrier cancellation built around the SDR testbench, which shows that the performance can be enhanced.

The FPGA implementation also provides an RSSI indicator derived from the magnitude of the narrowband EPC communication. The distance dependency

of the RSSI is shown in fig. 4.3. A d^{-4} dependence of the RSSI is theoretically expected for a LoS backscatter two-way channel with constant ΔRCS of the tag, and so the measured values where tried to be fitted with a d^{-4} function. A ripple of the measurement results can be observed, which stems from small scale fading. Furthermore, it can be seen that the measurement is non-monotonic, and so it is not possible to get an unambiguous ranging result from the measurement. It can be also seen that the RSSI does not fit well to the d^{-4} model, which is most likely due to the nonlinear behavior of the ΔRCS, discussed in section 5.4.3.

4.2.2 Two Dimensional Area Sweep

Another measurement was performed over the full measurement area available by the tag positioning system. This measurement had to be performed with less spatial resolution (10 cm), to keep the time needed for the measurement reasonable. In contrast to the previous measurement, the delays of the cables between the SDR and the antennas were measured and removed from the measurement results. Hence, the measured ranging distance only includes the delays introduced by the RF channel, the antennas of the interrogator, and the antenna of the tag. Furthermore, the measurement was performed with the REFlex tag introduced in section 5.4.1 on a block of *Rohacell*®[1]. A 511 bit long MLS sequence with a chip rate of 50 MHz transmitted with an ERP of −8 dBm was used as the ranging signal.

Figure 4.4 shows the measurement result taken with the TX and RX antenna marked with a red square and a red cross, respectively. Measurement results within the range of the colorbar (2.1 m to 3.1 m) depicted below the figure are shown as filled circles in the respective color. Results outside this range (outliers) are marked with "+" signs in yellow or blue. Points without any marker indicate that at this position no measurement was possible, because most likely the tag had insufficient power to operate.

Again, it can be seen that measurement results close to the antenna show less offset variation compared to results farther away. Possibly, this behavior can be explained by the fact that measurements taken closer to the antennas have a larger relative magnitude difference between the ground reflection and the LoS component due to the directional properties of the antennas. Therefore, a smaller influence of the ground reflection onto the ranging result can be expected.

The mean offset of about 2.6 m stems from the additional group delay of the RFID tag, the TX, and the RX antenna of the interrogator, as discussed in chapter 5.

[1] *Rohacell*® is a polymethacrylimide structural foam whose dielectric properties are almost like air (Rohacell 31 IG $\varepsilon = 1.05, \tan\delta = 0.0003$ measured at 2.5 GHz).

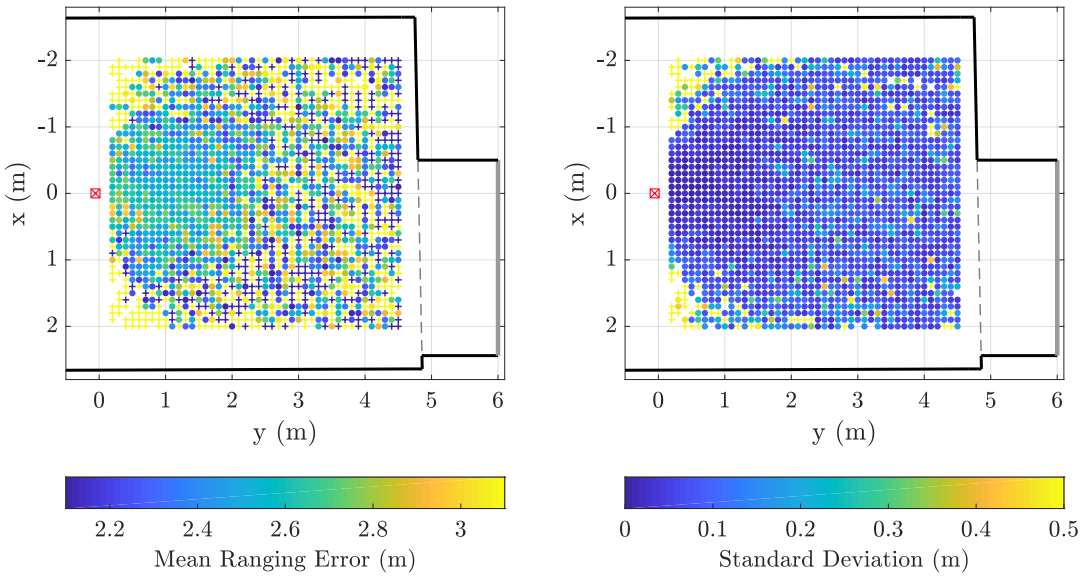


Figure 4.4: Ranging bias and sample standard deviation of the REFlex tag measured in the UHF band

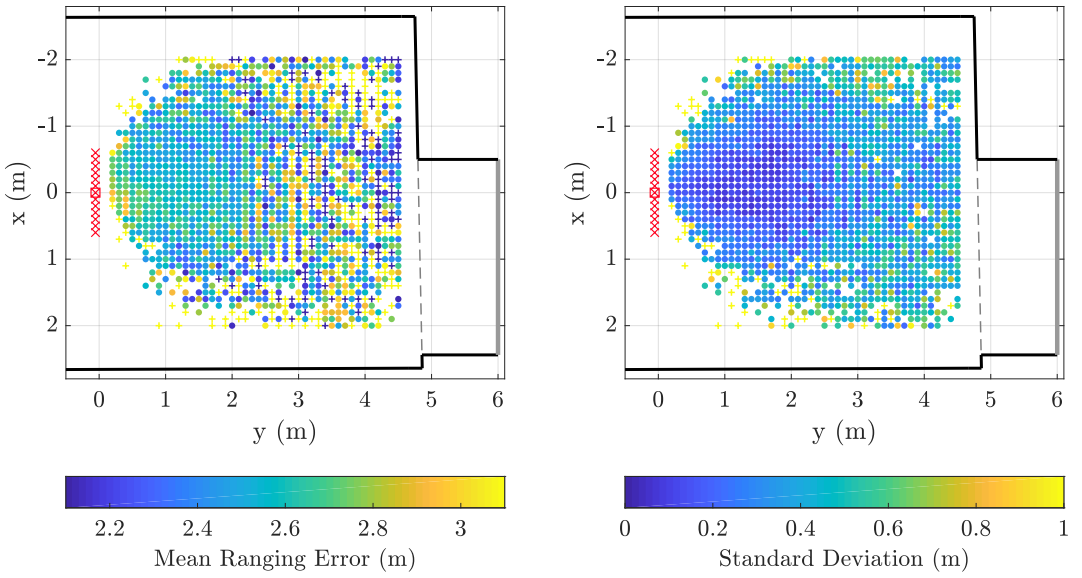


Figure 4.5: Ranging error and standard deviation averaged over the "virtual" antenna array

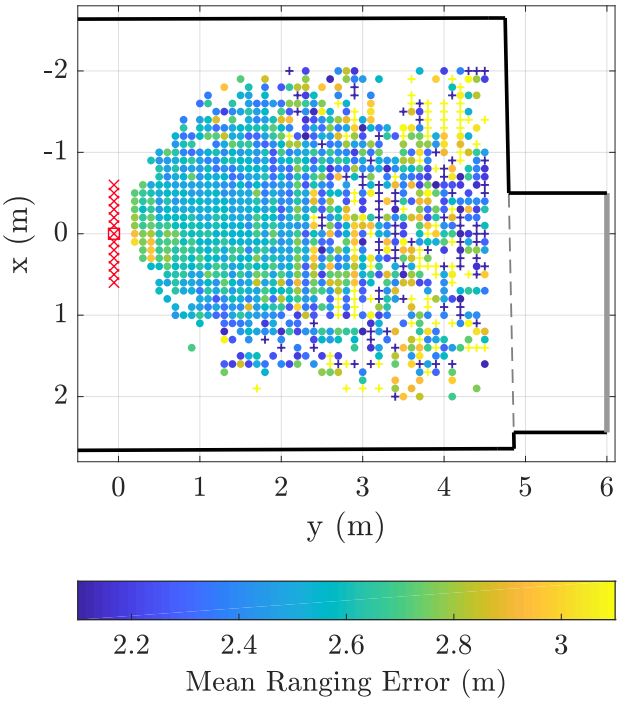


Figure 4.6: Measurement results averaged over the "virtual" RX antenna array, where results with a sample standard deviation above 0.5 m are omitted

The RX antenna was mounted on a linear axis, and therefore, it was possible to perform measurements with a "virtual" antenna array as the channel is expected to remain static during the measurements. The RX antenna was positioned at 13 positions with a spacing of 10 cm. Figure 4.5 shows the ranging error of a joint distance estimation over all RX antenna positions, derived by averaging the individual results. The mean ranging offset was calculated by subtracting the distance between the TX antenna and the middle of the RX antenna array from the averaged results. Only measurements where the tag was successfully interrogated 200 times from each RX antenna position were displayed.

It can be seen that the area with a relativly constant ranging offset is enlarged by the averaging of the individual results of the antennas. This behavior is expected as the multipath scenario for each antenna position is different, and thereby the shift of the ranging result is somehow uncorrelated. This method is not optimum by any means and it can be suspected that by utilizing array processing and enhanced signal processing methods including the properties of the dense multipath channel the ranging error can be significantly reduced [39], [40].

Furthermore, an attempt was made to find an indicator of reliability of the measurement results. The sample standard deviation shows if the individual measurements from multiple antenna positions are largely spread. Within the area in front of the interrogator it stays below 50 cm while in areas with large multipath distortions it seems to increase. The standard deviation of the measurements from multiple antennas is almost an order of magnitude larger than the standard deviation of a single antenna measurement due to noise. In fig. 4.6 all measurements with a sample standard deviation over 50 cm were removed. Thereby, some of the outliers, especially with a large distance to the interrogator, were removed. However, many outliers which are largely biased towards the interrogator remain.

Chapter 5

Influence of the RFID Tag onto the Ranging Performance

In chapter 2, the broadband ToF based ranging method was introduced. The measured delta channel impulse response, which is used to determine the ToF, is the convolution of the downlink h_{dl} with the delta impulse response of the tag h^{Δ}_{tag} and the uplink channel impulse response h_{ul}. The down- and up-link channel impulse responses are properties of the RF channel between reader and tag, therefore, they carry the desired ranging information. In the preceding chapters, the delta tag response h^{Δ}_{tag} was assumed as an ideal Dirac delta function with zero time offset. This chapter shows that this assumption does not hold true for normal COTS UHF RFID tags due to their narrowband antenna structure. Furthermore, we will discuss to what extend the delta impulse response of the tag distorts the measurement result if the correlation based method is applied without corrections. A manuscript summarizing the findings presented in this chapter is accepted to be published [16].

A negative influence onto the broadband ranging result originating from the non-ideal delta impulse response is expected, as the ranging method uses a significantly larger bandwidth compared to the narrowband identification. A common type for COTS tag antennas is the meandered dipole, which is a narrowband design. Distributed matching circuits like the T-match or inductive coupled loop [41] are used to provide a reasonable conjugate match to the mostly capacitive input impedance of the RFID IC. The dipole and the matching structure have two independent design frequencies. Tag designers use these in a way that an acceptable performance is achieved over the whole band of interest, e.g., from 865.6 MHz to 928 MHz for operation among the different regulatory regions worldwide. However, for the studied broadband localization system, the utilized frequency range

of the ranging signals (see section 2.2) is much wider than the frequency range for worldwide operation.

In order to analyze and correct for the influence of the tag, the delta impulse response h_{tag}^{Δ} has to be known. The broadband ToF based ranging method for RFID tags is relatively new and thus not covered extensively in literature. Most of the available publications regarding measuring and simulating the RF properties of UHF RFID tags focus on determination and improving the reading range for identification purposes, e.g., [5], [41], [42]. The broadband behavior of the ΔRCS and especially the behavior of the RF phase is of minor importance for the normal identification operation, and therefore rarely discussed in literature. However, for the introduced broadband ranging method it is of major importance and will be discussed in detail here.

Since the bandwidth of the ranging signal is finite, the knowledge of the transfer function of the ΔRCS in the utilized frequency band is sufficient. The evaluation of the phase of the ΔRCS is not available as a COTS solution in usual simulation environments, nor in usual measurement systems [43]. A measurement system was developed, which is able to measure the ΔRCS in magnitude and phase for backscatter based tags in an anechoic chamber in the course of a master thesis [6], [44]. It is able to measure in the UHF frequency band as well as in the ISM bands at 2.45 GHz and 5.8 GHz. Measurement results from this system will be used as a comparison to the results gathered by the simulations in section 5.4.

Section 5.1 gives an overview of common performance figures for EPC RFID tags. The subsequent section 5.2 focuses on showing a comprehensive mathematical definition of the ΔRCS. Section 5.3 presents a method for simulation of the frequency dependent ΔRCS of an RFID tag. Thereby, the ΔRCS is calculated from the farfield pattern of the antenna of the tag, the scattering-parameters (S-parameters) of the antenna ports, and the S-parameters of the tag IC in the two distinct backscatter states. Section 5.4 discusses the result of a simulations of a COTS RFID tag with a special focus on the implications onto the ranging performance. Furthermore, a special tag is presented which uses two separate frequency bands for identification and localization.

5.1 Commonly Used Performance Figures of EPC RFID Tags

For EPC UHF RFID tags, the read range is defined as a performance parameter of the tag and the evaluation of it is described by GS1 [45]. The measurement of the read range is split into two parts, the forward read range and the backscatter range, also called forward and backward range, respectively. To allow a comparison between different tags, all tests have to be conducted within a controlled

RF environment, since multipath scenarios would prevent comparable outcomes. The RF environment is specified by a minimum reflection attenuation of the floor, walls, and ceiling. Additionally, a maximum ambient RF noise level is specified.

The forward range is limited by the fact that the chip of the tag has to be supplied with sufficient power, such that the chip is able to operate. This range depends on many factors, e.g., the ERP of the CW signal transmitted by the reader in direction to the tag, the gain of the antenna of the tag, the polarization mismatch, the mismatch between the antenna of the tag and the RFID IC, and the minimum operating power of the RFID IC. GS1 has specified an LoS scenario with a 35 dBm ERP excitation for evaluation of the forward range. This provides a vivid figure of merit which enables easy comparison of different tags also for customers without RF know-how. However, in a real scenario this range might be different due to the prior mentioned factors and in particular due to fading caused by multipath. In a technical context, the best suited quantity probably would be the required field strength at the tag needed for operation. But this quantity is less descriptive for the general audience.

The backscatter range is limited by the ability of the reader to demodulate the backscatter modulated signal from the tag. In an LoS scenario this depends on the ERP of the CW signal transmitted by the reader in direction to the tag, the ΔRCS of the tag, the gain of the RX antenna of the reader, and the sensitivity of the reader. GS1 defines a test to determine the ΔRCS of the tag. The result of this test is used to calculate the backscatter range in meters. Thereby, a standard reader with a sensitivity of -70 dBm and a linearly polarized receive antenna with 5 dBi is assumed. Then, the ERP of the CW transmitted by the reader is adjusted to the sensitivity limit of the tag. As well as the forward range also the backscatter range is calculated in meters to make the quantity more descriptive.

Scientific publications, e.g., [46]–[48], normally use the ΔRCS given in square meters instead of the backscatter range specified by GS1. The two quantities can be translated by

$$r_{backscatter} = \sqrt[4]{\frac{10^{11}\,\lambda^2\,\Delta\sigma}{(4\pi)^3}}\ . \tag{5.1}$$

where λ is the wave length, $\Delta\sigma$ is the delta radar cross section of the tag, and the term 10^{11} represents the assumed scenario presented previously.

Furthermore, one can calculate the power of the backscatter modulated signal in a monostatic scenario by evaluation of the radar equation

$$P_{rx} = \frac{P_{tx}\,G_{reader}^2\,\lambda^2\,\Delta\sigma}{(4\pi)^3\,r^2}. \tag{5.2}$$

where P_{rx} is the received power, P_{tx} is the power of the CW signal transmitted by the reader to power the tag, r the distance between the antenna of the interrogator and the tag, and G_{reader} is the gain of the antenna of the interrogator.

5.2 Definition of the Complex Valued Delta Radar Cross Section

For the evaluation of the influence of the tag onto the ranging accuracy it is necessary to derive the relationship between the transmitted and the received ranging signal for a backscattering scenario. For simplification without any loss of information, this relationship will be shown in frequency domain using complex notation.

A prerequisite for the derivation is that some quantities which are normally only characterized just by magnitude become accessible in magnitude and phase. One example is the gain of an antenna. For narrowband communication systems, the gain is normally used as a factor to derive the received power P_{rx} in a communication system using the Friis transmission equation [49]

$$P_{rx} = P_{tx} G_{tx} \left(\frac{\lambda}{4\pi d} \right)^2 G_{rx} \tag{5.3}$$

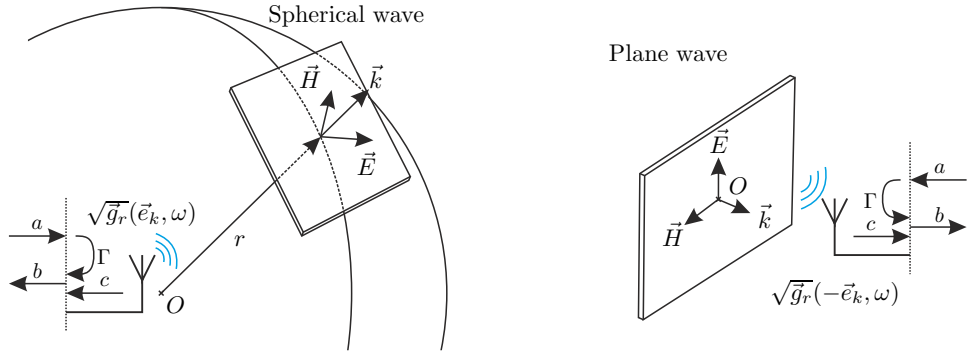
where P_{tx} is the transmitted power, λ is the wavelength, d is the distance between the two antennas, and G_{tx} and G_{rx} are the gains associated with the transmit and receive antenna, respectively. In narrowband systems the phase shift introduced by the RF link can be neglected in many applications as it is almost constant with respect to the utilized bandwidth. However, for the researched wideband ranging system, the frequency dependent phaseshift is of major importance as it carries the ranging information. In order to characterize the phase shift introduced by the antenna, we define the complex valued square root[1] of the realized[2] gain as

$$\sqrt{\vec{g}_r}(\vec{e}_k, \omega) := \lim_{r \to \infty} \frac{\sqrt{4\pi r^2}\, e^{jkr}}{\sqrt{Z}} \frac{\vec{E}(r, \vec{e}_k, \omega)}{a(\omega)} \tag{5.4}$$

where r is the distance from the phase center of the antenna to the position where the electric field strength $\vec{E}(r, \vec{e}_k, \omega)$ is evaluated, $a(\omega)$ is the normalized power wave incident to the antenna port, Z the impedance of the medium where

[1] Using the square root is necessary as the gain is a factor associated with power, and would therefore introduce a π phase ambiguity for the signal.

[2] The IEEE standard for definitions of terms for antennas [50] excludes the losses due to impedance mismatch on the terminals of the antenna from the gain. However, for further considerations it is simpler to use the realized gain, which also includes the mismatch losses.



(a) transmitting antenna (b) receiving antenna

Figure 5.1: Schematic representation of a transmitting (a) and a receiving (b) antenna indicating the farfield quantities as well as the normalized power waves on the antenna interface.

the plane wave is travelling[3], and the wave vector $\vec{k}$ which can be split into its magnitude k and direction $\vec{e}_k$. The limit operator indicates that $\sqrt{\vec{g}_r}$ has to be measured in the farfield. In order to be able to describe plane waves with different polarization states, $\sqrt{\vec{g}_r}$ is a column vector with an arbitrary chosen orthogonal polarization basis.

Figure 5.1 shows a transmitting and a receiving antenna in combination with the associated electromagnetic (EM) fields. For a transmitting antenna the EM field associated with the farfield is a spherical wave which can be represented by

$$\left\{ \begin{array}{c} \vec{E}(r,\vec{e}_k,\omega) \\ \vec{H}(r,\vec{e}_k,\omega) \end{array} \right\} = \left\{ \begin{array}{c} \sqrt{Z}\sqrt{\vec{g}_r}(\vec{e}_k,\omega) \\ \frac{\vec{e}_k}{\sqrt{Z}} \times \sqrt{\vec{g}_r}(\vec{e}_k,\omega) \end{array} \right\} \frac{a(\omega)e^{-jkr}}{r}. \tag{5.5}$$

To characterize the receiving properties of an antenna we place the phase center O of an antenna into a region where prior to placing the antenna, a plane wave[4] characterized by an electric field $\vec{E}$ and a wave vector $\vec{k}$ was assumed. By using Lorentz reciprocity [51], [52], we can evaluate the normalized power wave c at the connector of the antenna due to the incident wave by

$$c(\omega) = \frac{\lambda \sqrt{\vec{g}_r}^T(-\vec{e}_k,\omega)\,\vec{E}(\omega)}{\sqrt{4\pi Z}}\, e^{-j\frac{\pi}{2}} \tag{5.6}$$

[3]The characteristic wave impedance of vacuum Z_0 equals $\mu_0 c_0 \approx 376.7\,\Omega$.

[4]For a plane wave $\vec{E}$, $\vec{k}$, and the magnetic field strength $\vec{H}$ are orthogonal. Furthermore, the magnitude of $\vec{E}$ and $\vec{H}$ are related by the wave impedance $|\vec{E}| = |\vec{H}|Z$. Therefore, the wave is uniquely defined by two of these quantities, in our case $\vec{E}$ and $\vec{k}$.

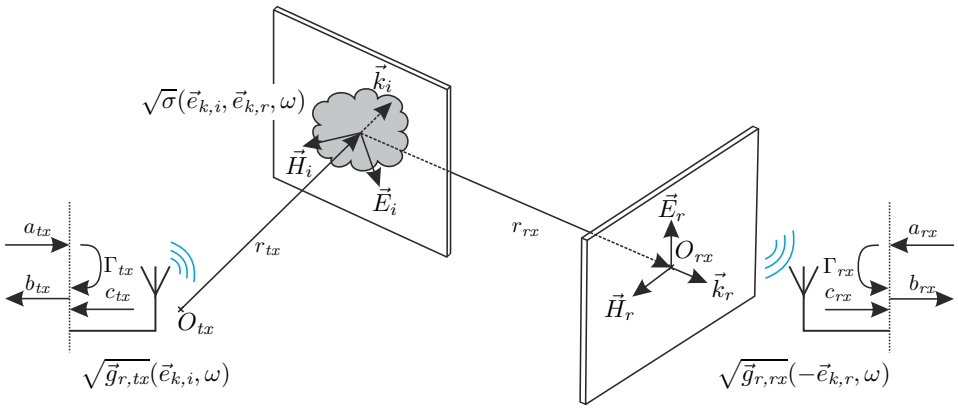


Figure 5.2: Schematic representation of a bistatic radar signal path indicating the farfield quantities as well as the normalized power waves on the antenna interfaces.

The next quantity which has to be defined is the complex valued square root matrix of the radar cross section (RCS). The RCS is a measure for how much power is scattered by an object due to an incident plane wave. This quantity is mostly used for evaluation of the visibility of radar targets. One application example is that the shape of military vehicles is often optimized for a low RCS, such that they are harder to detect by radar systems. Just like the normally used definition of the gain, one is normally interested only in the power of the reflected signal. For evaluation of the ranging accuracy, we need to have phase information of the reflected wave as well. Therefore, it is necessary to define the complex valued square root matrix of the RCS of an reflecting object as

$$\sqrt{\sigma}(\vec{e}_{k,i}, \vec{e}_{k,r}, \omega)\, \vec{E}_i(\vec{e}_{k,i}, \omega) = \lim_{r\to\infty} \sqrt{4\pi r^2}\, e^{jkr}\, \vec{E}_r(\vec{e}_{k,r}, r, \omega). \tag{5.7}$$

where $\vec{E}_i(\vec{e}_{k,i}, \omega)$ is the electric field strength of the incident plane wave, r the distance of the evaluation of the electric field $\vec{E}_r(\vec{e}_{k,r}, r, \omega)$ of the reflected spherical wave, and $\vec{e}_{k,i}$ $\vec{e}_{k,r}$ are the unit vectors pointing in direction of the incident plane wave and the reflected spherical wave, respectively.

We can now combine the prior definitions and derive the transfer function for an LoS reflection scenario as it is shown in fig. 5.2. The received normalized

power wave can be found by

$$c_{rx}(\omega) = \frac{\lambda \sqrt{g_{r,rx}}^T(-\vec{e}_{k,r},\omega)\, e^{-j\frac{\pi}{2}}}{\sqrt{4\pi Z}} \frac{\sqrt{\sigma}(\vec{e}_{k,i},\vec{e}_{k,r},\omega)\, e^{-jkr_{rx}}}{\sqrt{4\pi} r_{rx}} \frac{\sqrt{g_{r,tx}}(\vec{e}_{k,i},\omega)\sqrt{Z}\, e^{-jkr_{tx}}}{\sqrt{4\pi}\, r_{tx}} a_{tx}(\omega). \quad (5.8)$$

We have now derived the received normalized power wave due to a reflection over a single LoS scenario. This formulation can also be used to model the channel response in multipath environments by using superposition of all discrete paths between the transmitter and receiver antenna. Channel models derived by this method are called ray tracing models. The disadvantages of ray tracing models are that the computational complexity increases exponentially with the number of reflections considered and that the inclusion of diffuse scattering and diffraction is very challenging [4].

In RFID applications, one is normally interested in the backscatter modulated signal of the RFID tag. Equation (5.8) can be used to derive this quantity by replacing the square root of the RCS matrix $\sqrt{\sigma}(\vec{e}_{k,i},\vec{e}_{k,r},\omega)$ by the square root of the ΔRCS matrix $\sqrt{\Delta\sigma}(\vec{e}_{k,i},\vec{e}_{k,r},\omega)$.

For many applications the use of the scalar ΔRCS is sufficient, e.g., for calculation of the power of the backscatter modulated tag response at the receiving antenna (see eq. (5.2)). This scalar ΔRCS can be calculated from the square root of the ΔRCS matrix as well by using

$$\Delta\sigma(\vec{e}_{k,i},\vec{e}_{k,r},\vec{e}_{pol,i},\vec{e}_{pol,r},\omega) = |(\vec{e}_{pol,r})^T \sqrt{\Delta\sigma}(\vec{e}_{k,i},\vec{e}_{k,r},\omega)\, \vec{e}_{pol,i}|^2 \quad (5.9)$$

where $\vec{e}_{pol,i}$ and $\vec{e}_{pol,r}$ are unit vectors describing the polarization of the considered incident and reflected waves, respectively.

5.3 Simulation of the Delta Radar Cross Section

EM simulators are widely used tooles for rapid prototyping and for evaluation of the impact of several environmental parameters. In the following section the applicability of *CST Studio Suite®* for simulation of the ΔRCS will be shown. Furthermore, a systematical approach to derive the ΔRCS from the knowledge of the complex valued gain pattern and the impedance of the RFID chip will be presented.

The first simulation was performed by using the recommended simulation setup for determination of the RCS. Thereby, the farfield radiation due to a planar incident wave was determined. In order to evaluate the ΔRCS of the tag, two simulations with different lumped elements (the equivalent circuit models

for the absorbing and reflecting state) connected to the antenna structure were performed. The ΔRCS was calculated in post-processing by

$$\Delta\sigma(\vec{e}_{k,i}, \vec{e}_{k,r}, \vec{e}_{pol,i}, \vec{e}_{pol,r}, \omega) = 4\pi \lim_{r\to\infty} r^2 \frac{\|(\vec{e}_{pol,r})^T \Delta\vec{E}_r(\vec{e}_{k,r}, r, \omega)\|^2}{\|\vec{E}_i(\vec{e}_{k,i}, \vec{e}_{pol,i}, \omega)\|^2} \tag{5.10}$$

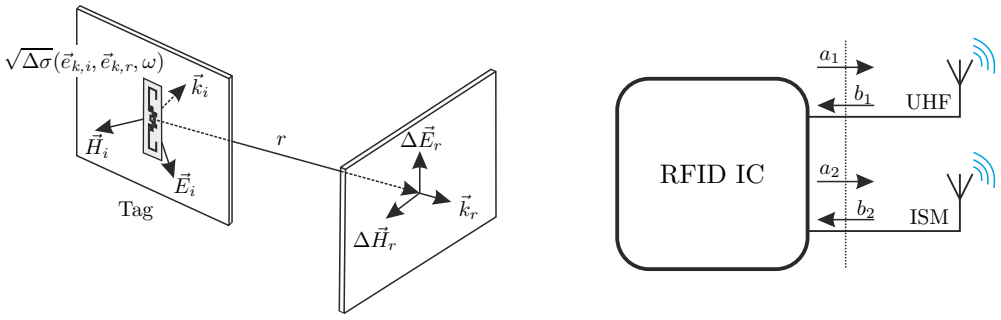
with

$$\Delta\vec{E}_r = \vec{E}_{r,reflect} - \vec{E}_{r,absorb}. \tag{5.11}$$

This approach has two major disadvantages. First, for a sweep over different incident directions the computational expensive EM simulation has to be performed for each incident direction and for each considered incident polarization. Second, within *CST Studio Suite®* it is not possible to connect an arbitrary frequency dependent load to the port of the antenna in a straight forward manner. Therefore, one is limited to a simple resistor, inductor, and capacitor serial or parallel equivalent circuit model for the chip impedance.

A more computationally efficient way to determine the ΔRCS by using only one farfield simulation per antenna port was found by systematic evaluation of the antenna in terms of generalized S-parameters. There are many ways to discuss the scattering of an antenna connected to an arbitrary load, e.g., [53]–[55]. In this work, the scattered field $\vec{E}_r$ is split into the field produced by a matched antenna and the radiated field due to an incident power wave at the discrete port of the antenna. The determination of the scattered field of the matched antenna requires a separate EM simulation for each incident direction and incident polarization of interest as we discussed beforehand. However, for the evaluation of the ΔRCS this quantity is not needed as it cancels in the calculation anyway. The radiated EM field caused by an incident normalized power wave on the antenna connector can be determined from a single antenna gain simulation. By using reciprocity, one can also determine the normalized powerwave at the antenna connector due to an incident plane wave onto the antenna from the former simulation. Therefore, one EM simulation is sufficient for the evaluation of the bi-static ΔRCS.

Figure 5.3 shows the two "interfaces" of an RFID tag antenna. Figure 5.3a shows the incident and reflected wave while fig. 5.3b shows the connection of the antenna to the attached RFID IC. While usual tags only have a single antenna optimized for operation in the UHF frequency range, the following formulation can be easily extended to an RFID tag with multiple antennas. Since this work also investigates the benefits of a two frequency tag with two separated antennas for ranging and identification, the following derivation will be shown for two antenna ports.



(a) Illustration showing the incident and reflected wave for characterization of the ΔRCS of an RFID tag

(b) Block diagram indicating the reference plane separating the RFID IC from the antenna

Figure 5.3: Illustration of the interfaces of an RFID tag used for simulation

The relationship between the incident and transmitted power waves of the antenna from the farfield and from the discrete ports can be described by

$$\begin{bmatrix} \vec{E}_r(\vec{e}_{k,r}, r, \omega) \\ \vec{b}(\omega) \end{bmatrix} = \begin{bmatrix} C_s(\vec{e}_{k,i}, \vec{e}_{k,r}, r, \omega) & C_r(\vec{e}_{k,r}, r, \omega) \\ C_i(\vec{e}_{k,i}, \omega) & S_{Ant}(\omega) \end{bmatrix} \begin{bmatrix} \vec{E}_i(\vec{e}_{k,i}, \omega) \\ \vec{a}(\omega) \end{bmatrix}, \tag{5.12}$$

where the incident EM field $\vec{E}_i(\vec{e}_{k,i}, \omega)$ is assumed as a plane wave from spatial direction $\vec{e}_{k,i}$ (farfield condition satisfied). As the incident wave could have an arbitrary polarization, $\vec{E}_i$ is described as a vector with an arbitrary chosen orthogonal polarization base. The reflected wave $\vec{E}_r(\vec{e}_{k,r}, r, \omega)$ generally has also a spatial pattern. Therefore, the described relationship depends on the investigated spatial direction $\vec{e}_{k,r}$. The reflected wave is investigated in the farfield region with a field strength decreasing inversely proportional to the distance from the tag r. The incident and reflected power waves at the discrete antenna ports, named $\vec{a}$ and $\vec{b}$, are handled in terms of power waves and generalized S-parameters. These column vectors have a length equal to the number of the antenna ports. The matrix $C_s(\vec{e}_{k,i}, \vec{e}_{k,r}, r, \omega)$ describes the reflection of an incident plane wave, if all discrete ports of the antenna are terminated with the reference impedance. In order to determine this quantity, two separate RCS simulations for each incident direction of interest have to be carried out. However, this quantity cancels when the ΔRCS is calculated, which can be seen in eqs. (5.10) and (5.15). The matrix $C_r(\vec{e}_{k,r}, r, \omega)$ describes how a power wave incident onto the discrete antenna ports results in a transmitted plane wave of the tag in the farfield. This relationship is a direct result of the standard farfield simulations where the antenna ports are exited one after the other. The matrix $C_i(\vec{e}_{k,i}, \omega)$ describes how an incident plane

wave is transferred to the discrete antenna ports. This quantity can be calculated by utilizing the reciprocity between a transmitting and receiving antenna [56] by

$$C_i(\vec{e}_{k,i},\omega) = \lim_{r\to\infty} \frac{C_r(\vec{e}_{k,i},r,\omega)r\lambda}{Z} e^{j(kr-\frac{\pi}{2})}. \tag{5.13}$$

Therefore, it is also directly accessible from the farfield simulation data. Finally, the matrix S_{Ant} is the S-parameter matrix describing the reflection coefficients and coupling coefficients of the discrete antenna ports, which are also a direct result of the farfield simulations.

By knowing the S-parameters of the RFID IC $S_{RFID,IC}$, one can calculate the backscattered EM field of the antenna including an arbitrary load due to a incident plane wave by

$$\vec{E}_r = \left[C_s + C_r\left[S_{RFID,IC}^{-1} - S_{Ant}\right]^{-1}\right] C_i\vec{E}_i. \tag{5.14}$$

Therefore, it is possible to derive the bistatic ΔRCS of the tag by using eq. (5.10) with

$$\Delta\vec{E}_r = C_r\left[\left[S_{RFID,IC,reflect}^{-1} - S_{Ant}\right]^{-1} - \left[S_{RFID,IC,absorb}^{-1} - S_{Ant}\right]^{-1}\right] C_i\vec{E}_i \tag{5.15}$$

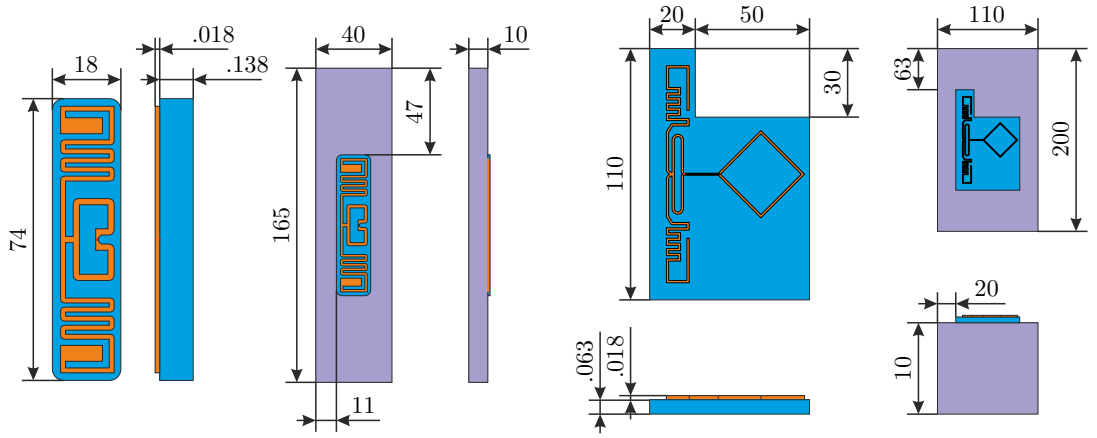
where $S_{RFID,IC,reflect}$ and $S_{RFID,IC,absorb}$ are the S-parameters of the IC of the RFID tag in the different backscatter modulation states.

5.4 Measurement and Simulation Results

In the following section the measurement results taken in an anechoic chamber and simulation results gathered by the previously shown method are presented. Section 5.4.1 introduces the RFID tags used in the simulations and the measurements. Section 5.4.2 provides details how the impedances of the RFID IC can be measured and also summarizes the impedance used for the simulations. Section 5.4.3 compares the measurements with the simulation results and shows the impact of the frequency response of the RFID tag onto the ranging accuracy, respectively.

5.4.1 Description of the analyzed RFID tags

The market for RFID tags is very versatile. For different applications, different antenna designs may be optimal. A commonly used design is the planar meandered dipole structure on adhesive stickers. The benefits are that mounting of the stickers is relatively simple, that the manufacturing process is cheap, and that the antenna pattern is relatively wide.



(a) UCODE 7 RFID tag (b) REFlex dual frequency RFID tag

Figure 5.4: Drawing of the two simulated, measured, and analyzed RFID tags; all dimensions are in mm

The research activities were mainly focused on two tags, the UCODE 7 based fashion tag and the REFlex tag. Drawings of both tags can be found in fig. 5.4. During the tests the tags were mounted on blocks (depicted in purple) such that they are operated on the targeted undergrounds. Their dimensions are provided in fig. 5.4.

The UCODE 7 fashion tags were provided by our industrial partner, unfortunately with very few additional informations alongside with the tags. For the simulations, the structure was manually measured and sketched, as the design data from the manufacturer was not accessible. The stack up is modeled by two layers: one conductive and one dielectric, since the actual stack up of the individual layers of the tag is not known nor their dielectric properties. The conductive structure is modeled as a copper sheet with a thickness of 18 µm. On top of this structure a dielectric sheet with a thickness of 138 µm and a relative permittivity of 3.5 is placed (see fig. 5.4a). This stack up does not exactly match the stack up of the examined tag, but it will be sufficient to derive qualitative analysis especially with regard to the expected ranging performance.

To provide the customer with the best reading range, the antenna design has to be matched to the material where the tag will be attached to. The UCODE 7 fashion tag is designed to be placed on garments. Since the resonance frequency of the antenna depends on the materials close to the tag, it was necessary to reproduce an environment almost equal to garments around the tag to get reasonable performance. Therefore, the tag was placed on a block of PTFE during the measurements ($\varepsilon_r \approx 2.1$).

The second tag investigated within this thesis was manufactured in a close cooperation with *NXP Semiconductor N.V.*. The main goal of this design is enhancing the ranging accuracy by using the 2.4 GHz ISM frequency band for ranging, while the EPC standard conformal communication is performed in the UHF band. The benefit for the quality of the received ranging signal is twofold. First, the ranging signal is well separated from the CW carrier which is used to supply the tag with power. This results in less stringent dynamic range requirements at the receiver (no blocking due to the strong CW). Second, the power of the transmitted ranging signal can be significantly increased since the allowed power in the ISM band [57] is higher compared to the UHF band [13].

To utilize theses benefits, a special RFID IC with two antenna interfaces was designed and manufactured. Antenna port 1 implements the standard conformal EPC UHF interface as it is available on normal RFID chips. The second antenna interface is connected to a modulation transistor for the ranging antenna which can be configured to different operation modes by setting the session flags[5] S2 and S3 of the tag. The operation modes are: modulation synchronous to the EPC modulation, square wave modulation with 30 kHz or 960 kHz, or switching the modulation transistor to a fixed state. The modulation is only activated if the SL flag is asserted. The modulation transistor is in a permanently open state if not activated. The modulation mode synchronous to the EPC allows to use the hardware demonstrator introduced in chapter 3 to derive ranging information as it will be shown in chapter 6. Furthermore, by using the other modulation modes, measurements with standard COTS laboratory equipment can be easily conducted without the need of demodulating the data send by the tag.

For this special RFID IC, a dual antenna tag depicted in fig. 5.4b was designed and produced by *NXP Semiconductor N.V.*. The antenna on the left side of the IC is a meandered dipole with an inductive matching loop optimized for EPC communication, and therefore connected to the UHF port of the RFID IC. The antenna on the right side of the IC is a loop antenna intended to be used for ranging in the 2.4 GHz ISM frequency band and is connected to the additional modulation transistor.

For the simulations, *NXP Semiconductor N.V.* provided the mechanical design data as well as the used stack up. The tag consists of a 18 µm thick copper layer on a 63 µm thick polyethylene terephthalate (PET) dielectric foil. The RFID IC is flip-chip mounted to the copper landing pads.

[5] Information about the session flags can be found in [2].

5.4.2 Impedance of the Different Modulation States

For the simulation of the ΔRCS of a tag, not only the shape of the antenna, but also the input impedance of the RFID IC in both modulation states has to be known.

The impedance values shown in the datasheets of COTS tags mostly include only the impedance in the absorbing state at the minimum operation power. This is the impedance to which the antenna must be complex conjugated matched to achieve a maximum forward reading range.

In order to be able to characterize the used tags, a test fixture for measuring the impedance of the flip-chip mounted REFlex IC was designed. The fixture was designed to have two differential feeding structures to the antenna ports of the flip chip mounted RFID IC. It also includes the elements needed for a through-reflect-line (TRL) calibration to a defined reference plane on the pads of the IC. The fixture deembedding was performed with the automatic fixture removal tool from *Keysight*.

The impedance of the absorbing state can be easily measured by a vector network analyzer (VNA) as the tag is permanently in it if no ($R \Rightarrow T$) modulation is present. A power sweep showed that the tag behavior is highly non linear. While the impedance is almost constant for power levels below the minimum operation power, but it changes if the power is increased. This effect is most likely caused by the energy harvesting circuit in conjunction with the limiting diodes of the IC. The impedance measurement of the UHF port of the tag showed good agreement with the datasheet values at the sensitivity limit.

The measurement of the impedance in the reflecting state is more complicated as it is not possible to bring a EPC compliant RFID IC into a state where the modulation transistor is activated permanently. Therefore, measurements can only be made during a ($T \Rightarrow R$) communication. Thereby, the VNA has to be operated on a single frequency, and the CW signal has to be modulated such that the tag responds with a ($T \Rightarrow R$) communication. By evaluating the time depended reflection coefficient of the tag one can determine the reflection coefficients of the tag in both states. This measurement requires an interrogation of the RFID tag for each frequency point of interest. Therefore, frequency sweeps require much more measurement time compared to normal S-parameter measurements. Furthermore, due to the inherent nonlinearity of the tag it is questionably if these measurements can be directly applied for evaluation of the ranging based on broadband low power spectral density ranging signals.

To measure the broadband reflection coefficient of the tag in both modulation states, a one port VNA based on the SDR platform introduced in chapter 3 was created. This setup was built during a seminar work [58] under my supervision. The UHF port of the REFlex tag was characterized by means of a superimposed

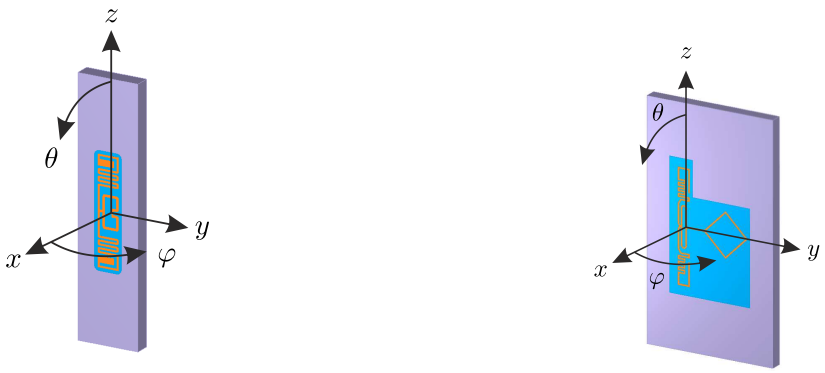
	absorbing		reflecting	
	865 MHz	2.45 GHz	865 MHz	2.45 GHz
UHF Port:				
	parallel	parallel	series	series
R	3350 Ω	3350 Ω	27.6 Ω	27.6 Ω
C	706 fF	706 fF	68.9 pF	68.9 pF
L			355 pH	355 pH
Ranging Port:				
	series	series	series	series
R	4.2 Ω	11.4 Ω	27.6 Ω	27.6 Ω
C	198 fF	157 fF	68.9 pF	68.9 pF
L			355 pH	355 pH

Table 5.1: Equivalent circuits models used for determination of the ΔRCS by simulation

low power band limited noise like sequence in both modulation states. This measurement was performed with different CW power levels and also at different center frequencies of the EPC communication. The measurement results show that the reflection coefficient of the tag in the reflecting state is almost constant over the power sweep of 18 dB above the minimum power level for activation of the tag. However, the reflection coefficient in the absorbing state depends highly on the power level of the CW which is used to supply the tag with power. In section 5.4.4, simulations will be shown which depict the offset in the ranging result for different impedances of the absorbing state.

The impedance of the ranging port of the REFlex IC was measured by a VNA in the different modulation states. This measurement was performed by switching the tag to the different modulation states by using EPC commands and performing power sweeps over both antenna ports. The circuit at the ranging port of the REFlex IC basically consists of four modulation transistors with different impedances in the conducting state and two clamping diodes for protection against damage by too high incident power and electrostatic discharge (ESD). They are arranged in a differential parallel circuit. Thereby, the tag can be set into a no, weak, and strong modulation state. As expected, the ranging port of the REFlex tag shows linear behavior while the incident power level is below 1 dBm[6] in a 100 Ω differential system. Also, no significant dependence of the impedance of the ranging port on the applied power level on the UHF port was found.

[6] 1 dBm incident power onto the IC is very unlikely to happen if it is connected to an antenna



(a) UCODE 7 RFID tag (b) REFlex dual frequency RFID tag

Figure 5.5: Orientation of the tags used for simulation and measurement

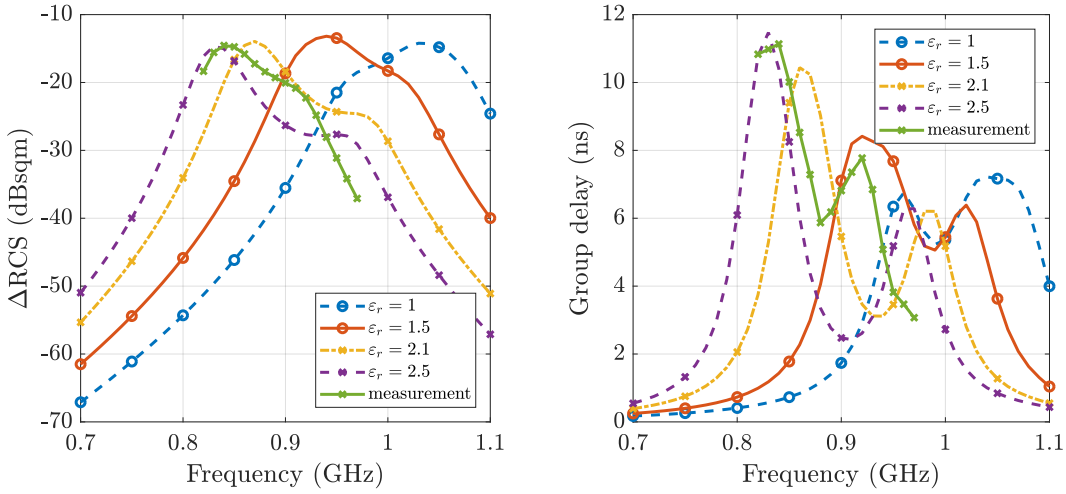
The equivalent circuit models used for the simulations with their respective values are summarized in table 5.1. These models are used for the simulations whenever it is not explicitly stated that different values are used.

The impedance values from the UCODE 7 datasheet [59] are used for the absorbing state of the UHF port in both frequency ranges. An RLC model was fitted to the measurements of the ranging port of the REFlex tag in the strong modulation state. This model is used for both ports in both frequency ranges. It also fits the UHF port as the power harvesting is short circuited by the modulation transistor during the reflecting state[7]. The measurements in the absorbing state of the ranging port could not be fitted by one RLC model for both frequency ranges, hence, two separate RC models were fitted to the measurement data.

5.4.3 Simulation Results Compared to Measurements in the Anechoic Chamber

In the following, simulation results will be compared against measured data from [6]. The results of the first simulations show the COTS UCODE 7 tag on a dielectric brick in a monostatic scenario in boresight to the tag. The simulation was performed for different relative permittivities (1, 1.5, 2.1, and 2.5) of the block where the tag is mounted. A frequency sweep at the minimum required power level for activation of the RFID was extracted from the measurements taken

[7] Also the measurements conducted during the seminar work showed good agreement with this values



(a) Magnitude of the ΔRCS

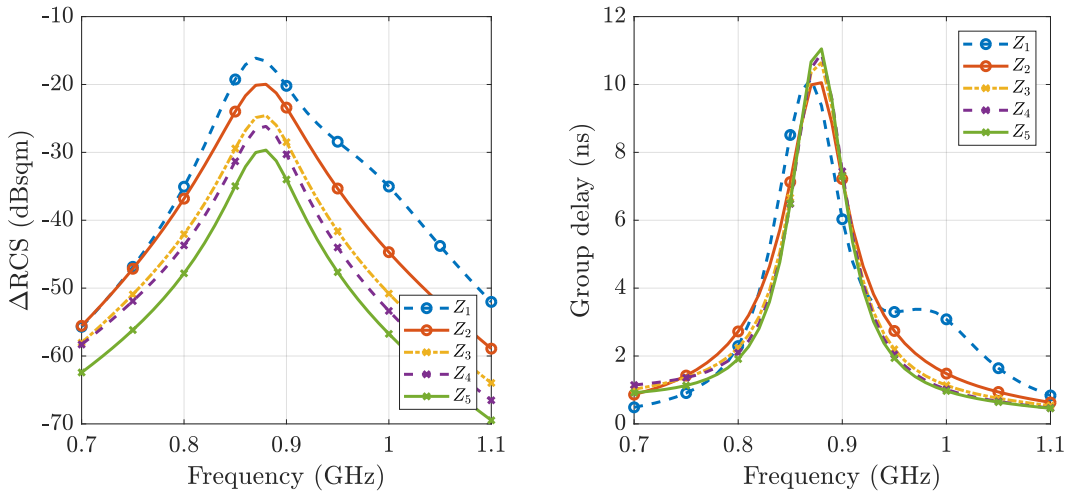
(b) Group delay

Figure 5.6: Comparison of the simulation results with different relative permittivities of the block to the measurement result in the anechoic chamber of the UCODE 7 tag

at different power levels[8] inside the anechoic chamber and is shown as a comparison to the simulation. Please note that measurement values are only accessible in the frequency range from 820 MHz to 970 MHz due to hardware limitations of the measurement system. Figure 5.5 shows the orientation of the coordinate system used for simulations and measurements.

Figure 5.6a shows the magnitude of the ΔRCS and fig. 5.6b shows the frequency dependent group delay evaluated directly from the slope of the phase of the ΔRCS in boresight direction ($\theta = 90°$, $\varphi = 0°$). It can be seen that the peak of the ΔRCS almost shifts by 200 MHz if the ε_r of the brick is varied between 1 and 2.5. It can also be seen that the magnitude of the ΔRCS is not flat over the frequency band utilized for ranging (815 MHz to 915 MHz) and that the variation across the frequency band of interest is in the order of 10 dB for the measurement and the simulation of the tag on the PTFE block. The group delay has a significant peak (11 ns) in the frequency band where the ranging signal is applied. This leads to the assumption that the ranging results will be shifted by up to 3.3 m due to the group delay introduced by the ΔRCS of the tag. For a monostatic LoS ranging measurement this would mean that the actual ranging result is shifted by 1.65 m as the spatial estimate is the half of the two-way round

[8]The data used was extracted from different measurements, thus it is not assured that the impedance of the tag in the absorbing state is equal as the tag has non linear behavior.



(a) Magnitude of the ΔRCS

(b) Group delay

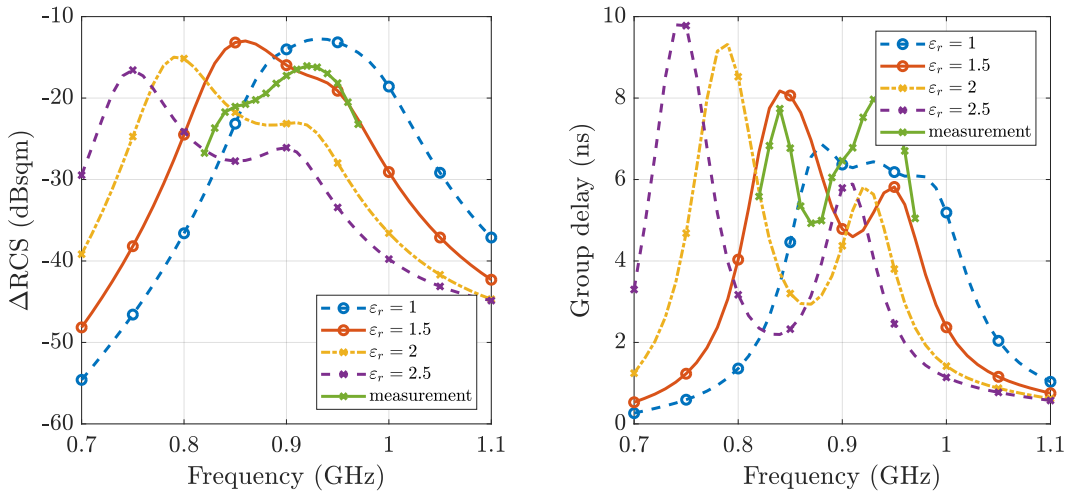
Figure 5.7: UCODE 7 simulation conducted with different impedances of the absorbing state to observe the change in the ΔRCS caused by the nonlinearity of the tag. The used impedances can be found in table 5.2.

	Z_1	Z_2	Z_3	Z_4	Z_5
power level above P_{min} (dB)	0	5	10	15	17
R (Ω)	1275	475	250	225	150
C (fF)	700	890	1120	1450	1700

Table 5.2: Absorbing state impedances used for the simulation showing the influence of the non linear behavior of the RFID tag (parallel equivalent circuit).

trip. Also a strong dependence of the group delay on the ε_r of the brick can be observed. Consequently, it can be assumed that the ranging error is dependent on the material the tag is attached to.

To analyze the influence of the nonlinear behavior of RFID tags, the simulation of the UCODE 7 tag on the PTFE block was evaluated for different absorbing state impedances shown in table 5.2. The impedances were chosen such that they resemble the measurement data from [58], which correspond to a power sweep over 17 dB above the minimum power level needed for activation. The resulting ΔRCS and group delay are depicted in fig. 5.7. The results show that the ΔRCS decreases by 15 dB at the center frequency used for EPC communication. For the normal EPC identification operation this imposes no real problem as a higher power on the tag means that the path loss between tag and reader is



(a) Magnitude of the ΔRCS

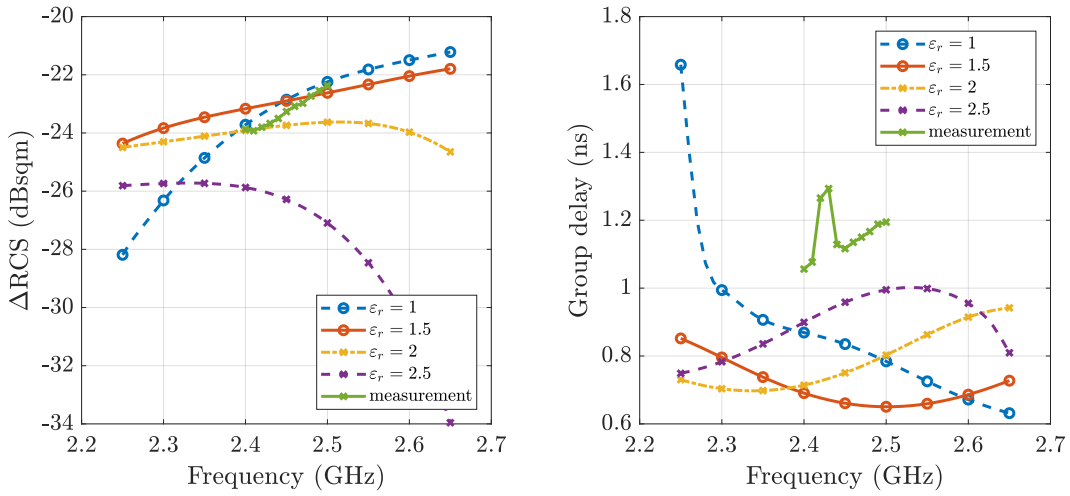
(b) Group delay

Figure 5.8: Comparison of the simulation results with different relative permittivities of the brick to the measurement result in the anechoic chamber of the REFlex tag in the UHF frequency range

lower, therefore, the power of the backscatter signal will likely be high enough for decoding. However, for ranging based on the RSSI of the received signal this behavior should be considered. With respect to the broadband based ranging, the influence of the different impedance in the absorbing state is negligible in terms of group delay in the utilized ranging frequency band from 815 MHz to 915 MHz. However, the group delay introduced by the resonance at 1 GHz changes significantly. Just because of that we cannot see a significant change within our ranging bandwidth for the UCODE 7 tag, it does not allow us to make general statements regarding all possible tags. Therefore, the influence of detuning of the chip has to be considered for practical applications.

Another simulation in the UHF band was performed for the REFlex RFID tag and the results are depicted in fig. 5.8. It can clearly be seen that this tag is optimized for operation with a mounting material with a low ε_r near to one. The group delay in the ranging frequency band is about 8 ns and thus about 3 ns lower than the group delay of the COTS tag. Since the simulations and measurements of the two tags differ in many ways we can conclude that different calibrations for different tag designs will be necessary.

The ΔRCS of the REFlex RFID tag in the ISM band was simulated and measured (fig. 5.9). It can be seen that the broadband behavior of the tag is almost flat in the ISM band and that it is less dependent on the ε_r of the mounting material. Furthermore, the group delay is lower compared to the UHF frequency



(a) Magnitude of the ΔRCS

(b) Group delay

Figure 5.9: Comparison of the simulation results with different relative permittivities of the brick to the measurement result in the anechoic chamber of the REFlex tag in the ISM frequency range

range. The variation of the group delay is in the order of 15 cm due to the variation of the ε_r. So it is much lower compared to the simulations in the UHF band. The two antenna design offers the possibility to optimize the ranging antenna separately from the antenna used for EPC communication.

5.4.4 Analysis of the Simulation Results with Regard to the Influence onto the Ranging Performance

Previously, we have taken a look onto the ΔRCS of the tag with regard to the magnitude and group delay. In the following, we will combine this information with the broadband ranging method introduced in chapter 2. The ranging offset due to the ΔRCS of the tag will be calculated using a 127 sample long MLS sequence with a chiprate of 50 MHz, bandlimited by a 50 MHz RRC filter with a roll off factor of 0.9. The ΔRCS is applied to this ranging signal by multiplication in frequency domain. The ranging offset is then determined by a peak search of the magnitude of an oversampled cross-correlation function between the signal distorted by the ΔRCS and the non-distorted signal. For ranging in the UHF bands the ranging sequence is centered around 870 MHz while for ranging in the

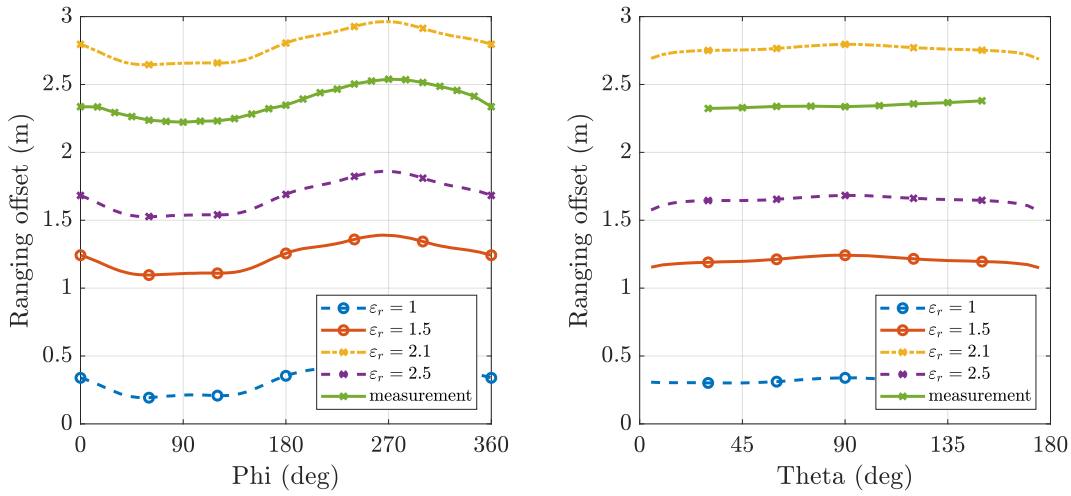


Figure 5.10: Direction dependent monostatic ranging offset of the UCODE 7 tag

ISM band it is centered around 2.45 GHz[9]. This ranging offset is evaluated for different tags in a monostatic scenario and presented in theta and phi cuts.

Figure 5.10 shows the direction dependent ranging offset of the UCODE 7 tag simulated with different permittivities ε_r of the mounting block and the measurement conducted on the PTFE block. It can be seen that the ranging offset highly depends on the ε_r of the surrounding material. This outcome is no big surprise as we have already observed in fig. 5.6b that the peak of the group delay shifts if ε_r is varied. It has to be noted that the difference of the offset due to a different mounting material is much higher than due to the directional dependence. For a single ε_r, the difference of the offset is about ± 15 cm for the φ cut and about ± 5 cm in the θ cut. We can also observe that ε_r changes the offset in a non-monotonic fashion, which was also expected as the resonance peak shifts through the bandwidth of the ranging signal.

Similar to the impedance sweep of the previous section, fig. 5.11 shows how the non-linear behavior of the RFID tag results in a slight ranging offset variation of about ± 7 cm. Since this variation is small compared to the overall variation it can be neglected. However, this only holds true for this particular case as it would have a much larger effect if the ranging sequence would be centered around 980 MHz due to the larger variation of the group delay of the second resonance which can be observed in fig. 5.7b. This exemplary evaluation with the UCODE

[9]These frequencies are chosen since the measured data were only available in a small frequency range (820 MHz to 970 MHz for the UHF band and 2.4 GHz to 2.5 GHz for the ISM band) due to hardware limitations.

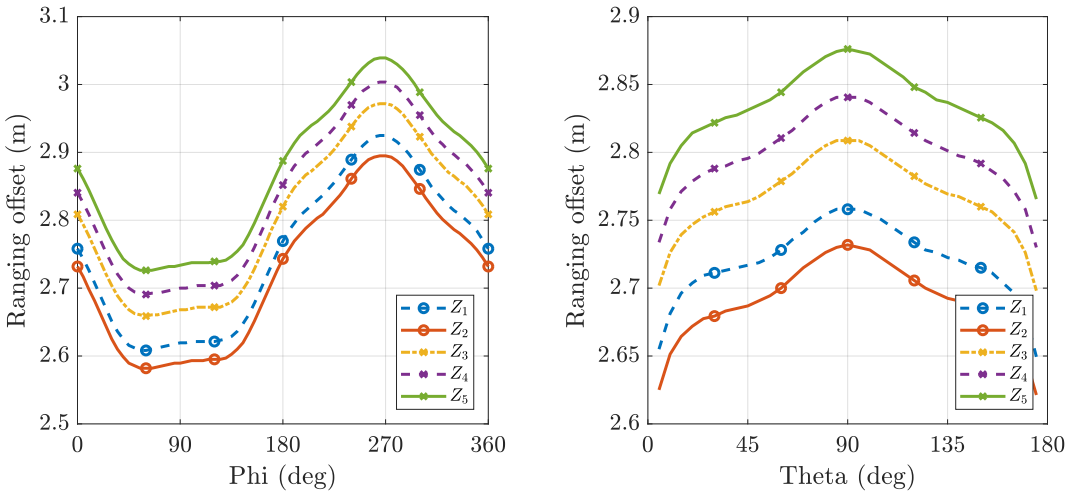


Figure 5.11: Ranging offset of the UCODE 7 tag due to different absorbing state impedances

7 fashion tag cannot be used to rule out the influence of the impedance change for all possible RFID tags.

In order to compare the results of the UCODE 7 tag with another tag, the simulation was also conducted with the REFlex tag in the UHF frequency band. The results are depicted in fig. 5.12 and show that for the REFlex tag the ranging offset is about 2 m if the tag is mounted on a brick with $\varepsilon_r \approx 1$. Compared to the UCODE 7, it can be observed that the ranging offset between the two tags, if mounted on the material for which they are designed, is about 0.5 m.

Finally, fig. 5.13 shows the ranging offset of the REFlex RFID tag in the ISM frequency band. Measurement and simulation match well, and the ranging offset is about 27 ± 10 cm. The small offset range holds true for all simulated ε_r values. Therefore, we can conclude that this design is relatively robust against changes of the surrounding materials with regard to ranging.

To sum it up, for an accurate ranging of COTS EPC RFID tags many factors can have an impact onto the ranging performance. It seems that accurate ranging is only possible if multiple environmental conditions are known beforehand. However, in scenarios where several parameters are fixed, e.g., on a conveyor belt with similar tags on similar items, relative ranging information can be provided also without calibration[10]. We have also seen that by using different frequency bands for ranging and identification, the ranging antenna can be solely optimized

[10] Assuming a scenario with low multipath reflections

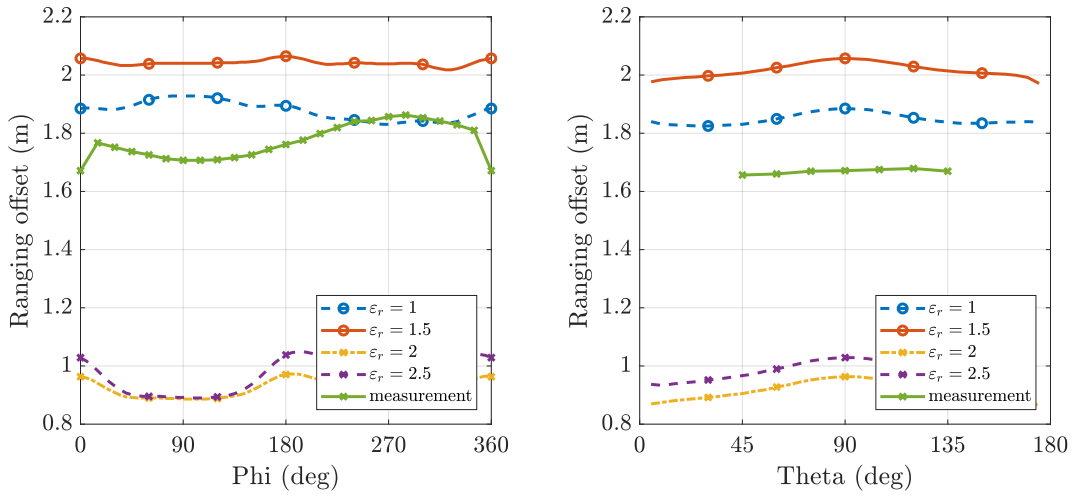


Figure 5.12: Direction dependent monostatic ranging offset of the REFlex tag in the UHF band.

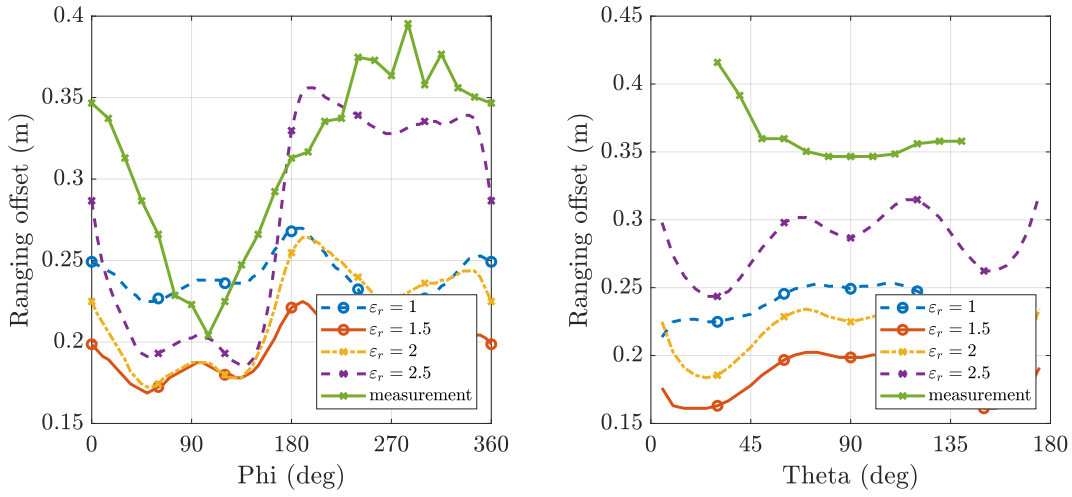


Figure 5.13: Direction dependent monostatic ranging offset of the REFlex tag in the ISM band.

for accurate ranging and the robustness to changes of environmental factors can be improved. Overall it can be concluded that the broadband ranging method can be used in specific applications, but the expected ranging error has to be investigated by a case to case study to ensure that it is within the required ranging accuracy.

Chapter 6

Extension of the Test Platform to MIMO Operation

As already discussed in section 2.3 the main performance limitation in dense multipath environments is the overlapping of multipath components, which cannot be separated due to the finite bandwidth, and therefore the finite spatial resolution. One way to enhance the separability is to increase the bandwidth. However, in the UHF frequency range this is problematic due to the large relative bandwidth that would be necessary to separate multipath components in typical indoor environments. This would make antenna designs difficult. Furthermore, the usable bandwidth is also limited by stringent radio spectrum regulations.

Another solution is the use of multiple antennas, which allows the use of statistical signal processing methods, in order to reduce the localization bias [39]. One option is, for example, array processing and thereby separation of the individual components by using the AoA of the received signals.

Furthermore, for the dual frequency tag introduced in section 5.4.1, a synchronized testbed is necessary, which queries the tag in the UHF band and performs ranging synchronously to the EPC response of the tag in the 2.45 GHz ISM band.

To include access to the benefits of MIMO systems and to the REFlex dual frequency tag, the SDR based testbed was extended to a MIMO platform. Section 6.1 shows how the FPGA implementation was adapted such that multiple SDRs can be synchronized. Section 6.2 gives an overview over the possible applications of the *MIMO extension*. Section 6.3 discusses a measurement setup and the gained results of a monostatic testbed with an active carrier cancellation. Section 6.4 shows the measurement setup and discusses the results obtained with the REFlex dual frequency tag.

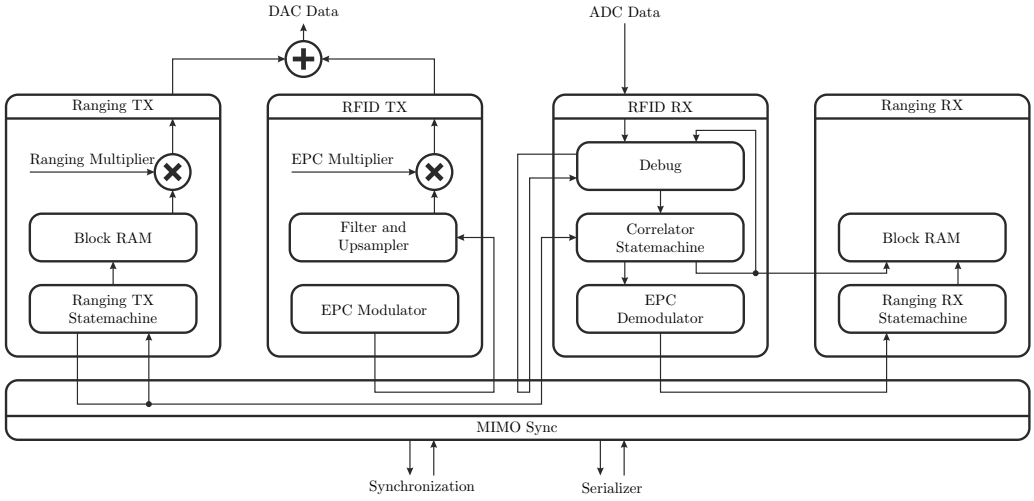


Figure 6.1: Block diagram of the FPGA implementation showing the *MIMO extension* and the synchronized connections

The implementation of the *MIMO extension* and measurement results of the monostatic setup have also been published in [60].

6.1 Changes to the FPGA Implementation

The following section shows the changes made to the FPGA implementation described in section 3.1.1 to enable synchronous operation. The main focus was on using the *MIMO interface*[1] to achieve MIMO operation without hardware modifications. This interface has eight differential wire pairs, which are intended to be used in simplex operation (four in each direction). Two pairs are hard wired to the clock distribution IC, making it possible to synchronize the 100 MHz clocks. Another two pairs are used by a serializer IC, enabling full duplex data transmission between two SDRs with a data rate of 1.28 Gbit/s to 2.16 Gbit/s. Additionally, two differential wire pairs in each direction are connected directly to the FPGAs.

For synchronization, the serializer is operated synchronous to the 100 MHz system clock. Therefore, it can be used to exchange 16 synchronization signals in the main clock domain of the FPGA. Due to the modular design of the FPGA implementation the signals which are necessary to be shared among multiple SDRs for synchronization were accessible. These signals are now concentrated

[1]The *MIMO interface* is a connector of the used SDR N210 intended to synchronize two SDRs via a COTS mini SAS SFF-8088 cable

and distributed in the newly developed *MIMO sync* block, which is also illustrated in fig. 6.1. The main idea is to distribute the synchronization signals generated by the functional blocks of the master unit to the inputs of the blocks relying on these signals in the master and the slave.

The following signals are used to synchronize multiple SDRs:

- EPC modulation state: The master produces the signals indicating the current modulation state. This state is used as input for the EPC filter and upsampler for the master and the slave.
- Reset signal of the counter used for the cyclic playback of the ranging signal: When all counters are reseted by the same signal, the ranging sequence playback and reception is synchronized.
- Synchronization signals of the EPC demodulator: These signals control the coherent averaging process for the reception of the ranging signal by indicating the time instances when the averaging must be performed. Furthermore, they reset the data storage of the received ranging between multiple interrogations.
- Trigger for the debug block: Enables synchronous triggering of the recording of the raw ADC data. This feature is mostly used for debugging and verification of the function of the FPGA implementation.

With this synchronization it is possible to transmit the EPC and the ranging signals synchronously. By using the complex ranging multiplier it is also possible to easily change the attenuation and the phase of the ranging signal without reuploading the ranging signal into the RAM of the signal generator. Furthermore, a complex multilpier is also implemented for the EPC signal, enabling experiments with beamforming by using multiple antennas to increase the reading range.

The drawback of this implementation is that only the master can be used for decoding of the EPC response of the tag. A joint EPC decoding on the master and slave would be possible with the hardware of the SDRs. But, it would require to use the *MIMO interface* bidirectional. In favor of a simple implementation and to be easier extendable to more slaves, it was decided to omit this feature.

The implementation of the *MIMO extension* allows operation as master and as slave. Therefore, all SDRs can be flashed with the same firmware. The configuration of this block is done via the *Microblaze* in a similar way as the configuration of the other blocks.

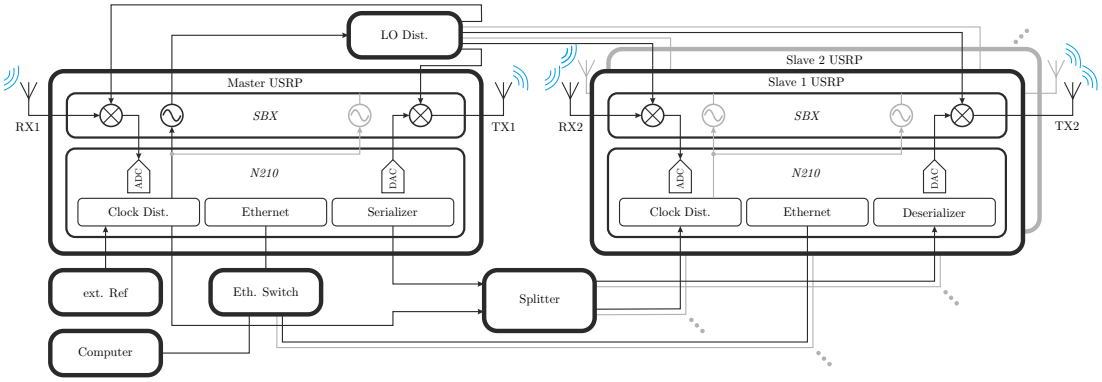


Figure 6.2: Linking multiple SDRs by using a splitter

6.1.1 MIMO Splitter

The previously described change of the FPGA firmware enables the synchronization of two SDRs by using the *MIMO interface* of the platform. Since it is desired to utilize more than two units, the previously discussed implementation deliberately uses the *MIMO interface* unidirectional from the master to the slave unit. Therefore, it is possible to synchronize almost an arbitrary number of SDRs by simply distributing the four differential signals of the master to all slave units. Figure 6.2 shows a possible assembly of a multiple node MIMO system. The configuration and the transfer of the measurement data of all SDRs is done over Ethernet by a single PC.

In order to be able to distribute the signals to multiple SDRs, a *MIMO interface* splitter PCB was build. The four differential signals of the master SDR are distributed by four 1:4 data fanout buffers (*NB6HQ14M* from *ON Semiconductor*®) to up to four slaves. Special care was taken to match the line lengths of the four signals for each slave. The unused TX lines of the slaves and the unused RX lines of the master are properly terminated at the board.

When coherent measurements are needed, the hardware modifications described in [35], [37] enable direct access to the LO inputs and outputs. So it can be used to share a common LO among multiple units. Furthermore, integrated synthesizers of the SDRs can be configured individually for each unit. So it is also possible to operate multiple SDRs only connected via the *MIMO interface* and ethernet, and therefore provide a maximum of flexibility.

6.2 Possible Applications of the MIMO Extension

The *MIMO extension* of the testbed discussed in the prevision section can be used in different ways. In the following, some of the possible applications are listed and discussed:

Beamforming: By using a single synthesizer to derive the LOs of multiple SDRs, beamforming with multiple transmit antennas is possible. As the actual state of the modulation of the EPC transmit signal is synchronized via the MIMO extension, all SDRs will contribute to the ($R \Rightarrow T$) communication. The phase and magnitude of the individual readers can be configured by setting a register of the FPGA via the *Matlab* class. This allows fast switching of amplitude and phase. One application example is to maximize the available power at the tag of interest and to enhance thereby the read range.

Joint Ranging with Multiple SDRs: There are different methods applicable to get the responses from all transmit to all receive antennas. One possibility is that the ranging sequence is activated at one reader after the other. The measurements are not taken exactly at the same time, which could introduce measurement errors in dynamic scenarios. An implementation of such a MIMO ranging will be shown in section 6.4. Alternatively, orthogonal ranging sequences can be used synchronously at multiple ranging SDRs, such that it is possible to record all channels at the same time.

Separate Ranging and Identification: For some setups, it is advantageous to split the ranging functionality from the identification. Thereby, a separate optimization is possible, which could enhance the dynamic range and thus also the noise performance. The following section 6.3 presents as an example a monostatic setup where two SDRs with external filtering were used to show the advantages of a carrier cancellation system. Furthermore, different frequencies for ranging and identification can be used to enhance the ranging accuracy. One advantage compared to a single frequency setup is that the ranging signal can be recorded without self interference from the carrier used for power transfer and also that the antenna for the ranging process can be optimized for ranging without negative influence on the read range of the tag. Additionally, ranging signals can be legally transmitted with a higher power level without special permission, if the ISM band at 2.4 GHz is used for example. During the REFlex project such a multi frequency tag was developed in a close cooperation with *NXP Semiconductor N.V.*. The results of the ranging measurement are shown in section 6.4.

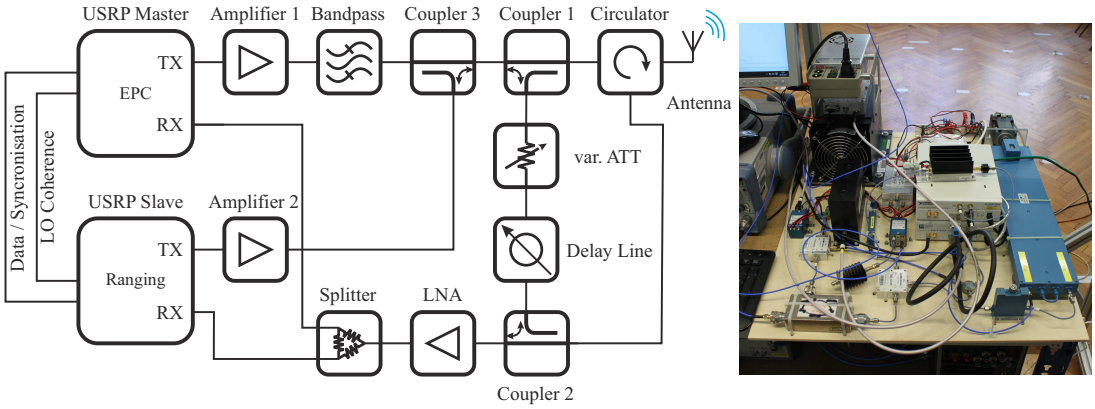


Figure 6.3: Block diagram and photograph of the monostatic measurement system

6.3 Monostatic RFID Reader Testbed

Self interference of the CW signal, used to deliver power to the tag, has a major negative impact onto the performance of the interrogator as already discussed in section 4.2. Since the used COTS SDR is not optimized for UHF RFID applications, it has no built in carrier cancellation. In a monostatic scenario, one antenna is used for TX and RX. The RX signal is typically separated by a directional coupler or a circulator. The imperfect matching of the antenna and the non-ideal isolation of the coupler results in self interference, which is typically worse than the self interference in a bistatic setup stemming from the coupling of the antennas. The first test with a monostatic setup without carrier cancellation showed that the interrogation range was not covering the whole room. The limited dynamic range of the used SDR was identified as the main reason that the demodulation of the EPC communication was not possible at all positions.

To show the performance enhancement of a carrier cancellation onto the ranging performance, a monostatic testbed was developed. It was built mostly with COTS components. A block diagram and a photograph of the measurement system is shown in fig. 6.3 and the used components are summarized in table 6.1. The carrier cancellation superimposes a copy of the transmitted signal onto the received signal such that the CW leakage is canceled.

A manually adjusted carrier cancellation was implemented to reduce the implementation effort. The disadvantage of this approach is that manual interaction is necessary if the reflections in front of the antenna change significantly or if the operation frequency is changed. Hence, it is not suitable for dynamic scenarios.

Special care was taken to minimize the overall noise figure of the setup. The measured noise power spectral density at the output of *amplifier 1* is approxi-

Designation	Manufacturer	Type
Antenna	Huber & Suhner	SPA-8090-75-8-0-V
Amplifier 1	Mini Circuits	ZHL-30W-252+
Amplifier 2	Mini Circuits	ZHL-2010+
Bandpass	K&L	3C42-866.6/T2-O/O
Circulator	Kathrein	791-376
Coupler 1 and 2	Mini Circuits	ZADC-6-2G-5W+
Coupler 3	Krytar	1850
Delay Line	Arra	D2448A
LNA	Hittite	HMC376LP3
USRP Master	National Instruments	USRP 2922
USRP Slave	National Instruments	USRP 2922

Table 6.1: Used components in the monostatic setup shown in fig. 6.3

mately 68 dB above the thermal noise floor (−106 dBm/Hz). The implemented carrier cancellation can suppress only the narrowband CW signal of the transmitter. Hence, *amplifier 1* raises the noise level at the input of the *LNA* above the thermal noise floor via the coupling over the cancellation path and the reflection from the antenna. To suppress this noise, an additional narrowband bandpass filter was inserted after *amplifier 1*. The 3 dB bandwidth of this filter is 2.2 MHz and it has a stopband (±5 MHz) attenuation larger than 34 dB. Since this filter would also suppress the ranging signal transmitted by the *master unit*, it is necessary to superimpose the signal behind this filter. This was done by the use of a directional coupler.

The measurement was conducted with the same parameters as the measurement presented in section 4.2.1. Objects close to the reader antenna change the reflection coefficient of the antenna port. Therefore, an adjustment of the carrier cancellation would be necessary if the tag with its carrier is moved too close to the antenna. Since the measurement was operated in an automatic fashion the range was reduced to the point where an adjustment was not necessary, hence, the positioning range was reduced to 0.7 m to 4 m.

Figure 6.4 shows the ranging offset and the sample standard deviation of the monostatic compared to the bistatic setup. It can be seen that the ranging error is nearly the same for both cases. This can be explained as the antennas used in the bistatic setup are also closely spaced so the that the up- and down-link channels are pretty equal for both situations. As expected, the standard deviation of the monostatic setup is lower by nearly one order of magnitude. This is due to the carrier cancellation and the thereby reduced overall noise figure of the whole setup.

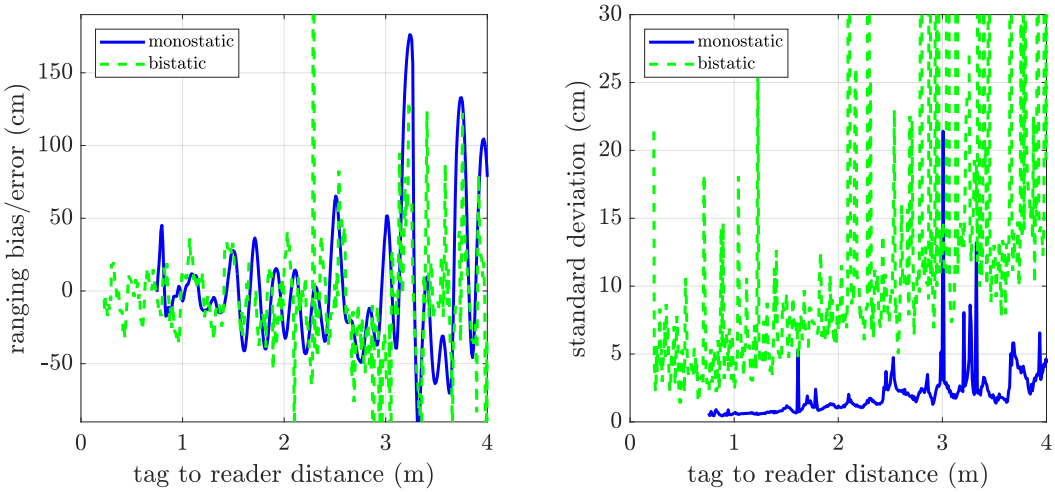


Figure 6.4: Comparison between the ranging results of the monostatic and the bistatic setup

It was thereby shown that the accuracy of the ranging result is mostly determined by the multipath environment it is operated in. Furthermore, it was verified that by employing a carrier cancellation, the SNR of the received ranging signal can be drastically enhanced.

6.4 Ranging in the ISM band

In the following section the measurement setup and the measurement results of the REFlex tag in the 2.4 GHz ISM band will be presented. For this measurement, the *MIMO extension* in combination with the *MIMO splitter* was used.

Figure 6.5 shows a block diagram of the used measurement system and fig. 6.6 shows a photograph of the antenna mount. *USRP 1* was configured as the MIMO master and connected to two *Huber&Suhner SPA-8090/78/8/0/V* patch antennas mounted on a metal frame. The TX antenna was fixed in the middle while the RX was mounted on a linear axis. To achieve the maximum permitted output power for the EPC communication (ERP of 33 dBm), an amplifier (*ZHL-30W-252+* from *Mini Ciruits*) was placed between the TX port of *USRP 1* and the TX antenna. *USRP 2*, *USRP 3*, and *USRP 4* were operated at a center frequency of 2.4418 GHz. The RX frequency synthesizer of *USRP 2* was used as the LO source for all *USRPs* operating on the ISM band. For the 2.4 GHz ISM band, six *Huber&Suhner SPA-2400/75/9/0/V* patch antennas were used. A TX array and

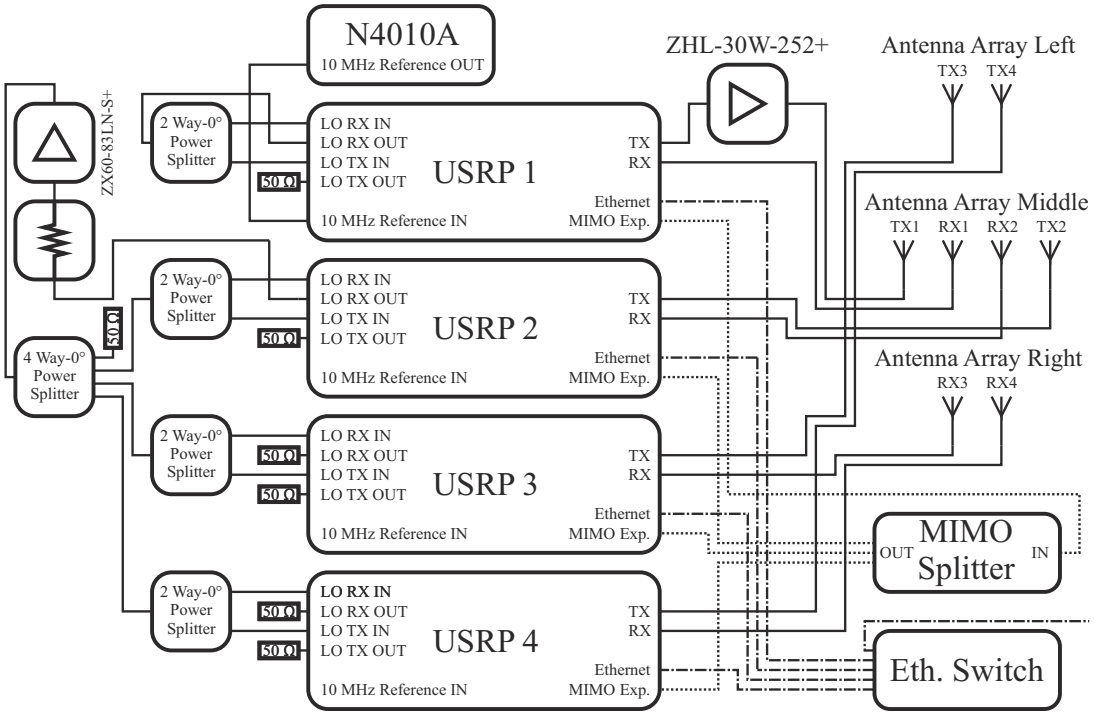


Figure 6.5: Block diagram of the measurement system used to perform ranging in the ISM band with the REFlex tag in the 2.4 GHz ISM band

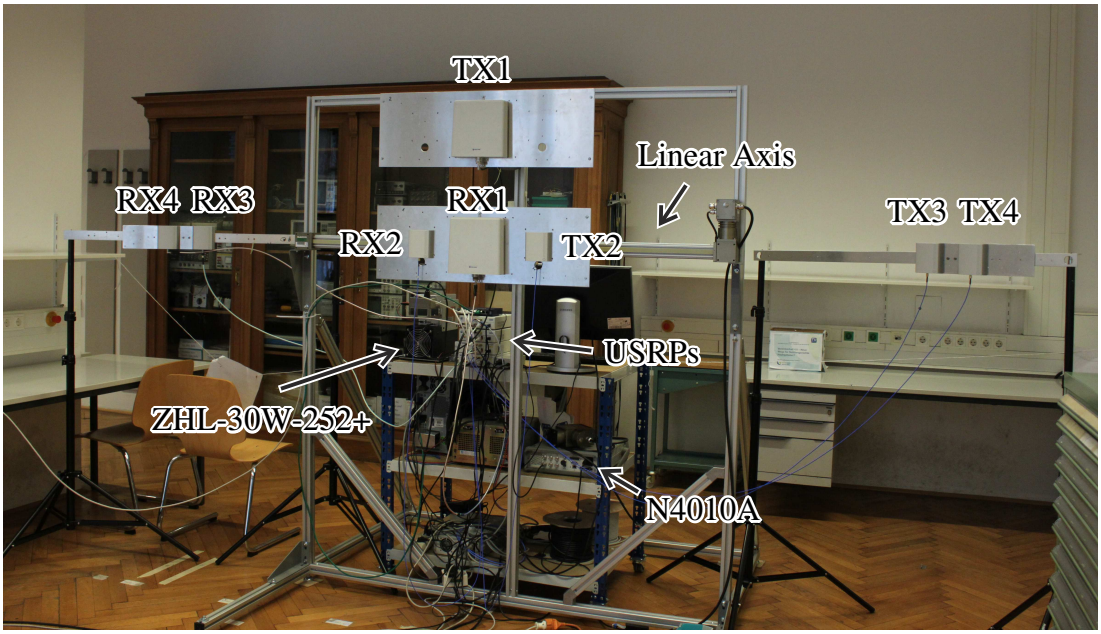


Figure 6.6: Measurement system used for evaluation of the broadband band ranging system

an RX array, each build up by two antennas, were positioned on the sides of the room. Furthermore, a TX and an RX antenna were mounted on the linear axis around the UHF RX antenna for reception of the EPC communication.

An external 10 MHz source was used as the internal source caused problems during some measurements resulting in temporary high jitter[2] between the clocks (100 MHz) caused by small abrupt frequency changes of the internal 10 MHz reference (*FOX924 TCXO*). These frequency changes were caused by the thermal compensation of the reference.

[2]The loop filters of the 100 MHz clock distribution IC of the *USRP* are designed by *ETTUS Research™* with a very small loop bandwidth of 14.2 Hz. So, the phase-locked loop (PLL) cannot follow abrupt changes in the reference frequency as they occur at the internal frequency reference due to the temperature compensation. This leads to an unpredictable phase shift between the synchronized *USRPs* from time to time. It is difficult to spot this behavior as the PLLs do not lose their locked status as no full cycle shift is observed. Nonetheless, a large jitter between the clocks occurs, but only sporadically for a very short period. The reasons for this choice of design of *ETTUS Research™* are not clear to the author. Maybe it is to suppress phase noise of the reference or maybe it is simply a mistake. The problem was reported to *ETTUS Research™*, but the company did not give a clear statement and stated that they cannot deliver support for custom FPGA implementations. However, long term tests with a "clean" 10 MHz reference did not show the temporary jitter behavior between multiple SDRs, and so the *USRPs* were not modified.

A 511 bit long MLS sequence with a chip rate of 50 MHz transmitted with an equivalent isotropic radiated power (EIRP) of 8 dBm was used as the ranging signal. Therefore, the used signal is compliant to the regulations for data transmission equipment operating in the 2.4 GHz ISM band with equipment without listen before talk feature [57]. The EPC CW carrier was transmitted with an ERP of 33 dBm at 865.7 MHz, which complies to the ETSI [13] standard. The EPC response of the $(T \Rightarrow R)$ communication was used for the ranging. To maximize the averaging time, Miller 8 modulation with a BLF of 40 kHz was used. Hence, the coherent averaging process was performed over 2128 subbits, and the averaging time was 21.7 ms.

The tag was positioned on a grid with a size of 4×4.5 m at a height of 1.45 m. The spacing between the individual points was 10 cm. Furthermore, the antennas on the linear axis were moved over 1.2 m with a stepsize of 10 cm. At each measurement combination (tag and antenna position) the tag was queried 600 times. The ranging sequence was thereby transmitted by each ISM band antenna for 200 times one after the other.

Figure 6.7 presents the measurement results of the REFlex tag in the 2.4 GHz ISM band, evaluated for the TX and RX antenna on the linear axis positioned in the middle position. Ranging errors within the range of the colorbar (0.2 m to 1.2 m) are shown as filled circles in the respective color. Results outside this range (outliers) are marked with "+" signs in yellow or blue. Points without marker indicate that at this position no measurement was possible, and most likely the tag had insufficient power to operate.

Compared to the measurements in the UHF band presented in section 4.2.2, the mean ranging error is reduced to 0.7 m. This is mainly due to the smaller group delay of the ISM antenna, which was already discussed in section 5.4. Compared to the UHF results the area where the ripple of the ranging offset is below 20 cm is significantly enlarged. That was expected as the tag in the 2.4 GHz ISM band has a larger usable bandwidth of the ΔRCS compared to the UHF band. Furthermore, the sample standard deviation of the measurement is also lower due to the higher power level of the ranging signal. However, this is partly compensated by the higher FSPL and the lower ΔRCS of the tag in the 2.4 GHz ISM band.

As for the UHF measurments, the linear axis was operated to build a "virtual" antenna array. The RX and TX antennas were positioned at 13 positions with a spacing of 10 cm. Figure 6.8 shows the ranging error of a joint distance estimation over all RX antenna positions, calculated by averaging the individual results and subtracting that result from the distance between the middle of the TX antenna positions and the middle of the RX antenna positions. Only measurements where the tag was successfully interrogated 200 times in each linear axis position were displayed.

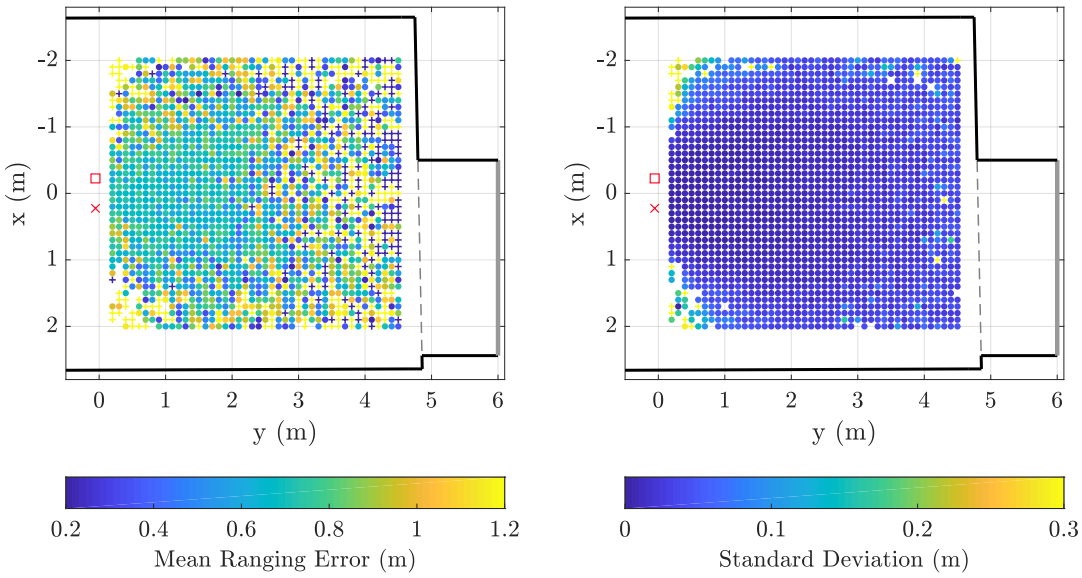


Figure 6.7: Measurement results of the REFlex tag in the ISM band evaluated for the TX and RX antenna on the linear axis positioned in the middle position

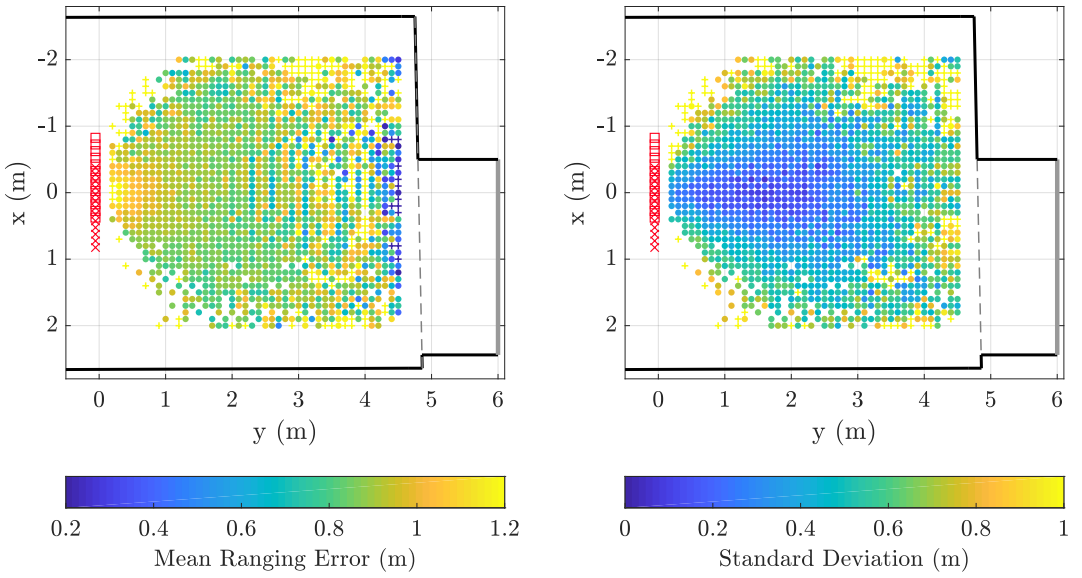


Figure 6.8: Ranging error and standard deviation averaged over the "virtual" antenna array in the 2.4 GHz ISM band

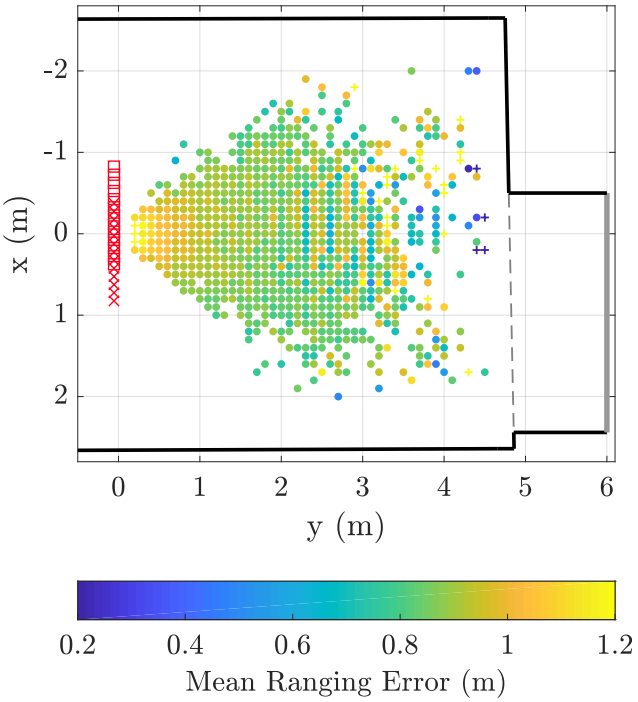


Figure 6.9: Measurement results averaged over the "virtual" antenna array, where results with a sample standard deviation above 0.5 m are omitted in the 2.4 GHz ISM band

Again, it can be seen that the area of usable ranging results is enlarged, which can be explained by the fact that the ranging offset is different for each antenna combination due to the multipath, and therefore, the averaged result has a smaller bias. It should be noted that this approach is by no means optimum and that the result can be further improved by utilizing signal processing methods which include the properties of the multipath.

As in section 4.2.2, an estimation of the quality of the ranging result was derived from the sampled standard deviation. Figure 6.9 shows only the results with a sample standard deviation below 0.5 m. It can be seen that after this filter operation only a few outliers are found within the measurement range. Thereby, it can be shown that such a filter could give a first estimate of how reliable a ranging result is. However, the threshold has to be adjusted for the application and the environmental parameters. It has to be noted that the orientation of the tag is practically the same for all measurement points. Applying this method to real world scenarios where the orientation of the tag is not fixed or the LoS is blocked could lead to problems.

In summary, MIMO operation provides a higher accuracy for ranging and positioning, but it comes at the cost of higher hardware expenses. The additional information gained from the MIMO operation can be utilized by statistical signal processing methods [40]. However, this thesis is focused on the implementation of the hardware testbed and on the effects of the non-ideal impulse response of the ΔRCS of RFID tags onto the ranging results obtained with a broadband ranging method.

Chapter 7

Conclusion and Outlook

This work focused on broadband localization of backscatter based RFID tags, which is a key enabler for multiple industrial applications where the pure identification function is insufficient. Most of the RFID systems that are deployed today are narrowband by design, but for accurate localization in multipath environments broadband systems and/or MIMO systems are necessary to separate the multipath components. This work focused on a broadband ranging method which can be utilized with standard narrowband RFID tags.

The main contributions of this thesis are the development of a ranging enabled RFID reader testbed based on a COTS SDR platform, analysis and discussion of ranging measurement results conducted in an empty office environment, the systematical investigation of the influence of the non ideal ΔRCS frequency response onto the broadband ranging results, and the extension of the testbed to MIMO operation.

The ranging enabled RFID testbed was built based on a *National Instruments™ USRP-2922* SDR consisting of an *N210* and *SBX* board designed by *ETTUS Research™*. The software framework provided by the manufacturer limits the available resolution and bandwidth due to the bandwidth of the Ethernet interface. Since the performance of the broadband overlay ranging method increases with broader bandwidth and better resolution, a custom FPGA implementation was created so that the full resolution and sample rate of the hardware could be utilized.

Measurements with the testbed were conducted in an empty office room with a COTS tag. They showed that even in that very favorable environment, large ranging errors due to the multipath are present. Furthermore, it could be observed that the mean of the measurement results is biased by approximately 2.5 m, which can be explained by an additional group delay stemming from the RFID tag.

To further quantify the influence of the RFID tag onto the ranging measurements, the ΔRCS of RFID tags was analyzed. A method for calculation of the ΔRCS of an antenna from the knowledge of the gain pattern and the impedance of the attached load in the two modulation states was developed. Hence, the ΔRCS of different tags can be easily compared by simulation. Two tag designs mounted on dielectric materials for which they were designed were analyzed and a difference of $\approx 1\,\mathrm{m}$ of the ranging bias was observed. Furthermore, it was shown that different dielectric materials attached to the tags shift the resonance frequency of the antenna as expected. That shift of the resonance frequency is critical, since it also shifts the group delay, and therefore the ranging bias. A sweep of the relative permittivity of the mounting material of a COTS UHF RFID tag from 1 to 2.5 showed that the ranging offset changes by $\approx 2.5\,\mathrm{m}$ for the given COTS tag design. This dependence on the surrounding material has to be considered for accurate ranging results. Furthermore, RFID ICs are nonlinear devices which change especially their absorbing state impedance. The analyzed tag shows a variation of the ranging bias of $\approx 15\,\mathrm{cm}$ due to this nonlinear behavior. Finally, also the spatial direction of the incoming and reflected wave has an influence onto the ranging bias in the order of 30 cm for the given tag. All the previously presented values show the behavior of a specific tag design. It is not possible to extrapolate a general rule from these simulations, but it can be observed that many environmental influences disturb the ranging measurements.

A dual frequency tag, where the identification part is separated from the ranging part, can be used to make the ranging measurements more robust. Such a tag was produced in a close cooperation with *NXP Semiconductor N.V.* and is presented in this work. It consists of a part operating according the EPC standard [2] and an additional modulation transistor which is solely used for ranging. This modulation transistor is connected to a 2.4 GHz antenna. Due to the design of the antenna, the sensitivity to different mounting materials is significantly reduced. Furthermore, the frequency response of the ΔRCS is almost flat in the 2.4 GHz ISM band. In order to conduct experiments with this special RFID tag, the reader testbed was extended to support MIMO operation. In a large empty office environment, measurements were conducted with the previously mentioned tag. The observed benefit of the dual frequency tag compared to the COTS RFID tag is a smaller variation of the ranging bias. A MIMO setup with three TX and three RX antennas was constructed. A cooperation with the Signal Processing and Speech Communication Laboratory of Graz University of Technology during the project REFlex showed that a positioning error below 0.15 m for 80 % of all positions in the empty office environment can be achieved by using the measurement data of this MIMO setup [40], [61].

The realization of this testbed can be further utilized for research and improvement of broadband ranging of passive backscatter based RFID tags. On the

hardware side, the frontend of the SDR can clearly be enhanced by providing an automatic carrier cancellation. During this work, a manual carrier cancellation was built. It has the drawback that it can only be used in static scenarios since it requires manual readjustment every time the RF scenario changes. Nevertheless, the results gathered with this measurement setup have shown that the carrier cancellation makes a great performance improvement.

As a conclusion it can be said that localization of tags which were not designed for ranging is a very challenging task. The properties of the ΔRCS of the tags limit the accuracy of the broadband ranging method. While this method can be used in several scenarios, it must not be considered as an out of the box solution at the current stage of development. Many factors need to be taken into account for deriving spatial information from the measurements. However, it can be observed that the ranging results gained with this method have a better quality than results derived from narrowband methods. Furthermore, the localization accuracy can be significantly improved by utilizing MIMO systems and specialized tags.

References

[1] K. Finkenzeller, *RFID Handbook*, 2nd. John Wiley & Sons, Ltd., 2003, ISBN: 0-470-84402-7.

[2] *EPC radio-frequency identity protocols generation-2 UHF RFID*, version 2.1, GS1 EPCglobal Inc., Jul. 2018. [Online]. Available: `http://www.gs1.org/epcglobal` (visited on 04/16/2019).

[3] J. Landt and B. Catlin, *Shrouds of time: The history of RFID*, online, version 1.0, AIM Inc., Oct. 1, 2001. [Online]. Available: `https://rainrfid.org/wp-content/uploads/2015/12/History-of-RFID.pdf` (visited on 10/17/2018).

[4] A. F. Molisch, *Wireless Communications*, 2nd. Wiley-IEEE Press, Dec. 2010, ISBN: 978-0-470-74186-3.

[5] P. V. Nikitin and K. V. S. Rao, "Antennas and propagation in UHF RFID systems", in *Proc. IEEE Int. Conf. on RFID*, Apr. 2008, pp. 277–288. DOI: `10.1109/RFID.2008.4519368`.

[6] D. Neunteufel, "Delta-RCS characterization of RFID tags and implications on localization accuracy", Master's thesis, Technische Universität Wien, Jan. 2018.

[7] A. Buffi, A. Michel, P. Nepa, and B. Tellini, "RSSI measurements for RFID tag classification in smart storage systems", *IEEE Transactions on Instrumentation and Measurement*, vol. 67, no. 4, pp. 894–904, Apr. 2018, ISSN: 0018-9456. DOI: `10.1109/TIM.2018.2791238`.

[8] Z. Zhang, Z. Lu, V. Saakian, X. Qin, Q. Chen, and L. R. Zheng, "Item-level indoor localization with passive UHF RFID based on tag interaction analysis", *IEEE Transactions on Industrial Electronics*, vol. 61, no. 4, pp. 2122–2135, Apr. 2014, ISSN: 0278-0046. DOI: `10.1109/TIE.2013.2264785`.

[9] M. Scherhäufl, M. Pichler, and A. Stelzer, "UHF RFID localization based on evaluation of backscattered tag signals", *IEEE Transactions on Instrumentation and Measurement*, vol. 64, no. 11, pp. 2889–2899, Nov. 2015, ISSN: 0018-9456. DOI: `10.1109/TIM.2015.2440554`.

[10] M. Gunia, A. Zinke, N. Joram, and F. Ellinger, "Setting up a phase-based positioning system using off-the-shelf components", in *Proc. 14th Workshop on Positioning Navigation and Communications*, Oct. 2017, pp. 1–6. DOI: 10.1109/WPNC.2017.8250065.

[11] M. L. Breton, L. Baillet, E. Larose, E. Rey, P. Benech, D. Jongmans, and F. Guyoton, "Outdoor UHF RFID: Phase stabilization for real-world applications", *IEEE Journal of Radio Frequency Identification*, vol. 1, no. 4, pp. 279–290, Dec. 2017. DOI: 10.1109/JRFID.2017.2786745.

[12] S. Sarkka, V. V. Viikari, M. Huusko, and K. Jaakkola, "Phase-based UHF RFID tracking with nonlinear Kalman filtering and smoothing", *IEEE Sensors Journal*, vol. 12, no. 5, pp. 904–910, May 2012, ISSN: 1530-437X. DOI: 10.1109/jsen.2011.2164062.

[13] *Electromagnetic compatibility and radio spectrum matters (ERM); radio frequency identification equipment operating in the band 865 MHz to 868 MHz with power levels up to 2 W and in the band 915 MHz to 921 MHz with power levels up to 4 W*, version 3.1.1, European Telecommunications Standards Institute, Nov. 2016. [Online]. Available: http://www.etsi.org/standards-search (visited on 04/16/2019).

[14] *Regulatory status for using RFID in the EPC Gen2 (860 to 960 MHz) band of the UHF spectrum*, GS1 EPCglobal Inc., 2016. [Online]. Available: https://www.gs1.org/sites/default/files/docs/epc/uhf_regulations.pdf (visited on 02/28/2018).

[15] P. V. Nikitin, R. Martinez, S. Ramamurthy, H. Leland, G. Spiess, and K. V. S. Rao, "Phase based spatial identification of UHF RFID tags", in *Proc. IEEE Int. Conf. on RFID*, Apr. 2010, pp. 102–109. DOI: 10.1109/RFID.2010.5467253.

[16] F. Galler, D. Neunteufel, and H. Arthaber, "Complex-valued delta RCS simulation of RFID tags for time of flight ranging performance assessment", *submitted for review to IEEE International Conference on RFID Technology Application (RFID-TA)*, Sep. 2019.

[17] M. Scherhäufl, M. Pichler, and A. Stelzer, "UHF RFID localization based on phase evaluation of passive tag arrays", *IEEE Transactions on Instrumentation and Measurement*, vol. 64, no. 4, pp. 913–922, Apr. 2015. DOI: 10.1109/TIM.2014.2363578.

[18] M. Cremer, A. Pervez, U. Dettmar, C. Hudasch, T. Knie, R. Kronberger, and R. Lerche, "Transmit beamforming for angle-of-activation (AoAct) estimation in passive UHF RFID systems", in *Proc. IEEE International Confe-*

rence on RFID Technology and Applications (RFID-TA), Sep. 2015, pp. 1–7. DOI: 10.1109/RFID-TA.2015.7379790.

[19] *RFU650 UHF reader datasheet*, SICK AG. [Online]. Available: https://www.sick.com/ag/en/identification-solutions/rfid/rfu65x/rfu650-10100/p/p428444 (visited on 04/10/2018).

[20] *ISC.ANT.U500/270-DM UHF long range reader with direction detection datasheet*, Feig Electronic GmbH. [Online]. Available: https://www.feig.de/en/products/identification/product/id-iscantu500270-dm/ (visited on 04/10/2018).

[21] *xArray RAIN RFID gateway*, Impinj. [Online]. Available: https://www.impinj.com/platform/connectivity/xarray/ (visited on 04/10/2018).

[22] A. Buffi and P. Nepa, "A phase-based technique for discriminating tagged items moving through a UHF-RFID gate", in *Proc. IEEE RFID Technology and Applications Conference (RFID-TA)*, IEEE, Sep. 2014, pp. 155–158. DOI: 10.1109/RFID-TA.2014.6934219.

[23] E. Kaplan and C. Hegarty, *Understanding GPS: principles and applications*, 2nd. 2006, ISBN: 1-58053-894-0.

[24] D. Dardari, F. Guidi, C. Roblin, and A. Sibille, "Ultra-wide bandwidth backscatter modulation: Processing schemes and performance", *EURASIP Journal on Wireless Communications and Networking*, vol. 2011, no. 1, p. 47, 2011. DOI: 10.1186/1687-1499-2011-47.

[25] F. Guidi, N. Decarli, S. Bartoletti, A. Conti, and D. Dardari, "Detection of multiple tags based on impulsive backscattered signals", *IEEE Transactions on Communications*, vol. 62, no. 11, pp. 3918–3930, 2014. DOI: 10.1109/tcomm.2014.2363118.

[26] F. Guidi, N. Decarli, D. Dardari, F. Natali, E. Savioli, and M. Bottazzi, "A low complexity scheme for passive UWB-RFID: Proof of concept", *IEEE Communications Letters*, vol. 20, no. 4, pp. 676–679, 2016. DOI: 10.1109/lcomm.2016.2530658.

[27] H. Arthaber, "Method and system for locating objects", pat. US9471820B2, Sep. 2016, Application granted.

[28] T. Faseth, "Wireless localization for intelligent transport systems", PhD thesis, Vienna University of Technology, 2012.

[29] H. Arthaber, T. Faseth, and F. Galler, "Spread-spectrum based ranging of passive UHF EPC RFID tags", *IEEE Wireless Communication Letters*, vol. 19, no. 10, pp. 1734–1737, Oct. 2015. DOI: 10.1109/LCOMM.2015.2469664.

[30] R. Gold, "Optimal binary sequences for spread spectrum multiplexing", *IEEE Transactions on Information Theory*, vol. 13, no. 4, pp. 619–621, Oct. 1967. DOI: 10.1109/TIT.1967.1054048.

[31] T. Kasami, "Weight distribution formular for some class of cyclic codes", University of Illinois - Urbana, Apr. 1966.

[32] *Unwanted emissions in the spurious domain*, version SM-329-12, International Telecommunication Union, Sep. 2012. [Online]. Available: https://www.itu.int/rec/R-REC-SM.329/en (visited on 04/17/2019).

[33] M. Buettner and D. Wetherall, "A software radio-based UHF RFID reader for PHY/MAC experimentation", in *Proc. IEEE Int. Conf. on RFID*, Apr. 2011, pp. 134–141. DOI: 10.1109/rfid.2011.5764613.

[34] *Schematics of ETTUS SDR USRP2922 (N210+SBX)*, Ettus Research. [Online]. Available: http://files.ettus.com/schematics/ (visited on 06/26/2019).

[35] F. Galler, "SDR-based RFID reader with sub-symbol-synchronization", Master's thesis, Technische Universität Wien, Nov. 2014.

[36] F. Galler, T. Faseth, and H. Arthaber, "SDR based EPC UHF RFID reader DS-SS localization testbed", in *Proc. IEEE 16th Annual Wireless and Microwave Technology Conf. (WAMICON)*, Apr. 2015, pp. 1–4. DOI: 10.1109/WAMICON.2015.7120382.

[37] ——, "Implementation aspects of an SDR based EPC RFID reader testbed", in *Proc. Int. EURASIP Workshop on RFID Technology (EURFID)*, Oct. 2015, pp. 94–97. DOI: 10.1109/EURFID.2015.7332391.

[38] F. Galler, S. Hinteregger, T. Faseth, N. Leder, K. Witrisal, G. Magerl, and H. Arthaber, "Performance evaluation and verification of spread-spectrum based UHF RFID ranging", in *Proc. IEEE Int. Conf. on RFID*, May 2017, pp. 124–129. DOI: 10.1109/RFID.2017.7945597.

[39] S. Hinteregger, E. Leitinger, P. Meissner, and K. Witrisal, "MIMO gain and bandwidth scaling for RFID positioning in dense multipath channels", in *Proc. IEEE Int. Conf. on RFID*, May 2016, pp. 1–6. DOI: 10.1109/RFID.2016.7488027.

[40] S. Grebien, J. Kulmer, F. Galler, M. Goller, E. Leitinger, H. Arthaber, and K. Witrisal, "Range estimation and performance limits for UHF-RFID backscatter channels", *IEEE Journal of Radio Frequency Identification*, 2017. DOI: 10.1109/jrfid.2017.2749514.

[41] G. Marrocco, "The art of UHF RFID antenna design: Impedance-matching and size-reduction techniques", *IEEE Antennas and Propagation Magazine*, vol. 50, no. 1, pp. 66–79, Feb. 2008, ISSN: 1045-9243. DOI: 10.1109/MAP.2008.4494504.

[42] K. She, Y. He, B. Li, Z. Hou, Y. Zhu, and L. Zuo, "Theory and measurement of delta RCS for RFID tag on various materials", in *Proc. 6th Int. Conf. Wireless Communications Networking and Mobile Computing (WiCOM)*, Sep. 2010, pp. 1–4. DOI: 10.1109/WICOM.2010.5600728.

[43] *Tagformance pro measurement system*, Voyantic, 2016.

[44] D. Neunteufel, F. Galler, and H. Arthaber, "Comprehensive measurement of complex-valued delta radar cross-section", in *Proc. Int. EURASIP Workshop on RFID Technology (EURFID)*, Sep. 11, 2018. DOI: 10.1109/EURFID.2018.8611768.

[45] *Tag perfomance parameters and test methods*, GS1 EPCglobal Inc., 2008. [Online]. Available: http://www.gs1.org/epcglobal.

[46] A. Pouzin, T. P. Vuong, S. Tedjini, M. Pouyet, and J. Perdereau, "Bench test for measurement of differential RCS of UHF RFID tags", *Electronics Letters*, vol. 46, no. 8, pp. 590–592, Apr. 2010. DOI: 10.1049/el.2010.3488.

[47] P. V. Nikitin and K. V. S. Rao, "Theory and measurement of backscattering from RFID tags", *IEEE Antennas and Propagation Magazine*, vol. 48, no. 6, pp. 212–218, Dec. 2006. DOI: 10.1109/MAP.2006.323323.

[48] S. Skali, C. Chantepy, and S. Tedjini, "On the measurement of the delta radar cross section (ΔRCS) for UHF tags", in *Proc. IEEE Int. Conf. on RFID*, Apr. 2009, pp. 346–351. DOI: 10.1109/RFID.2009.4911176.

[49] H. T. Friis, "A note on a simple transmission formula", *Proceedings of the IRE*, vol. 34, no. 5, pp. 254–256, May 1946. DOI: 10.1109/JRPROC.1946.234568.

[50] "IEEE standard for definitions of terms for antennas", *IEEE Std 145-2013 (Revision of IEEE Std 145-1993)*, pp. 1–50, Mar. 2014. DOI: 10.1109/IEEESTD.2014.6758443.

[51] S. W. Lee, *Antenna Handbook*, Y. T. Lo, Ed. Chapman & Hall, 1993, vol. Fundamentals and mathematical techniques, ISBN: 0-442-01592-5.

[52] J. Kunisch, "Implications of lorentz reciprocity for ultra-wideband antennas", in *Proc. IEEE International Conference on Ultra-Wideband*, Sep. 2007, pp. 214–219. DOI: 10.1109/ICUWB.2007.4380944.

[53] R. C. Hansen, "Relationships between antennas as scatterers and as radiators", *Proceedings of the IEEE*, vol. 77, pp. 659–662, 1989. DOI: 10.1109/5.32056.

[54] G. Robert, "The general theory of antenna scattering", PhD thesis, Ohio State University, 1963.

[55] C. A. Balanis, *Antenna Theory*, 3rd ed. Wiley-Interscience, 2005, ISBN: 0-471-66782-X.

[56] J. Kunisch and J. Pamp, "UWB radio channel modeling considerations", *Proc. ICEAA*, pp. 277–286, Sep. 8, 2003, ISSN: 8882020088.

[57] *Wideband transmission systems; data transmission equipment operating in the 2,4 GHz ISM band and using wide band modulation techniques; harmonised standard covering the essential requirements of article 3.2 of directive 2014/53/EU.* [Online]. Available: http://www.etsi.org/standards-search.

[58] S. Hechenberger, "Reflection coefficent of an UHF RFID tag at different modulation states", Technische Universität Wien, Seminar report, Dec. 4, 2018.

[59] *UCODE 7 datasheet*, SL3S1204, version 3.5, NXP Semiconductors, Jul. 27, 2015. [Online]. Available: https://www.nxp.com/docs/en/data-sheet/SL3S1204.pdf (visited on 10/16/2018).

[60] F. Galler, S. Grebien, T. Faseth, K. Witrisal, G. Magerl, and H. Arthaber, "Extension of an SDR UHF RFID testbed for MIMO and monostatic time of flight based ranging", *IEEE Journal of Radio Frequency Identification*, vol. 1, no. 1, pp. 32–38, Mar. 2017. DOI: 10.1109/JRFID.2017.2749200.

[61] S. Grebien, F. Galler, D. Neunteufel, U. Mühlmann, S. J. Maier, H. Arthaber, and K. Witrisal, "Experimental evaluation of a UHF-MIMO RFID system for positioning in multipath channels", *submitted for review to IEEE International Conference on RFID Technology Application (RFID-TA)*, Sep. 2019.