A Spatial Selective RFID Reader w. Frequency Diversity

May 2012

Department of Electronic Systems
Rune Simonsen - Software Defined Radio

AALBORG UNIVERSITET

Department of Electronic Systems
Fredrik Bajers Vej 7B
9220 Aalborg Ø
Telephone 99 40 86 00
http://es.aau.dk/

Title: A Spatial Selective RFID Reader w. Frequency Diversity

Theme: Advanced Software Radio Implementation

Project term: P9-P10, Spring and Fall semester 2011-2012

Project group: 12gr1057

Member of the group:

Rune Simonsen
runesim@es.aau.dk

Supervisors:
Patrick Claus F. Eggers
- *Assoc. Professor*

Rasmus Krigslund
- *PhD. Fellow*

Number of copies: 4
Number of pages: 84
Appendices and attachments: 47 and 1 CD
Completed: May 31nd 2012

Abstract:

This project concerns RFID UHF EPC Class 1 Gen.2 physical layer modifications, in effort towards gaining robust communication and intelligent reader capabilities. The work is two-folded; It presents implementation of and research in a RFID Multi-carrier reader system, to enable tag diversity, combating dispersive channels. Furthermore it presents a solution towards obtaining a reader with the possibility of interrogation zone control, by exploiting deliberate interference in software preprocessing. Thus, limiting the reconnaissance area of the reader. This constitutes a tool for spatial tag location as well as limiting the well known tag collision challenges presented by a reader talks first protocol.

The Multi-carrier reader was successfully implemented and tested, however trails conducted towards documenting frequency diversity, showed ambiguous results. Furthermore the deliberate interference concept was proven successful as a tool for limiting the interrogation zone, to prevent all tags in the vicinity to respond.

As this project presents work conducted in the field of Software Defined Radio, the implementation and research is realised by the widely used USRP platform in conjunction with the open source GNU Radio software toolkit.

Preface

This master thesis is the result of work conducted on the final semesters on AAU - Electronic Systems - Software Defined Radio (SDR), with the theme "Advanced Software Radio Implementation". The project was supervised by Associate Professor Patrick Claus F. Eggers and Ph.D. Fellow Rasmus Krigslund.

As Rasmus Krigslund has conducted much work in the field of RFID technology, as part of his Ph.D., the thesis was established from problem statements derived as bi-products of his work. Thus, the project proposal was created in cooperation with Rasmus Krigslund and Patrick Claus F. Eggers, in the fall of 2011, addressing relevant challenges met in RFID systems.

Reading guide

Literature references are displayed as [x] where x is the number of the reference given in the bibliography, listed on page 83. Chapter/section/appendix references are displayed as chapter/section/appendix yy where yy is the number of the chapter, section or appendix. This is equivalent for figure references also. A list of used abbreviations can be found in Nomenclature, appendix F.

A CD is part of the report, where all software is included, as well as the used GNU Radio toolkit version. A digital version of the report is also stored, as well as all figures used in the report. The figures are numerated with the numbers used in the report.

Acknowledgments

For the inputs from highly engaged people, providing a motivating environment, for help and support given to an extending far beyond the expected, the author would like to thank his supervisors. Also Kim Olesen and Kristian Bank, laboratory engineers at APNet, for inputs and assistance with lab experiments and introducing necessary equipment. Jesper Kristensen - Danfoss Power Electronics, for inputs to the areas of USRP, GNU Radio and FPGA implementation. Although not in direct contact, the author would also like to thank Ph.D. Michael Buettner, University of Washington, for providing much work towards an USRP RFID reader. Lastly my family, for care and support in an important time of my life.

Overview

An overview and a small description of each chapter is presented by the following.

Part I: Analysis

Chapter 1: Introduces an RFID overview and classifies the different types. A preliminary solution space is presented, leading to project design objectives.

Chapter 2: Introduction to the basis system architecture of a RFID reader and how it can be modified to enable the design objectives.

Chapter 3: The EPC Gen2 protocol is introduced, illustrating RFID communication concepts and other relevant parts of an RFID communication.

Chapter 4: Describes a multipath narrow and wide-band channel model assumed to be valid in the RFID communication, with the important aspect of the coherence bandwidth.

Chapter 5: Deducts the theory supporting the proposed methods.

Chapter 6: Presents the platform considerations, for specifying the used hardware.

Chapter 7: Introduces the USRP hardware platform and capabilities as well as the GNU Radio software toolkit.

Part II: System design

Chapter 8: A USRP RFID reader package is adopted and presented, both in theory and performance.

Chapter 9: The first concept, the multi-carrier reader implementation steps and performance is described.

Chapter 10: The steps taken towards an interrogation zone controlled reader, is presented.

Part III: Closing

Chapter 11: Reflections on behalf of the implemented systems and obtained experiment results, is presented in terms of a discussion.

Chapter 12: The final conclusion of the entire project is made.

Contents

Part I

Analysis

1 Introduction

1.1 RFID overview

This chapter acts as an introduction to RFID systems and the variety of them. RFID tags are widely used in the logistics business, to ease management of pallets and parcels, however the technology is moving towards item-level tagging. Different types of tags are accessible, all depending on the given application for which they are developed and used. The most central differences are highlighted in the following, to be able to specify the focal variant.

The RFID communication link operates in several different frequency bands, ranging from LF tags beginning at 125 KHz, HF tags at 13.56 MHz and UHF tags operating in the range from 860-960 Mhz and also in 2.4 GHz. Governed by their operating frequency they are divided into inductive LF tags, where the tag antenna is small compared to the wavelength and radiative UHF tags, where the antenna is comparable in size to the wavelength. The frequency range and operating modes are illustrated by figure 1.1.

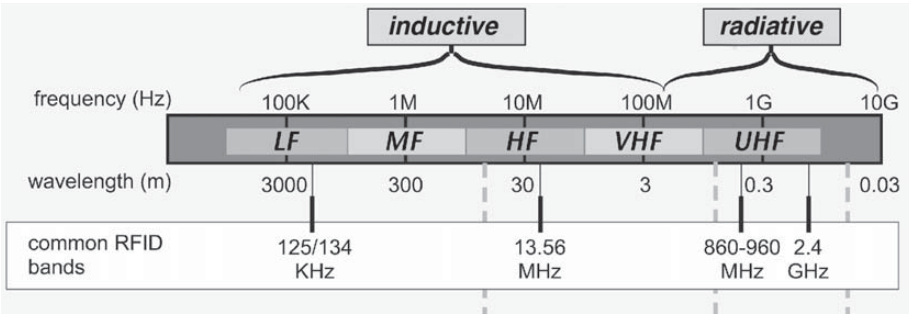

Figure 1.1: Illustration of the different frequency and operation mode [6,p. 24]

The inductive and radiative modes constitutes radical differences between developed tags, as they have completely different fields of application. The inductive systems requires near field presence of the tag, as it relies on the reader inducing energy into the tags coil structured antenna with several windings. Hence it's range is limited to the immediate distance of the reader. A rule of thump for the readable distance is that the tag needs to be as close to the reader as the size of the tag antenna itself. This simplifies the ambiguity regarding the localisation of the tag, as the tag being detected by the reader is obviously the one in its apparent vicinity. This renders the gain from implementing RFID technology

onto small inexpensive products to be minimum, as it increase the expenses while not presenting much difference compared to the traditional optical barcode system.

When considering the radiative UHF tags, the interrogation of a tag however can be done by a theoretical distance of upto 10 meters (2 - 5 m in practice). This produces a wide variety of applications for the RFID technology, however introducing other challenges compared to the inductive system. Many tags can be located in the vicinity of the reader, causing inflictions as to how they are managed in terms of resource sharing. Another aspect of the radiative scheme, is the lack of knowledge of the whereabouts of the exact tag that is being interrogated. This is obviously a trade-off between the inductive and radiative approach, as the freedom of range reduces the specificity of the individual tags location.

As mentioned the LF/HF tags are powered in an inductive manner by the use of an antenna that consists of multiple windings constituting a coil. As the UHF tags are designed to be beyond the reach of inductance, they are powered by different means. This leads the UHF tags to be further characterized by the way they are powered, defined as passive, semi-passive and active, denoted by the following

- **Passive tag** - The tag is powered by a continuous wave propagating from the reader, hence has no internal power supply implemented on the tag.
- **Semi-passive tag** - The tag communicates via the continuous wave from the reader, however the IC is powered by an internal power source.
- **Active tag** - The tag is fully equipped with a power supply that feeds both the RF communication and the onboard circuitry.

Especially the passive tags are of great interest to the development of the RFID technology, as they are cheap to manufacture, small in size and does not depend on the lifetime of implemented batteries. This enables the deployment of such tags to be widely spread, as they need to be comparable in price with the traditional barcode systems. Obviously the tag is bounded from increasing the expense of the products which they are meant to identify, by anything noticeable to the consumer. A considerable gain would be achieved if the trade off between inductive and radiative RFID systems could be minimized, in the scenes that the positive effects by utilizing the inductive system could be capabilities of the radiative system as well. Hence rendering the tag selectivity of a near field system to apply in a far field communication, although multiple tags are in the vicinity of the reader represents an object of interest in the further work.

To reflect the preferred technology in the industry and introduce possible solutions to

systems that are significantly in use, the UHF passive tags are selected as the type, that this project will focus on.

In the following section, more concrete challenges when considering the UHF passive tags are discussed. A preliminary solution space will also be presented, in the effort to introduce an analysis of the relevant parts in a RFID system.

1.2 Preliminary solution space

As conducted in [4], the physical layer represents a field prone to improvements. Thus this section serves as a discussion and presentation of the preliminary solution space, regarding relevant challenges when considering RFID communication in this layer. Two methods are presented, to give basis for further analysis and how they are considered to contribute to the RFID technology.

1.2.1 Synchronous multi-carrier interrogation

A typical UHF RFID system is deployed in large warehouses, stores, package delivery firms among others, with heavy logistics. Common for all locations are the effects of the surrounding environment, in which the systems operate. When radio waves are induced in the air, they are reflected from concrete walls and metallic fixtures, causing multiple paths for the signal to reach the receiver. Each path of the signal differs in attenuation, phase shift and delay.

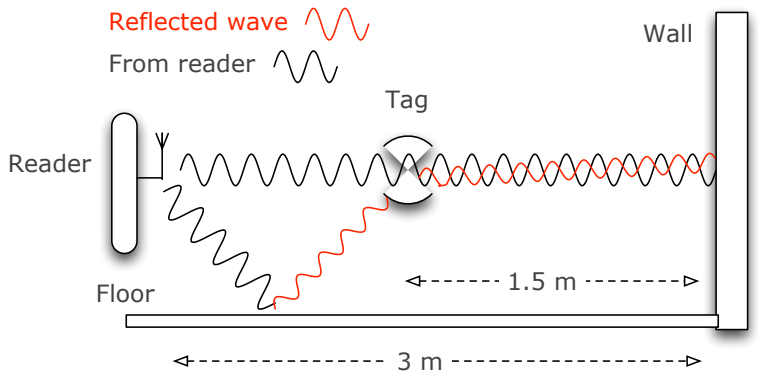

Figure 1.2: Illustration of a possible signal cancellation, killing the communication link between reader and tag.

This causes unwanted signal components from all the non direct paths, possibly adding destructively when the components are exactly opposite phase. As RFID communication is narrowband, the possibility of nearly complete cancellation may occur, making the phenomenon critical to the technology. A reader to tag communication link is illustrated by figure 1.2, communicating at a given frequency.

As the signal travels across the room it is reflected, thus hitting the tag from multiple directions. Three paths are illustrated, one direct path, one reflected from the wall behind the tag and one reflected from the floor. A simplified scenario but illustrates how the effects can decrease the performance.

The tags are developed as wideband receivers operating in the range of 860-960 MHz as illustrated by figure 1.3, where it is shown how different RFID frequency allocations are made across the globe. Hence to introduce robustness to the link, the nature of the tag design could possibly be exploited, as they at least respond in a 100 MHz band.

	North America	**Europe**	**Singapore**	**Japan**	**Korea**	**Australia**	**Argentina Brazil Peru**	**New Zealand**
Band size [MHz]	902–928	866–868	866–869 923–925	950–956	908.5–914	918–926	902–928	864–929 (parts)
Power	4W EIRP	2W ERP	0.5W ERP (2W in upper band)	4W EIRP	2W ERP	4W EIRP	4W EIRP	0.5–4W EIRP
Number of channels	50	10	10	12	20	16	50	Varied

Figure 1.3: Illustration of RFID frequency allocation - [13,p. 126]

This could be utilized at the reader by hopping to a different frequency in the available band, mitigating the occurrences of signal cancellation, as a frequency shift is proportional to a phase shift, enabling the reader to combat deep fades. Commercial readers utilize frequency hopping, but more as a method to reduce interference from other readers, hence classified as Dense Reader Mode.

If figure 1.2 is considered, the effect of a 15 MHz frequency shift can be argued with a small calculation. The path length difference between the direct wave and the wall reflected wave is 3 m. Deriving a phase shift introduced by the 15 MHz frequency hop is given by $2\pi(15\text{ MHz})(3\text{ m})/c = 54^\circ$, where c is defined as the speed of light ($\approx 3x10^8$ m/s).

If the discussed initiative where to be realized, it requires the reader to become aware of

a deep fade at the receiving tag to do the frequency hop. As this presents a considerable challenge and possibly also requires a change in the given RFID standard, it could be favorable to be considered in the context of a SIMO [1] system. This would enable a synchronous multi-carrier assisted communication between the reader and tag, where the wideband of the tag is utilized, to gain diversity without the knowledge of the occurrence of a deep fade. A possible message signal in a frequency selective channel is illustrated by figure 1.4, where a deep fade occurs at one of the carrier frequencies.

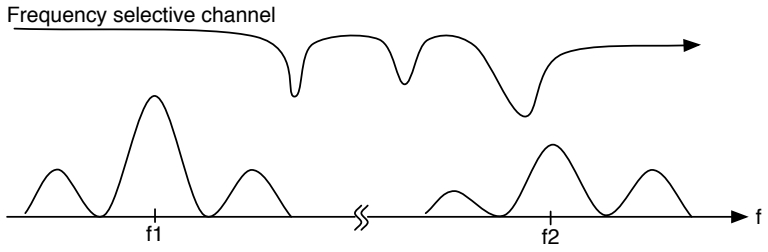

Figure 1.4: Frequency spectrum of a multi-carrier tag response, in a frequency selective channel

By the nature of the tags responding mechanism a multi-carrier system may operate in both uplink and downlink, as the tag is expected to respond on both frequencies, while in the mean time also be fed with power and data from both carriers. This is a non proven hypotheses that derives as a research element in this work. An initial parameter of an investigation towards an implementation, would be to know how rapid the channel changes, as it governs the minimum frequency spacing between the two carriers. Thus knowing the coherence bandwidth, represents the minimum frequency spacing required to obtain a desired diversity gain. Knowing the necessary frequency spacing provides only a small part of the solution, as the diversity effects in the tag represents the real challenges in obtaining the desired diversity gain. The tag consists of simple receiver technology, hence the behaviour of these components when exposed to a multi-carrier system becomes the main aspects.

[1] Single Input Multiple Output

1.2.2 Deliberate zero-point interference

As pointed out previously when considering RFID UHF systems, the ability to pinpoint the physical location of the exact tag that is being interrogated is limited, as the tags are in the far field region of the reader. This ambiguity in the system could in many cases be a factor desired to minimize, especially as the trend head towards item level tagging. For instance if the system operates in a shopping mall checkout, where products placed on a conveyer belt are to be detected, as shown on figure 1.5.

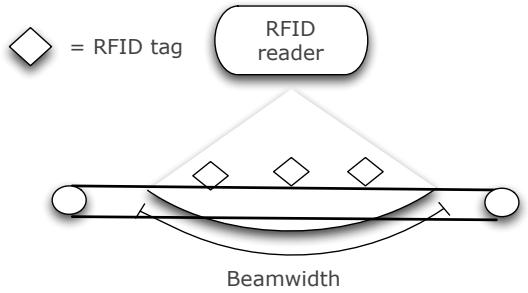

Figure 1.5: Illustration of a typical RFID reader interrogation zone due to beam width

In this situation it is not desired to get tag responses from neighbouring checkouts or even adjacent products on the moving belt, while the probability of not being able to read detuned tags, needs to be minimized. If detuned tags needs to be read with high probability, increasing the transmit power of the reader is an option. However typical readers have a directional patch antenna that is less than one wavelength across. This creates an large interrogation zone that could render the system unsuitable in cases like the checkouts, as the reader typically is designed to target a wide area. Thus, combining the increased transmit power with a patch antenna is sub-optimal in a case like this. Not only does the broad interrogation zones reduce the ability to suppress nearby tags or determine the position of the current tag responding, it also extend the probability of scattered reflections, that could lead to deep fades in the channel between tag and reader.

To address this effect large high gain antennas could be mounted on the front end of the RFID reader, creating a narrow beam. However a two-element array, could be utilised in the efforts to obtain a narrow beamwidth effect, by the use of software signal preprocessing.

Tags that are in close proximity to the reader, are able to respond if two conditions are met. Firstly the energy level in the signal from the reader needs to be sufficiently high for the tags internal circuity to power up. Secondly the signal quality required for the tag to properly interpret reader commands needs to be above some tag limitation, thus the

Signal to Noise Ratio (SNR) or Signal to Noise and Interference Ratio (SNIR) must be at a certain level. Hence these two parameters can be exploited when the interrogation zone is to be defined. The energy level in the air around the tag can be sufficiently high, however if the signal quality is low the tag may be energised while not responding due to not being able to decode instructions from the reader. When considering the two-element array that is assumed available at the front end of the reader, it is possible to introduce a sum and difference signal on each antenna element. This causes a scenario as depicted by figure 1.6, where an interrogation signal (S) creates a typical interrogation zone, where it is expected that tags reply with a high probability. However as the interference signal (I) is applied with a null-point in the center of S, the SNIR decreases in the boundaries of the interrogation zone. This causes the desired effect, as the energy level may be high enough to energies tag circuitry, but the interference signal decreases the SNIR, rendering the tag unaware of the read commands.

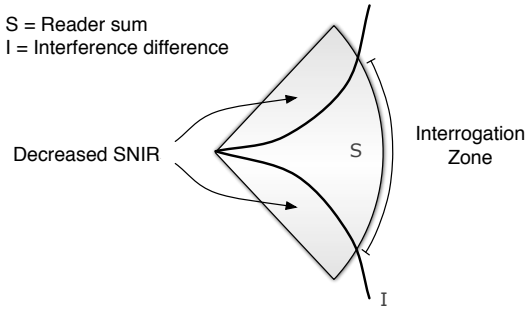

Figure 1.6: Illustration of reader and interference signal, causing a limited interrogation zone as the SNIR decreases at the boundaries

By utilising the two-element antenna array, the reader regains the ability to determine the location of the tag in an open environment and to suppress input from multiple tags in the vicinity, by broadcasting a linear combination of two signals. However it does not increase the directivity of the antenna, to gain an increased interrogation zone length. This method would also have an impact in the higher layers of the RFID protocol, as a tool to limit tag and reader collision assisting the ALOHA protocol. However is an aspect not to be considered further in this work.

Considerations in 1.2.1 and 1.2.2 towards improving the UHF RFID reader technology by introducing new elements in the physical layer has been presented. These considerations constitute the possibility of implementing synchronous multicarrier interrogation, while exploiting a multi antenna system to obtain interrogation zone control. These considerations leads to design objectives for the project in the following section.

1.3 Design objectives

In the preliminary solution space, it was discussed how different assets could be obtained in a RFID system, in terms of a multi-carrier interrogation reader for gaining frequency diversity and interrogation zone control by the use of a multi-antenna system. These assets leads to the following objectives for the project.

Multi-carrier RFID reader

A preliminary objective regarding the implementation of the just described features, to enable research regarding the operation and performance on live UHF tags, is to implement a RFID reader capable of communicating with live EPC Gen2 tags.

Further to introduce frequency diversity at the RFID system, the following bullet points are specified:

- Implementation of a RFID reader, capable of radiating RFID message signals on two independent carriers, with a frequency spacing that surpasses the coherence bandwidth of a given channel.
- A RFID reader system that is capable of receiving tag response backscattered on the two carrier frequencies, with enabled decoding of both tag message signals simultaneously.

The main focus when considering the diversity gain scheme, is noted to be on the downlink. Thus providing frequency assistance to the tag decoding performance. It is expected that the tag responds on both frequencies due to its response mechanism, hence a traditional diversity scheme could also be considered in the reader.

In the deliberate interference case the reader is aimed to be expanded with the following key features:

Deliberate interference RFID reader

- Implementation of a RFID reader, with interrogation zone control via controlled interference.
- A system with multi-antenna element transmission
- Each transmission chain is gain and phase controlled independently.

A common feature for both aspects is a link quality measure. Hence a signal to noise ratio (SNR) or received signal strength indication (RSSI) measure is relevant.

The following chapter contains aspects regarding the further analysis of a RFID system that needs to be conducted, to gain information on the physical layer of a reader.

2 System architecture

In this chapter, a basic system architecture of how a RFID system is composed, is presented. This act only as a overall illustration of the physical layer, as commercial RFID reader schematics on a block diagram level, has shown to be unobtainable. However the purpose of the schematic is to illustrate how the proposed additions to an RFID system, can be implemented, thus the basic components should suffice. The standard system is illustrated by figure 2.1.

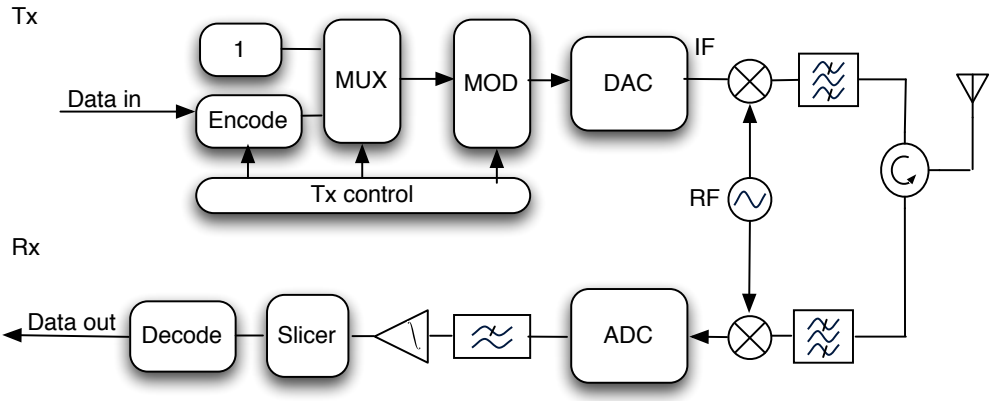

Figure 2.1: The basis block diagram of how a standard RFID reader system may be constructed in the physical layer.

It is noted that the presented architecture is a mono-static reader, as a single antenna element is used for both the TX and RX chain. To gain a higher receiver sensitivity a bi-static system, where two elements are used, is in many cases desired.

In 1.2.1, the concept of a multi-carrier reader was presented. This concept could be incorporated in the just presented standard reader, as illustrated in figure 2.2. The second carrier may be modulated, or just a pure sinusoid, hence a switch is illustrated from the Tx chain on to the second oscillator. The effects of the second carrier being modulated or not, involves considerations towards gaining both up and downlink diversity. The Rx chain is considered to be identical to the standard Rx chain, if uplink diversity is not considered.

Furthermore hardware for the deliberate interference subsystem is added to the standard Tx architecture in figure 2.3. This creates a reader with the ability to mimic a high directional antenna array, with only two elements, due to the interference cancellation in the

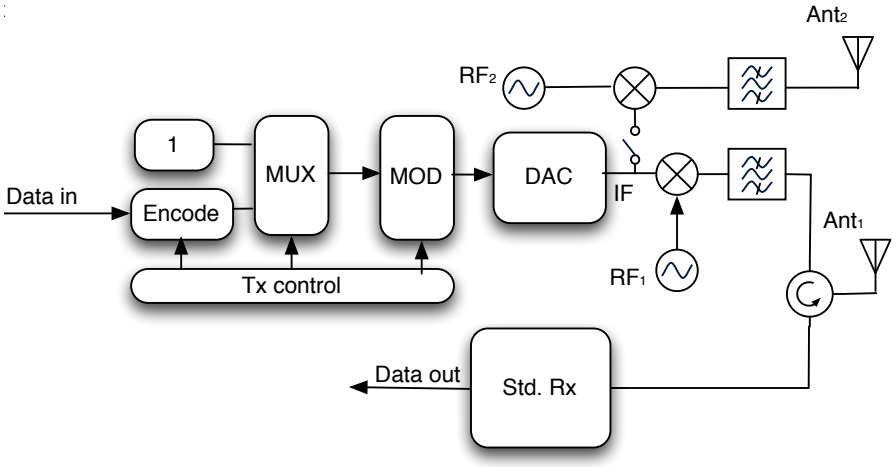

Figure 2.2: The basis block diagram of the standard RFID reader, with proposed hardware for implementing the multi-carrier system

broadside direction. Again the standard Rx chain is used, as no changes in the receiver is necessary with the proposed system.

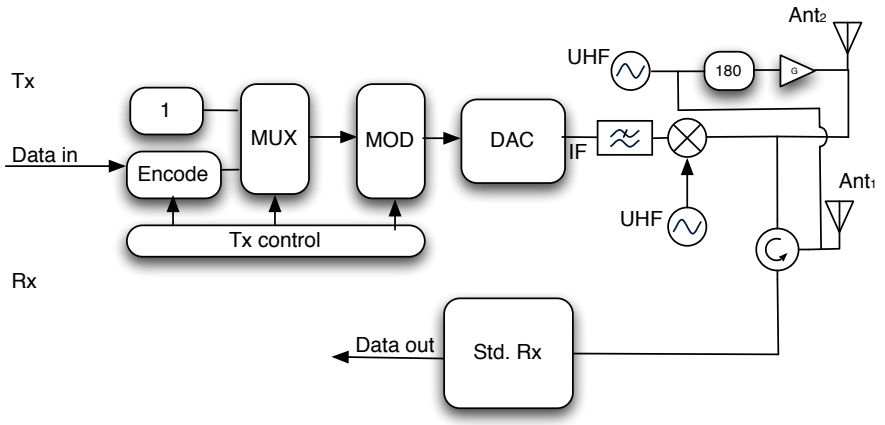

Figure 2.3: The basis block diagram of how a standard RFID reader system may be constructed in the physical layer.

EPC Class1 Gen2

To get an quick overview of the relevant parameters and concepts in the EPC Gen2, this chapter describes the RFID standard with a focus on the reader to tag and tag to reader communication. Elements that are noted in this section are of importance to the development of the possible solutions in this work.

RFID Protocol

The EPC Gen2 standard governs the communication between reader and passive UHF tags in the 900 MHz band and is a reader-talks-first protocol. Information from reader to tag is conveyed by modulating an RF signal, from where the tag is also energised. The reader transmits a continuous wave (CW) in the full communication session to insure that the tag remains energised. In the uplink the CW is then modulated by the antenna reflection coefficient of the tag antenna, causing a backscatter modulation. The parameters that constitutes this communication are presented in the following.

3.1 Reader to Tag

When considering the reader to tag communication link, also referred to as the downlink, it is noticed that every initiative taken in the protocol is for the complexity of the tag to be held at a minimum on the cost of complexity at the reader.

The basis flowchart of a reader is depicted on figure 3.1, where it is seen that the reader consists of an encoder, filtering and the modulator. These elements are addressed in the following headlines.

RT Data encoding

To comply with the EPC Gen2 standard, encoding of the binary data stream at the reader, is to be handled by the use of Pulse Interval Encoding (PIE). By this scheme, the information is carried by the duration of the encoded symbols. Each bit it mapped as illustrated

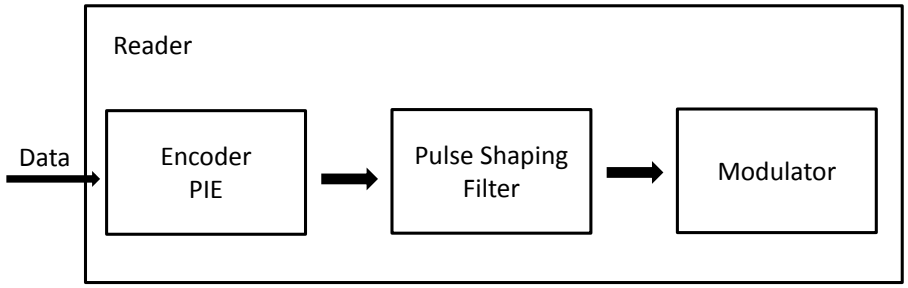

Figure 3.1: Illustration of a basis reader transmission train

by figure 3.2, where 1-Tari indicates a data-0 and data-1 varies from 1.5 to 2 Tari. Tari is the time unit reference chosen by the reader and goes from 6.25 μs to 25 μs [1], thus data rates ranging from 26.7 kbps to 128 kbps. This type of encoding ensures that tags stay energised, even if a series of symbols with low energy is send, hence creating a average energy level of 63 %. The specified tolerance for the unit Tari is -+1%.

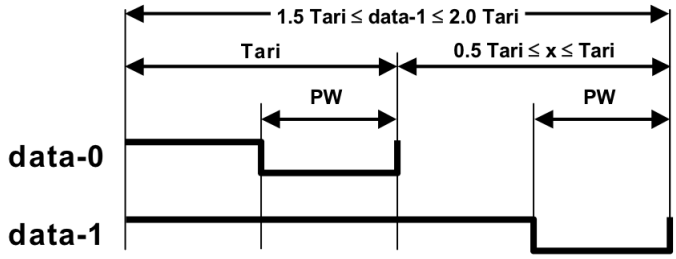

Figure 3.2: Illustration of PIE symbols in reader to tag communication [1,p. 42]

RT Modulation

The modulation form governed by the standard can be a variety of Amplitude Shift Keying (ASK), in terms of Double-Side-Band-ASK (DSB-ASK), Single-Side-band-ASK (SSB-ASK) or Phase Reversal [1]. The RF envelope of the reader to tag link is illustrated by figure 3.3

The DSB-ASK is the conventional modulation form, where the message signal produced by the encoder, modulates a carrier [17]. The DSB-ASK is easily implemented, however it has poor spectrum utilization, as it consumes twice the bandwidth of the baseband message signal. As the double side band signal is symmetric around the carrier frequency, it is possible to suppress the upper or lower side band. This is obtained by the quadrature signal being the Hilbert transform of the in-phase signal rendering a SSB-ASK signal [17,p. 88]. This reduces the consumed bandwidth of the modulated signal to be equal the baseband signal. It is noted that both DSB-ASK and SSB-ASK does not require a

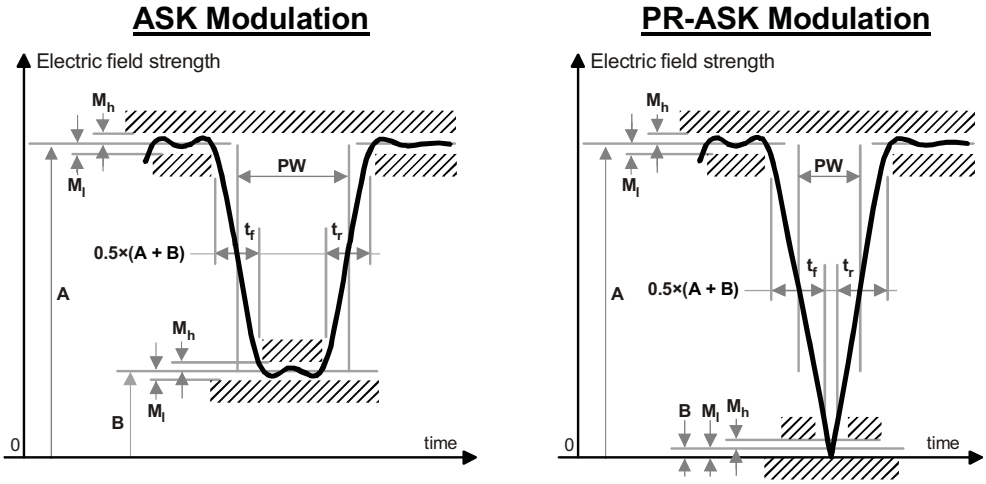

Figure 3.3: Illustration of the modulation RF envelope in reader to tag communication [1,p. 42]

coherent demodulator. The PR-ASK modulation scheme is obtained by phase inversion at the end of each baseband symbol.

The modulation depth is defined as $\frac{A-B}{A}$, where A and B are defined on figure 3.3, as the highest and lowest amplitude level of a symbol. The depth in percent is required in the interval 80% to 100%.

3.2 Filtering

As depicted in figure 3.1 a pulse shaping filter is implemented in the reader transmitter train, to satisfy the ripple requirements of the EPC Cen2 standard. The RF envelope ripple is bounded by $0.05(A-B)$ V/m, in terms of M_h and $mathrmM_l$ shown on the ASK modulation in figure 3.3. A Raised Cosine filter enables to meet this requirement when the roll-off factor is 1 [10,p. 96].

3.3 Tag to Reader

When considering the tag to reader communication link, very few resources are available for this communication to take place and furthermore to be successfully demodulated and decoded at the reader. The tag has a communication flow graph as illustrated in a simplified version by figure 3.4, where an Encoder and a Demodulator is the only components relevant to highlight in conjunction with the EPC Gen2 standard.

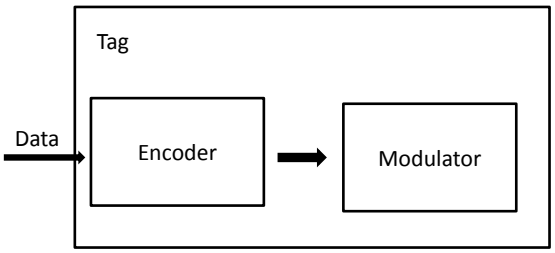

Figure 3.4: Illustration of the tag communication modules

TR Modulation

The modulation form of the passive tag is characteristic as it utilises the principle of antenna reflection coefficient modulation as a backscattering technique. The tag modulates the incoming wave from the receiver, by the use of modulating its antenna impedance, thus the modulation form is ASK. However PSK can also be utilized by the tag, although the phase is not shifted a complete 180^o.

TR Data Encoding

The encoding from the tag in the uplink communication can be ether FM0 or Miller sub-carrier encoding. The FM0 encoding introduces phase inversion at the end of every symbol, and a phase transition in the middle of a data-0 symbol, where as data-1 has no transition. This is depicted by figure 3.5. The FM0 encoding produces the highest data rate, with accordingly lower robustness towards decoding errors.

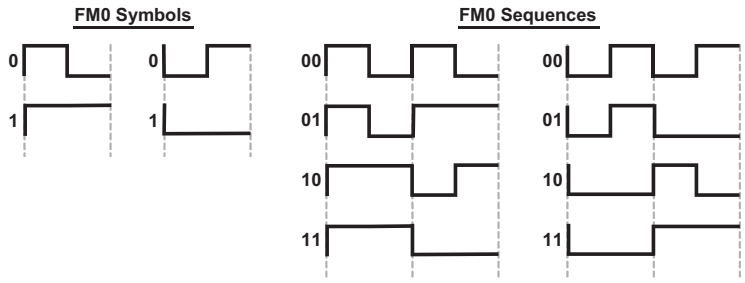

Figure 3.5: Illustration of FM0 data symbol encoding

Miller coding enables the use of sub carrier sequences, as each bit can be encoded to consist of 2, 4 or 8 cycles. This reduces the transmission rate, however introduces more resiliency as there are more subcarrier cycles per bit . The different miller encodings are depicted by figure 3.6

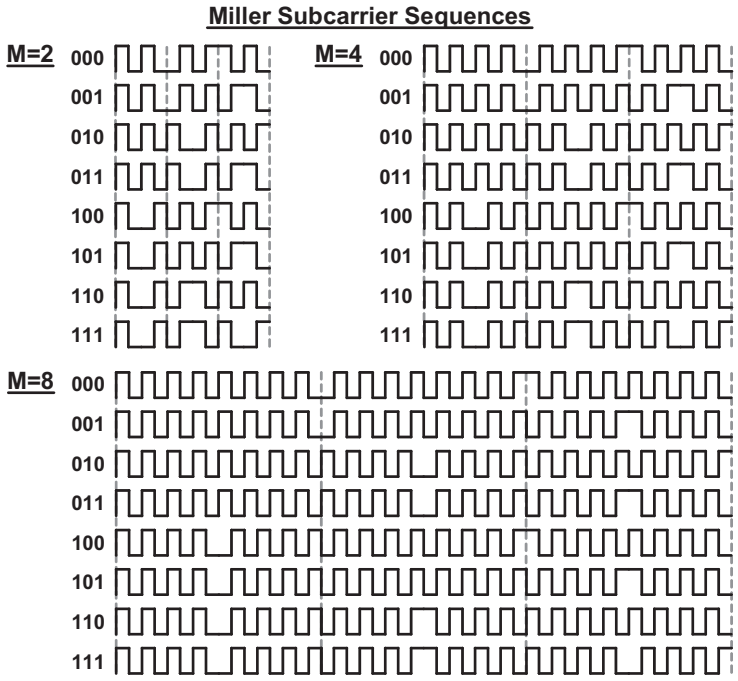

Figure 3.6: Illustration of the different miller type data encoding, with different subcarrier cycles per symbol.

RT Preamble

To initiate every packet from reader to tag, a preamble is used to set different parameters for the uplink. This enables the reader to set the subcarrier frequency (SCF) from 40 kHz to 640 kHz, the miller index M between 1, 2, 4, 8 (where 1 = FM0) and a tag to reader calibration symbol, TRcal. The backscatter link frequency is derived as

$$\mathrm{BLF} = \frac{\mathrm{SCF}}{\mathrm{M}}$$

where

$$\mathrm{SCF} = \frac{\mathrm{DR}}{\mathrm{TRcal}}$$

Timing requirements

Without further details about the higher layers of the EPC Gen2 protocol, it is necessary to address requirements that are driven from the MAC layer. In shot the MAC layer handles the scenario of multiple tags being in the vicinity of the reader, to reduce the

risk of tag collisions. To limit this situation a form of handshake control is implemented, as a tag reply a random 16 bit number (RN16), that is then decoded and echoed from the reader in terms of an acknowledge (ACK) command. When the tag receives the ACK, and verifies the transmitted RN16, it backscatters its ID. The standard specifies T1 and T2 as part of the timing requirements for the tag and reader response respectively. Hence these parameters are the timing between dependent transmissions, such as the ACK reply to a RN16 tag response. T1 is specified as being 10 times the period of a SCF cycle (40 kHz - 640 kHz), which represents the time a tag has to begin its response to a reader command. If the SCF is set to 40 kHz, T1 = 250 μs, where as at 640 kHz, T1 = 15.6 μs. The reader is required to introduce a response to the tag, within 20 times the uplink frequency, thus allowing delays of 500 μs and 31.25 μs respectively. These timing requirements are essential to the systems performance.

The main concept of a RFID interrogation shoud be clear from the presented chapter. The main parameters are highlighted as being the modulation types, modulation depths and timing requirements. The following chapter presents the channel in which the communication takes place.

4 Channel model

In this section the channel model between the tag and reader is described. The focal point being the deduction of the coherence bandwidth, as it constitutes a key element in gaining frequency diversity.

When a transmitted signal is propagating towards the receiver, it follows different paths, before arriving at the receiving antenna. The variation of these paths, in terms of length and attenuation results in fluctuations of the received signal strength. This aspect of the channel is referred to as multipath fading effects. As the channel between the transmitter and receiver changes with time, its influence on the transmitted signal is unpredictable, hence statistical measures are used to predict behaviour of such multipath effects.

The channels statistical measures used in case of a narrowband signal is initially presented, to support the later wideband case.

Firstly let the communication link of an RFID setup be presented by figure 4.1. This illustrates how the source signal $s(t)$ from the reader, is influenced by the channel $h(t)$, causing the resulting signal $x(t)$ at the receiver. In the time-domain this relation is argued by the convolution,

$$x(t) = s(t) * h(t) \tag{4.1}$$

Figure 4.1: A block diagram illustrating the input/output variables of reader/tag communication link

In the narrowband case the channel gain is the only parameter to be considered. Thus let the transmitted signal be defined as

$$s(t) = A\cos(2\pi f_c t) \tag{4.2}$$

then in therms of the in-phase and quadrature components the received signal can be denoted by [16,p. 73]

$$x(t) = I(t)\cos(2\pi f_c t) - Q(t)\sin(2\pi f_c t) \tag{4.3}$$

where

$$I(t) = \sum_{i=1}^{N} |a_i| \cos[-2\pi v_m a x \cos(\gamma_i)t + \varepsilon_i] \tag{4.4}$$

$$Q(t) = \sum_{i=1}^{N} |a_i| \sin[-2\pi v_m a x \cos(\gamma_i)t + \varepsilon_i] \tag{4.5}$$

$a_i(t)$ being the attenuation factor for the signal received from the i'th path, and ε_i is the phase and γ_i is the angle from the incident wave to the direction in witch the receiver moves.

As both the in-phase and quadrature components are a sum of multiple random variables, then by the virtue of the central limit theorem they both follow a Gaussian distribution defined by the the probability density function (pdf)

$$f_x(x) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{x^2}{2\sigma^2}\right) \tag{4.6}$$

From this, the distribution function of the received envelope can be deducted. There are generally two scenarios when considering the envelope distribution. It can be defined when no dominant component is evident, typically when transmitter and receiver lacks a line of site (LOS) path, defined as the well known Reyleigh distribution

$$f(r) = \frac{r}{\sigma^2} exp\left(\frac{-r^2}{2\sigma^2}\right) \tag{4.7}$$

where as if there is a dominant component, the envelope follow the Rican distribution

$$f(r) = \frac{r}{\sigma^2}\exp\left(-\frac{r^2+A^2}{2\sigma^2}\right) I_0\frac{rA}{\sigma^2} \tag{4.8}$$

I_0 refers to the modified Bessel function with order zero and A denotes the non-zero mean.

As noted earlier the key element is to derive an expression of the coherence bandwidth of the channel. To do so we expand our consideration to the wideband case. Here the channels impulse response (CIR) $h(\tau)$, is influenced by not only a single delay element, but due to the multipath effects the channel induces memory. Instantiated by dispersion in time, this leads the CIR to be defined in the time invariant case as

$$h(\tau) = \sum a_i \delta(\tau - \tau_i) \tag{4.9}$$

Considering the channel as being time variant defines the two-dimensional complex CIR as being

$$h(t,\tau) = a_i(t,\tau) exp(-j2\pi f_c \tau) \tag{4.10}$$

From the one-dimensional CIR the power delay profile (PDP) can be derived from

$$p(\tau) = |h(\tau)|^2 \tag{4.11}$$

Hence in the two-dimensional CIR case the PDP, can be derived by integrating with respect to t

$$p(\tau) = \int_{-\infty}^{\infty} |h(t,\tau)|^2 dt \tag{4.12}$$

The standard deviation of the PDP is utilized in determining the coherence bandwidth of the channel. The PDP can be interpreted as the PDF of the channel, if it is normalised with respect to its zeroth-order moment.

$$P_m = \int_{-\infty}^{\infty} p(\tau) d\tau \tag{4.13}$$

The first-order moment, being the mean delay, derives as

$$T_m = \frac{\int_{-\infty}^{\infty} \tau p(\tau) d\tau}{P_m} \tag{4.14}$$

Finally deriving at the rms delay spread as

$$\sigma_\tau = \sqrt{\frac{\int_{-\infty}^{\infty} \tau^2 p(\tau) d\tau}{P_m} - T_m^2} \tag{4.15}$$

In terms of the statistical boundaries it is assumed that the time varying channel $\tilde{h}(\tau;t)$ is considered to be a wide-sense stationary (WSS) process, as only the first and second order moments do not vary with respect to time t. Furthermore the attenuation and phase shift is considered to be independent, thus it is assumed to be uncorrelated scatter (US). These assumptions together produces the widely used WSSUS model, also assumed here for the following derivation of coherence bandwidth to be valid.

The coherence bandwidth B_{coh}, is often defined as the bandwidth in which two narrow-band signals with $\Delta f = f_2 - f_1$ is correlated by some factor ρ_{coh}. The correlation coefficient between f_1 and f_2 with a rms delay spread σ_τ can be deducted from the following [16,p. 240]

$$\rho = \frac{I_0^2(k_0 v \tau)}{1 + (2\pi)^2 \sigma_\tau^2 (f_2 - f_1)^2} \tag{4.16}$$

Again I_0 is the zero order Bessel function, k_0 is the wave number, v is the velocity and τ the time delay between the two transmitted signals. An often used correlation coefficient is set to 0.5 and with zero temporal separation (no time delay between f_1 and f_2), the Bessel function reduces to unity. B_{coh} can then be resolved by evaluating equation (4.17)

$$0.5 = \frac{1}{1+(2\pi)^2\sigma_\tau^2(B_{coh})^2}$$

$$B_{coh} = \sqrt{\frac{1}{1+(2\pi)^2\sigma_\tau^2 0.5}} \tag{4.17}$$

The coherence bandwidth can then be defined as a frequency range where all frequency component correlates by a given correlation factor, typically set to 0.5. Hence B_{coh} being the 3-dB bandwidth of the correlation function. It is noted that the temporal separation can be directly converted into spacial distance, if to radiating elements are used, however needs to be omni-directional [15,13A]

It is specified that a limitation when operating the RFID reader system both regarding the multi-carrier diversity and the deliberate interference interrogation, is that the surrounding channel becomes as controlled as possible. This leads the coherence bandwidth to be an estimate of the channel correlation function in a typical Reader/Tag communication environment. Hence from [12,p. 1246] a 0.5 correlation coefficient is estimated to a typical 6 MHz minimum frequency spacing. It is however chosen to operate the system with a 10 MHz spacing, when relevant.

5 Concept theory

5.1 Deliberate Interference

As is described in the preliminary solution space, the ability to control the interrogation zone of the reader is a desired feature. This can be utilized in spatial tag singulation, introducing multiple applications for the RFID technology. This section derives the analytical considerations towards obtaining such feature in a live UHF RFID system.

Recall the two conditions required for a tag to respond as being a sufficient energy level β, for powering up the tag circuitry and a sufficient SNR γ, to enable a successful decoding. Let γ be defined as

$$\gamma = \frac{S}{N}$$

Where S is the desired signal power and N is the noise power.

A typical reader uses a directional patch antenna or dipole to radiate the interrogation signal towards tags, for them to obtain values of β and γ that surpasses some required thresholds, enabling a response. These thresholds are a field of development, and changes from tag to tag. A typical value for β is ≈ -10 dBm [5], with new tags down to as low as - 18 dBm. γ is expected between 10 - 30 dB [11,p. 2]. An illustration of a patch antenna radiation pattern is given by figure 5.1, where the possible tag response area is determined by the SNR and power requirements of the tag. Hence the angle ϕ is an expression of the interrogation zone, as a function of β and γ.

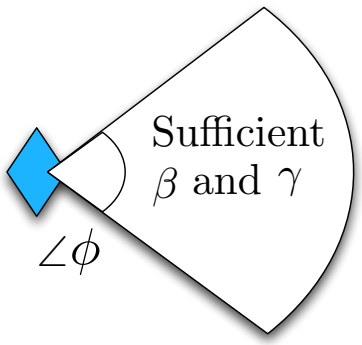

Figure 5.1: An illustration of the tag response enabled area of a typical RFID reader with a broad radiation pattern

What is relevant in the context of gaining control of the interrogation zone, is then to control the parameters β and γ to obtain a decremented ϕ. The power required for the tag to energize its internal components can very well be met, however if the SNR conditions at the tag are poor, the tag is unable to interpret the commands from the reader. Thus, if β is high enough for the tag to get energized the only parameter controlling ϕ is γ. The desired event is to obtain a small angle ϕ, where a high SNR is obtained in that angle span only. However they constitute each others opposite, as tuning for a high electrical field from the reader to obtain sufficient SNR, causes an extended interrogation zone angle ϕ. To circumvent this we introduce SINR. SINR is defined as

$$\text{SINR} = \frac{S}{N+I}$$

S is the signal power, I the interference power and N the noise power. This causes the total received power at the tag to be a sum:

$$\text{Tag}_{tot} = S_p + I_p + N_0 \tag{5.1}$$

S_p is the power received from the reader, I_p is the interference power and N_0 is the noise power. Hence this leads to the tag being sufficiently powered if $Tag_{tot} > \beta$. However if I_p gets to dominant, the requirements for the SNR/SINR is not met, thus the tag is powered but is unable to decode and respond. With a fair approximation it can be assumed that $I_p >> N_p$, thus the SINR can be reduced to SIR. Let the requirements for SIR equal the requirements for γ, and the interference signal be a controlled parameter, hence can be utilised in the effort to introduce a controlled interrogation zone.

When considering a tag's signal level requirement, the power from the reader received by the tag is of interest. This is in general determined by the use of Friis Transmission Equation defined in equation (5.2) [2,95], where P_r is the power delivered to the receiver load and P_s is the input power to the reader antenna.

$$\frac{P_r}{P_t} = e_{cdt} e_{cdr} (1 - |\Gamma_t|^2)(1 - |\Gamma_r|)^2 \left(\frac{\lambda}{4\pi R}\right)^2 D_t D_r |\rho_t \cdot \rho_r|^2 \tag{5.2}$$

The term $\left(\frac{\lambda}{4\pi R}\right)^2$ is defined as the free-space loss factor. If it is assumed that the radiation efficiency $e_{cd(t/r)}$ is unity (no conduction-dielectric losses), the polarization of the

transmit and receive antenna is matched ($\rho_{t/r} = 1$) and the loads/lines are matched to the antennas, equation (5.2) reduces to

$$\frac{P_r}{P_t} = \left(\frac{\lambda}{4\pi R}\right)^2 G_t G_r \tag{5.3}$$

However Friis transmission equation is classified as a point to point measure. In this case the power delivered in relation to the angle ϕ is of interest. The transmit antenna gain factor becomes angle-dependent, deriving the received power at the angle ϕ in the azimuth plane, as

$$P_r(\phi) = \left(\frac{\lambda}{4\pi R}\right)^2 G_t(\phi) G_r P_t \tag{5.4}$$

As G_t describes the directional redistribution of the power, that is feed to an antenna element, this dictates the interrogation zone. As it is described in equation (5.1), the tag receives the sum of powers, induced by the reader signal, interference and noise power. As stated earlier the noise power is neglected, thus let the total power be $S_p + I_p$. Is is assumed that S_p alone induces enough power in the air, to power the tag if it is located within the Half-Power Beam width (HPBW), as depicted by figure 5.2, introducing an interrogation zone of say $\phi = 60°$.

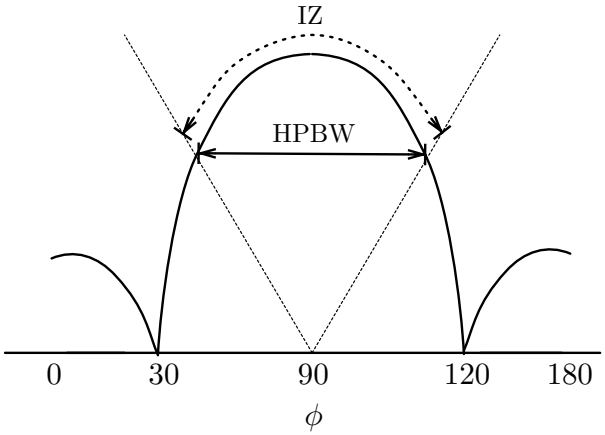

Figure 5.2: Illustrating the interrogation zone of a reader, in which the tag is able to respond.

However if the SIR relation is considered in terms of $G_t(\phi)$, the received power by the tag in terms of both the signal and the interference power can be addressed by letting equation

(5.4) describe the relation between the two powers in terms of SIR:

$$\mathrm{SIR}(\phi) = \frac{P_{r-s}(\phi)}{P_{r-i}(\phi)}$$

$$\mathrm{SIR}(\phi) = \frac{\left(\frac{\lambda}{4\pi R}\right)^2 G_{t-s}(\phi) G_r P_t}{\left(\frac{\lambda}{4\pi R}\right)^2 G_{t-i}(\phi) G_r P_t} \tag{5.5}$$

where $P_{r-s}(\phi)$ is the power received from the interrogation signal, $P_{r-i}(\phi)$ is the power received from the interference signal at the angle ϕ. Hence it is a matter of introducing the interference signal in certain areas to decrease the SIR. To illustrate an example let the reader radiation pattern be similar to the one shown in figure 5.2, but now let an interference signal be introduced in terms of a radiation pattern with a null in $\phi = 90^\circ$. Utilizing a null is desired as it provides a narrow pattern, well suited for the purpose of creating a limited filed of readability. The antenna array excitation behavior is described in more details in appendix E.

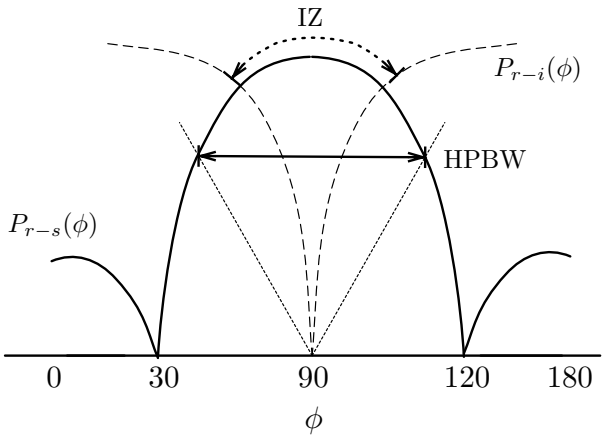

Figure 5.3: An illustration of a limited tag response enabled area, due to the introduction of a controlled interference signal with a null at $\phi = 90^\circ$

From the deducted theory it should be clear how the SIR requirement is not met, in the area where the interference signal has its dispatched power, hence a limited angle of enabled tag readability is obtained. The following section presents the theory of the Multi-carrier interrogation proposal.

5.2 Multi-carrier interrogation

This section serves to present the theory of a downlink frequency diversity scheme.

In chapter 4 the channel between the reader and tag is desribed with theory of how the communication is exposed to fading as a result of the multipath effects. These effects are degrading to the performance of the system, as a tag could potentially be located in a deep fade. Hence the concept of providing the receiver (tag or reader) with a replica of the same signal, decreases the chance of detection error as the probability of all the signal components being in a deep fade is inverse proportional to the number of signals. Let the probability of a signal being in a deep fade be denoted by p, then p^L is the probability that all L independently fading replicas will be influenced by the same fade. The method to introduce these replica of the signal in an RFID system, is to employ frequency diversity where the same information signal is transmitted on L carriers. To ensure that the different carriers do not experience equal fading, the frequency spacing must be greater than the coherence bandwidth, thus

$$\Delta f_c >> B_{coh}$$

When obtaining two or more signal copies from different carrier frequencies, the simplest form of diversity is to switch between the carriers. This can be a controlled process where the receiver measures the SNR on all carriers, thus picking the best (selection), or it can be switched diversity, where the receiver randomly jumps to the next frequency, if SNR conditions are poor on the current. However in these schemes signal energy is wasted as all other information bears then the one currently selected, is discarded. An alternative method is to utilize combining diversity. Here all information is exploited, where in its simplest form denoted by Equal Gain Combining, every signal is phase corrected and added. The signals then add coherently where as the noise adds incoherently. A superior combining scheme is the Maximum Ratio Combining, where each signal copy is weighed in accordance to there amplitude. Here the resulting SNR conditions at the receiver constitutes the sum of all SNR's as

$$\gamma_{MRC} = \sum_{n=1}^{N} \gamma_n \tag{5.6}$$

where N is the number of received signals.

From [16,p. 254] the general expression of the pdf for all inputs is derived as

$$pdf_{\gamma} = \frac{1}{N_r - 1} \frac{\gamma^{N_r - 1}}{\bar{\gamma}^{N_r}} \exp - \frac{\gamma}{\bar{\gamma}} \tag{5.7}$$

where $\bar{\gamma}$ is the mean SNR. It is assumed that the SNR distributions of each signal is Rayleigh fading.

From the pdf, the cumulative distribution function (cdf), can be deducted and plotted, to reveal the diversity gain trend when the amount of redundancy increases. This is shown in figure 5.4. It is noted that the diveristy gain is evident by the slope of the cdf, also refeered to as distribution compression, as the variance is minimized.

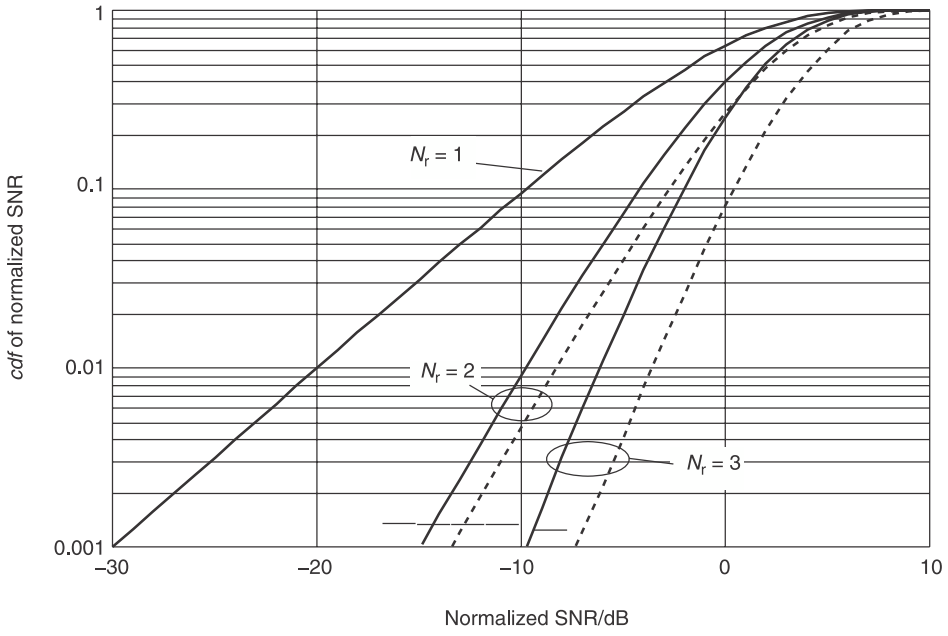

Figure 5.4: Illustration of the cdf of the normalized SNR ratio for selection diversity as the solid lines and MRC as the dashed lines [16,p. 255]

In the case of downlink frequency diversity, the tags low complexity prohibits the use of traditional diversity schemes such as MRC or EGC. Hence the reader is the only part of the system, that can be altered to enable such communication benefits. A basic tag frontend circuitry basically consists of a rectifier, an envelope detector and a low pass filter (LPF), as illustrated by figure 5.5. As noted earlier the energy level obtained from the CW and the SNR/SNIR conditions of the transmitted data, is the two main parameters targeted for

improvement. A hypothesis set, arguing to do so in a frequency diverse manner, is to let the reader transmit a modulated carrier in combination with an unmodulated carrier, that both lies within the bandwidth of the tag. This may increase the receptive energy level of the tag, while still preserve spectrum usage to a minimum. However the data decoding in the tag, is not assisted by the second carrier if not both carriers are modulated, creating information redundancy.

By the means of a standard datasheet of a commercial tag, it is not possible to define exact values of the components, that compose the envelope detector, nor the LPF. However assumptions about the system can be made, on a basis of the signals that must pass through it. Firstly it must be assumed that the envelope detectors time constant satisfies the following inequality

$$\frac{1}{f_t} \ll \tau_{RC} \ll \frac{1}{\Delta f}$$

where τ_{RC} is the time constant of the envelope detector, f_t is the main carrier frequency of the reader, and $\Delta f = |f_t - f_c|$ denotes the frequency difference, where f_c is the second carrier frequency. Furthermore the LPF can be characterized by the maximum downlink datarate, noted in section 3 as being 128 kbps. As the modulation is a simple two state ASK, the bit rate equals the symbol rate, hence the message bandwidth $M_{bw} = 128$ KHz. From this it is clear that the time constant of LPF needs to fulfill $\tau_{LPF} \ll \frac{1}{M_{bw}}$. In addition it is noted that the cut-off frequency must be greater than Δf, to suppress intermodulation products of the two carriers[8,p. 57].

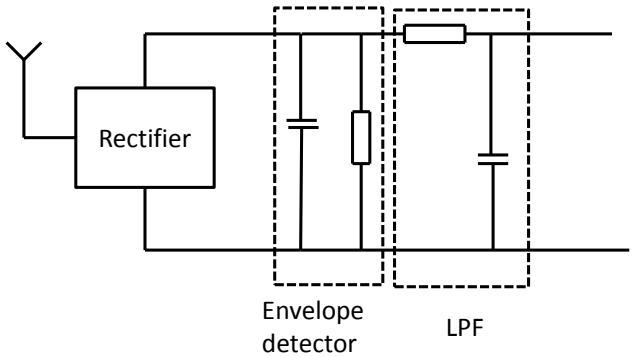

Figure 5.5: Tag front-end components

In the case of modulating the transceiver carrier only, let the received signal at the tag be denoted

$$s(t) = m(t)\cos(2\pi f_t t) + A\cos(2\pi f_c t + \phi(t)) \tag{5.8}$$

where $m(t)$ is the primary message signal from the transceiver modulated onto the carrier frequency f_t. A is the amplitude level of the secondary carrier f_c and $\phi(t)$ is the phase difference between the two carriers.

The signal passes the envelope detector, thus outputs as [9]

$$|s(t)| = \sqrt{m^2(t) + A^2 + 2Am(t)\cos(2\pi\Delta f t + \phi(t))} \tag{5.9}$$

where $\Delta f = |f_c - f_t|$

Using the Taylor series

$$\sqrt{1+x} = 1 + \frac{1}{2}x - \frac{1}{8}x^2 ... + remainders \tag{5.10}$$

$|s(t)|$ can be written as

$$\begin{aligned} |s(t)| = r(t) = \sqrt{A^2 + m(t)^2}\Bigg(1 + \frac{1}{2}\left[\frac{2Am(t)\cos(2\pi\Delta f t + \phi(t))}{\sqrt{A^2 + m^2(t)}}\right] \\ - \frac{1}{8}\left[\frac{2Am(t)\cos(2\pi\Delta f t + \phi(t))}{\sqrt{A^2 + m^2(t)}}\right]^2 + remainders\Bigg) \end{aligned} \tag{5.11}$$

Further processed by the LPF in the tag, the resulting signal is striped of its high frequency components, deriving as [9]

$$r_{LP}(t) = \sqrt{A^2 + m(t)^2}\left(1 - \frac{1}{4\sqrt{A^2 + m(t)^2}}\right) \tag{5.12}$$

In chapter 3 it is noted that the modulation depth (MD) of a R-T command needs to be larger than 80 % and smaller than 100 %. Also from chapter 3 MD is derived as

$$MD = \frac{E_{max} - E_{min}}{E_{max}} \tag{5.13}$$

E_{max} denotes the maximum electrical field strength of the RF envelope, and E_{min} denotes the minimum. The power ratio of the two carriers needs to be carefully chosen, to meet the MD requirement.

(5.13) can be used together with (5.12), to set an expression for the MD of the multi-carrier system as [8,p. 3]

$$\frac{\left(\sqrt{m(t)^2 + A^2} - A\right)}{\sqrt{m(t)^2 + A^2}} \tag{5.14}$$

In a similar fashion the derivation can be made when both carriers are modulated, so equation (5.14) becomes

$$\frac{\left(\sqrt{2m(t)^2} - m(t)\right)}{\sqrt{2m(t)^2}} \tag{5.15}$$

In addition to the modulation depth, the frequency difference between the two carriers $\Delta f = f_c - f_t$ needs to be customized to enable proper perception, in terms of minimizing the effects of the beat frequency, given by

$$f_b = |f_c - f_t|$$

The frequency components, being at the sum and difference frequency, received by the tag when both carriers are transmitted is illustrated by figure 5.6.

When the signal has passed the LPF in the tag front-end, the high frequency components are removed. If the frequency spacing of the two carriers is two small, the resulting beat frequency introduces a frequency components that interferes with the message signal from the reader. Thus it is crucial to select Δf to be larger then the cut off frequency of the LPF in the tag.

As the cut off frequency of the tag is not known, an estimated can be made from the

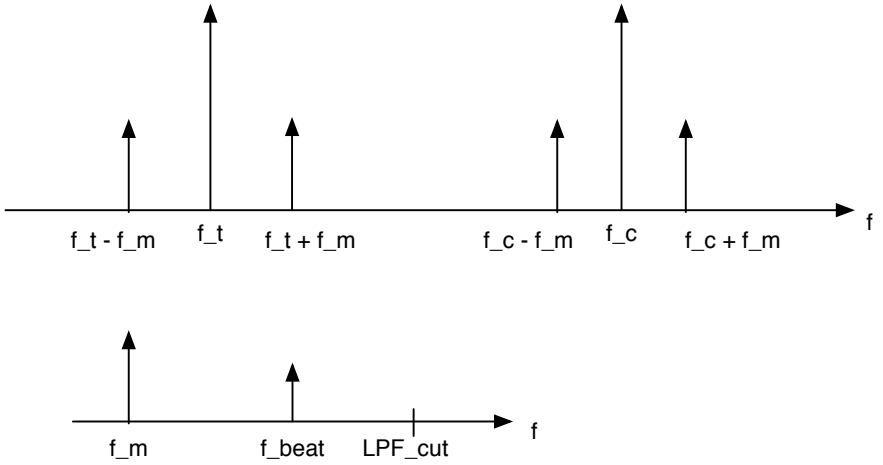

Figure 5.6: Frequency spectrum of the receiver signal, and the filtered signal with the beat frequency being to small

bandwidth occupation, when the highest data rate is being used in downlink. Although it is assumed that the frequency spacing used to fulfill the coherence bandwidth is sufficient, to maintain the beat frequency above the LPF cut off frequency.

The concept theory is derived, where the different parameters for the two concepts are specified, enabling an actual implementation of the proposed systems. The available platforms and the considerations made towards selecting a suitable platform on behalf of theory derived until now, is to follow.

6 Platform considerations

This chapter serves to clarify the hardware available for implementing the proposed system. Furthermore the chosen platforms technical capabilities are highlighted. As a reference point let it be defined that a dynamic RFID reader which is capable of easy software manipulation and deployment of features that goes beyond the standard EPC Gen2 reader, is the initial aim of the implementation.

From the preliminary description of the systems required capabilities a SDR-based RFID reader presents an ideal platform concept, when the need to handle low level communication parameters is essential. The Universal Software Radio Peripheral (USRP) presents such a platform, where software defined RFID development may be possible.

Several USRP devices are developed by ETTUS Research, however the USRP1 and USRP2 is available hardware to conduct this work. The main features of the two platforms are highlighted, from what an evaluation is done, with the proposed RFID reader features in mind. Especially the apparent I /O features are addressed in the evaluation.

Firstly all USRP operates with external front-ends, denoted as Daughterboards. These boards handle the up and down conversion, and is compatible with all USRP versions. Some Daughterboards are full Rx/Tx capable, where as others are only Rx or Tx capable.

6.1 USRP1

The USRP, being the first SDR developed by Ettus, communicates with the host pc via a half duplex USB interface, capable of transfer speeds of up to 32 MB/s. Four 12 bits ADC's with a 64 MS/s provides two complex receiver chains, and four 14 bits 128 MS/s DAC's combines up to two complex transmission chains. The heart of the radio consists of an Altera Cyclone EP1C12Q240C8 FPGA. The motherboard holds four extension sockets (2 TX, 2 RX) in order to connect 2–4 RF front-ends. The maximum effective total bandwidth by complex processing is limited to 8 MHz (16 bit, 4 bytes/sample), due to the 32 MB/s data rate of the USB 2.0 interface.

When dual Rx and Tx is utilized 95 % of the logic elements are consumed of the FPGA resources. This may cause a problem when the implementation takes form, as it is unknown

if any part needs to be implemented directly in the FPGA.

A complete architecture of the USRP1 is illustrated by figure 6.1

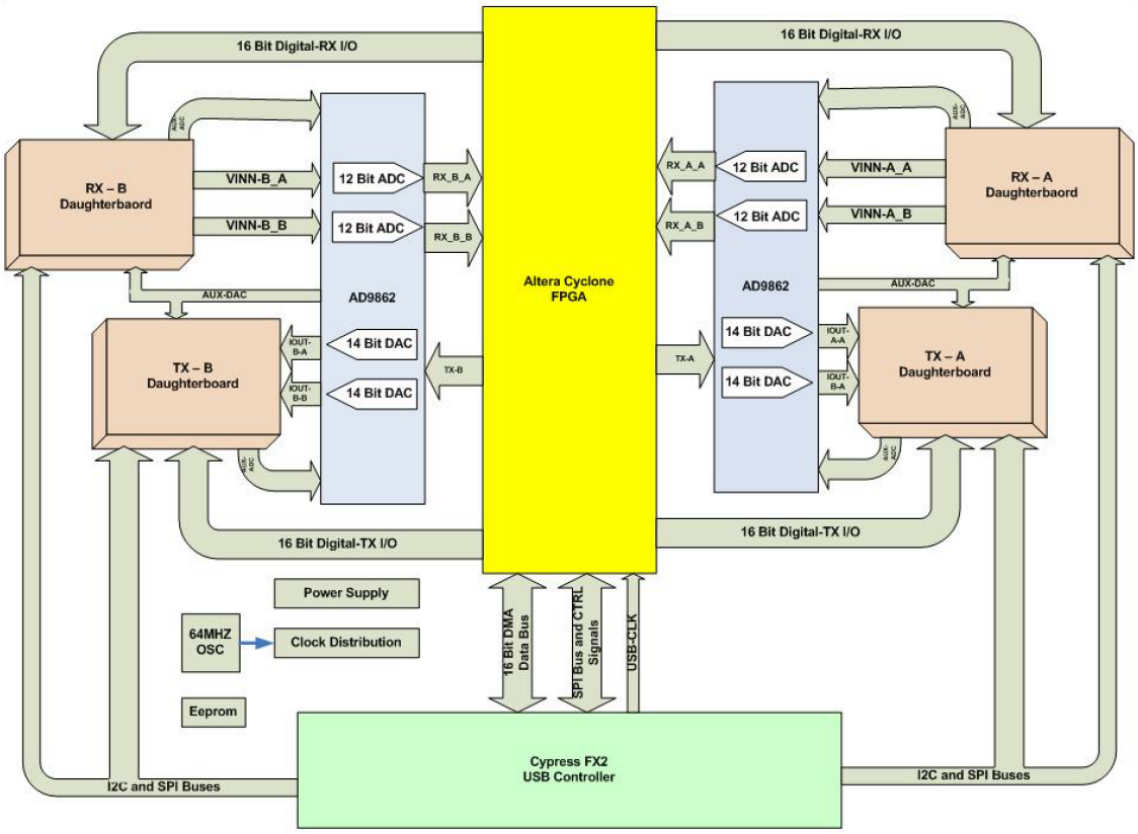

Figure 6.1: The complete USRP1 hardware architecture [3]

6.2 USRP2

The USRP2 is the second generation SDR from Ettus, however does not act to replace the USRP, as the platform presents both proes and cones, when considered against the USRP1. The host interface is Gigabit Ethernet, two 14-bit ADC's with a samplerate of 100 MS/s and two 16-bit DAC's at 160 MS/s. The effective complex bandwidth is 25 MHz, 16 bit. Daughterboard capacity 1 Rx and 1 Tx. The motherboard holds a Xilinx Spartan 3-2000 FPGA, with resources listed in table 6.1. The resources are not directly comparable as the USRP2 only handles single Rx and Tx chain.

Logic	Consumed
Slice Flip-Flops	45 %
4-input Look-Up-Tables	64 %
Occupied Slices	86 %
RAM Blocks	15 available
Multipliers	13 available

Table 6.1: Table of consumed resources of the USRP2 FPGA code

Illustrating the key features head to head, in table 6.2.

	USRP1	USRP2
Interface	USB 2.0	Gigabit Ethernet
FPGA	Altera EP1C12	Xilinx Spartan 3 2000
Bandwidth	8 MHz @ 16 bit	25 MHz @ 16 bit
ADC	12 bit, 64 MS/s	14 bit, 100 MS/s
DAC	14 bit, 128 MS/s	16 bit, 160 MS/s
Daughterboards	2 TX and 2 RX	1 TX and 1 RX

Table 6.2: Table of the key performance and I/O features of the two platforms

The USRP2 capabilities when it comes to a high speed gigabit interface enabling a full 25 MHz sampled spectrum, is desirable. However it lacks the possibility of directly developing a MIMO setup, as it only supports 1 Tx and 1 Rx or 1 transceiver daugterboard extension. The RFID spectrum in Europe only covers 2 MHz (866-868 MHz), therefor the entire spectrum can be sampled with the USRP. Although a multi-carrier RFID reader may extend the frequency spacing to exceed the European RFID spectrum. Recall that the RFID spectrum used in different regions of the world spans 100 MHz. Due to lack of multiple Rx/Tx chains on the USRP2, the USRP1 is chosen as the proceeding platform. The limited FPGA resources may present a future problem, however the USRP2 is not capable of running the required number of channels.

7 USRP and GNU Radio

This chapter serves to introduce the USRP platform and GNU Radio software, as in how it joins to be a versatile SDR. By using FPGA technology the platform succeeds in getting software as close to the Digital/Analog Converters as possible, making it suitable for research implementations. The system is described in details where it is see relevant to the implementation at this stage. The development structure in host computing software as well as FPGA Hardware descriptive language (HDL) is highlighted, in the end of this chapter.

This documentation focuses only on the USRP1, as it is chosen as the platform. The USRP1 is developed as an open specification project to initially support the GNU Radio software toolkit. This enables a complete open source SDR development environment. GNU Radio is released under the GPL version 3 license. Hence everything in both hardware and software, is permitted to be altered in any way developers see fit. In figure 7.1 an overall diagram of the SDR system is illustrated, where each part (USRP, Daughterboard and GNU Radio) is described in the following sections. It is noted that the illustration is simplified as each daughterboard has a Rx and Tx chain, summing to the two Tx and two Rx complex chains.

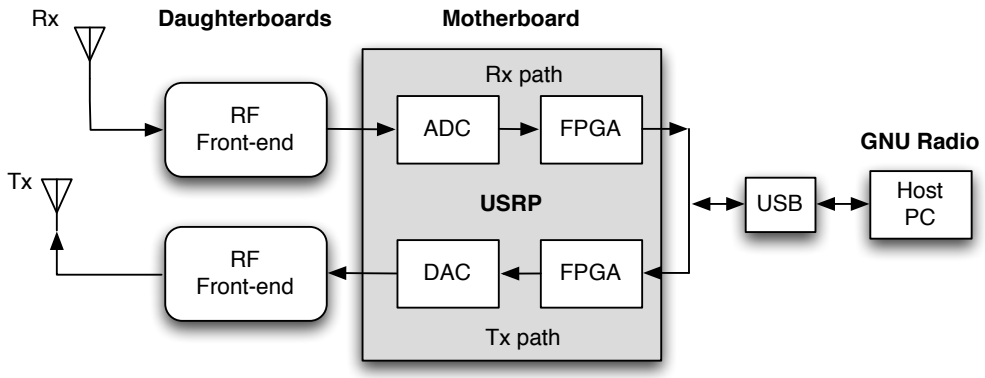

Figure 7.1: USRP high level blockdiagram, showing the main components if the USRP1 system

7.1 The USRP motherboard

The core of the USRP motherboard is an Altera Cyclone EP1C12Q240C8 FPGA, that mainly covers the heavy processing of transmit/receive data and block linking. Hence Rx data is processed by four high-speed ADC's, each capable of 64 MS/s at a resolution of 12-bit. Tx data is processed by four high-speed DAC's, each capable of 128 MS/s at a resolution of 14-bit. Two ADCs and two DACs constitutes a Rx/Tx side. The board is divided into an A side and a B side, that further more is divided into Rx_A and Tx_A. Figure 7.2 illustrates how the resources are distributed for the processes in the FPGA and the DAC/ADC processing chip (AD9862), for both the Rx and Tx chains in side A and B.

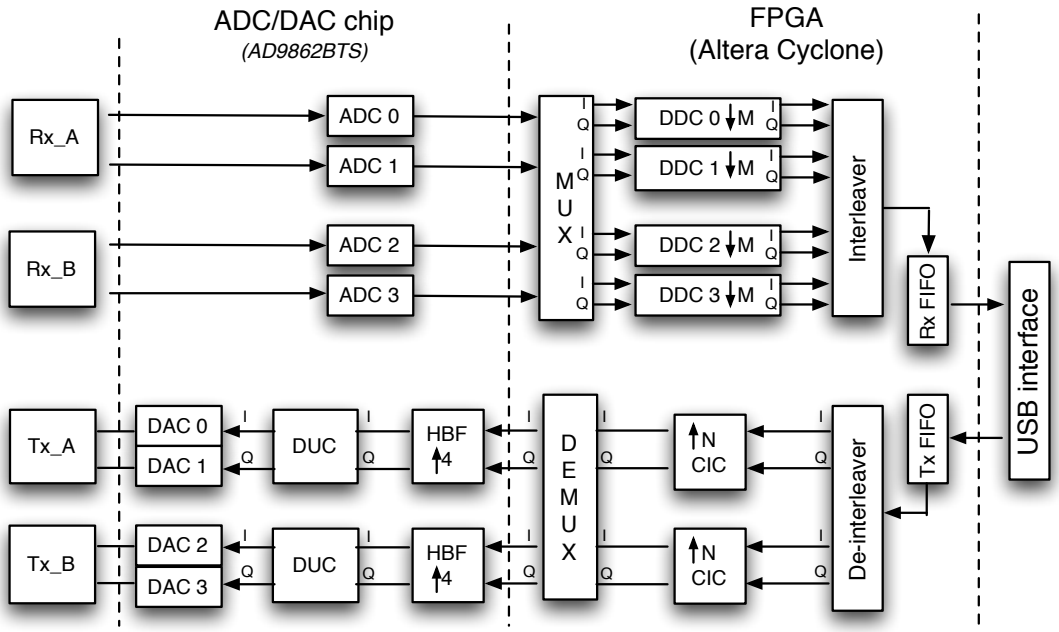

Figure 7.2: Illustration of the USRP1 subsystems from USB host controller, to the Rx/Tx IO extension ports for daughterboards

In the Rx chain the received signal is sampled by 64 MS/s ADCs, hence the Nyqist rate is 32 MHz. However the USB 2.0 interface is only capable of processing 32 MB/s, and as both I and Q samples are 16 bit (4 bits zeroed), they consume 4 bytes. This reduces the bandwidth to 8 MHz due to the USB interface. Hence as shown in figure 7.2 a decimation by a factor M, is introduced by a Direct Down Converter (DDC). The multiplexer allows for custom routing of each ADC. The interleaver serializes the data to a FIFO buffer in the form

$$\{I_n^0, Q_n^0, I_n^1, Q_n^1, I_{n+1}^0, Q_{n+1}^0 ...\}$$

where I_n^X and Q_n^X represents the n'th IQ samples from the X'th DDC.

In a similar but reversed manner in the Tx signal path, the data from the host is processed by the USB interface into the Tx FIFO buffer. The data is deinterleaved, to reach a Cascaded integrator-comb (CIC) filter, that handles $N/4$ of the targeted interpolation sum. The de-multiplexer maps the data stream to each Half-band filters inside the DAC, that further interpolates by a factor of 4, obtaining the full N interpolation factor. The interpolation rate can be set from 16 to 512. Hence N = 16 with a bandwidth of 8 MHz, interpolates to the 128 MS/s range of the DAC. The Digital Up Converters (DUC) can further up convert, however normally not used to modulate to CF.

7.2 Daughterboard

As it is pointed out in the previous section, the USRP motherboard consists of side A and a side B. Each side can be equipped with a RF front-end, to suit application needs. In this case the RFX900 750-1050 MHz transceiver daughterboard is utilized on both side A and B. From the schematic [19], it is evident that the board is implemented with a AD834(7/9) quadrature mod- and demodulator, capable of direct conversion from baseband to CF. A Voltage Controlled Oscillator is used to drive a phase-locked loop (ADF4360) as the local oscillator. From software the daughterboard CF is set, and the DUC/DDC on the motherboard is used to fine tune the CF. The maximum transmit power is 23 dBm, when the ISM band filter is enabled. Futhermore the Tx/Rx port isolation is denoted to be 22 dB at 900 MHz, with a noise figure of 8 dB.

7.3 GNU Radio

The GNU Radio toolkit provides the software core of any development done with the USRP. As a easy step into the SDR processes, it provides a drag-drop-connect Simulink like environment, in terms of the GNU Radio Companion (GRC). Here the USRP can act as sink and/or source. The design principle is flowgraphs, constructed by blocks, designed to perform the signal processing aspect. GNU Radio provides an extensive utility/block library, that covers most application.

When more advance customization is required, the underlying processes of GNU Radio can be changed or new functions can be implemented. Thus custom applications can be executed as a standalone application, rather than being constructed in GRC. Resource

demanding blocks, that need to process data fast, are implemented in C++. However the C++ methods and its input arguments are called from at a higher abstraction level in Python. Python is used to setup all input arguments and variables, connect the flowgraph blocks, as well as setting up USRP settings like the interpolation, decimation rate, daughterboard CF etc. The software structure is as illustrated in figure 7.3, where the Simplified Wrapper and Interface Generator (SWIG) block is connecting Python with C++.

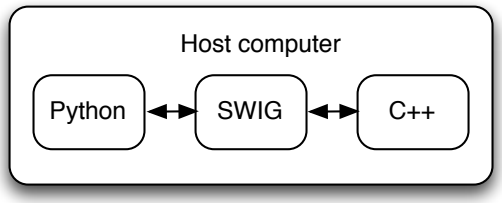

Figure 7.3

SWIG act as 'Glue code', enabling the function blocks implemented in C++, to be interfaced with a main Python program.

GNU radio operates natively under Linux distributions but can run under Mac OSX with limited performance. Current GNU Radio versions requires Universal Hardware Driver (UHD), making it more platform versatile, with support of interface applications like Simulink and Matlab.

7.4 FPGA

As earlier noted the FPGA in the USRP1 is an Altera Cyclone EP1C12Q240C8, that due to the open licensed development codec is fully customizable. The FPGA, due to its manufacture being Altera, is handled by Verilog HDL. The relevant aspects towards the application developed in this project, is that the complete top-layer and bulk source code is available for modification. This is all done by the Altera Quartus II development tool. As the source code consumes nearly all resources in the FPGA, only a limit amount of new functions is possible to implement. However changes made in the FPGA source code to alter the functionality of already existing blocks should be possible.

Part II

System design

8 USRP RFID package

The USRP and GNU Radio in general is supported to a large extend by the developers behind Ettus Research, in conjunction with a continually growing number of developers and researchers that utilizes the USRP platform to conduct SDR implementations. This leads to an extensive amount of applications developed and shared within the GNU Radio community. As this project focuses on implementing extended features to a EPC Gen2 RFID system, it is not within the time frame nor is it the aim, to implement a full RFID tag reader on the USRP platform. Therefore an already developed RFID EPC Gen2 reader is adopted and utilized as basis for the further work, towards gaining the desired functionality. This chapter serves to introduce the aspects of a USRP1 RFID reader package implemented by PhD student Michael Buettner from the University of Washington, USA.

The overall structure and relevant functionality of the RFID reader is presented in the following. Information gained by consulting article [7], published by Mr. Buettner in relation to his work. Further more the experience derived from the authors work with the RFID package will also take part in this chapter, as it presents a considerable effort, to obtain a working system.

USRP RFID reader structure

The overall software structure is constructed as illustrated by diagram 8.1. The interesting block here is the Decoder/Transmitter block. Here the tag response is decoded and the readers MAC and physical layer behavior is implemented in C++. Hence all reader commands like Query, Query Repeat, ACK and NAK is generated by function calls from this block. The interrogation session preamble described in Chapter 3 is also constructed here, taking part in every Query round. This block is the main point of interest, as all reader parameters are set here. To simplify the reference to the developed and used software, this block is now referred to as the Reader_Command_Gate. By consulting the RFID reader package source code the need for this reference change should be clear, however to follow the notation in [7] the block is introduced as Decoder/transmitter.

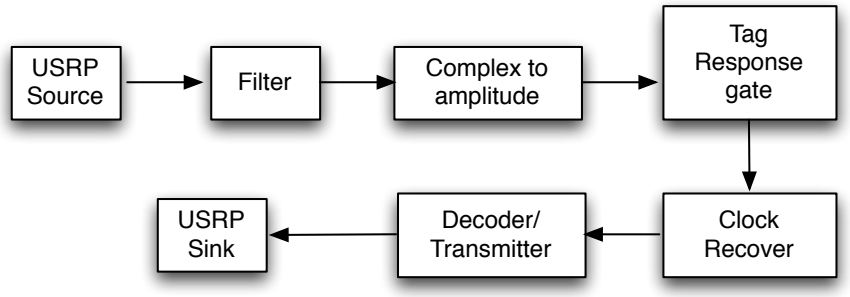

Figure 8.1: Software structure block diagram for the RFID reader developed by Michael Buettner

Also the Tag Response Gate presents a functionality that is relevant to highlight, as it is implemented to gain a block that governs when the received data stream is latched to the later blocks. This is to limit the processing power requirements, as the Clock Recovery and Decoder/Transmitter block, then only operates when Tag/Reader commands are to be decoded or transmitted.

The software is noted to be developed under the previously used GNU Radio USRP drivers, and does not support the UHD, that is used in newer versions of GNU Radio. It is therefor crucial that the installed GNU Radio version is 3.3.0/3.4.0. This is noted to be a general problem with the GNU Radio/USRP development reuse, as meany blocks are developed for certain versions of GNU Radio. This also presents a challenge when the development scene is consulted for support, as it is always assumed that users are running the latest version of GNU Radio.

The RFID reader package proved to be a rather comprehensive system to obtain a successfull EPC response decoding. The package has been under running development, with a public subversion repository, that proved very help full, as the source code then could be followed in its progress. A key tool to give a quick overview of the source code was used on terms of Flow Crystal C++. It's a code management tool that provides a object data flow graph of the instantiated objects and the connections between them. This together with the repository history gave way for better understanding the individual behavior of the reader objects.

Firstly all .cc files constituting the reader, was defined with an improper header in terms of C's standard IO with "#include <stdio.h>", hence is changed to the C++ std IO, "#include <cstdio>". This should however not cause any difference, to the functionality of the software, however is seen as being the proper std IO to use for C++ applications. This also enables the use of C++ standard blocks like min and max, as they do not exist directly in C

language. The C std macro uses data type transition in its functions, hence the operations are slower. It is noted that these changes, renders the application useless if complied with for instance Visual C++, as functions like min/max are defined differently. This should optimize the performance by changes made, like illustrated in the following listing.

```
1 #Line 625
2     int mm = std::min((tx_msg->length() - d_msg_count) / sizeof(gr_complex), (long unsigned ↩
          int) noutput_items - nout);
3
4 ###replaced by
5
6     int mm = min((tx_msg->length() - d_msg_count) / sizeof(gr_complex), (long unsigned int) ↩
          noutput_items - nout);
```

In rfid_gen2_reader.cc, it was evident that the return variable was mismatched for the main program. The return variable needs to address the SWIG input parameter, to latch the correct information to the main python program. The following code was added

```
1 # Line 42
2 {
3 return v > 0 ? 1. : (v < 0 ? -1. : 0);
4 }
```

Further the decoding functionality is identified in the code as using a correlation function. A bit is determined by correlating the received signal with a data-0. If the correlation is above 0.5, the bit is estimated to be a data-0. However the correlation factor for determining if the received signal is a data-0 or data-1, is set to 0.8, not 0.5. There may be a reason unknown to the author for this setting, however it is interpreted as an error, and is set to 0.5.

The RFID package needs to be included in the GNU Radio compilation files by

```
1
2 src/misc_files/grc_gr_gen2_rfid.m4 -> gnuradio/config
3 src/gr-gen2-rfid -> Gnuradio/
4 src/misc_files/usrp_source_base.cc -> gr-usrp/src/
5 src/misc_files/fusb_linux.cc -> usrp/host/lib/legacy/
6
7 include grc_gr_gen2_rfid.m4 -> gnuradio/config/Makefile.am
8 include GRC_GR_GEN2_RFID -> gnuradio/configure.ac
```

It is noted in [7] that a custom FPGA binary is used by the RFID package. This is however found not to be the case, resulting in a need for outcommenting the custom binary pointer

in the python source code.

```
#fpga = "usrp_rfid.rbf"
```

[7] indicates that the customized binary, served to reduce system latency by moving the CW from the host computer, to a function handled directly by the FPGA. As the bandwidth of the system is 8 MHz half duplex, Rx and Tx shares these resources. However when the FPGA handles the CW transmission, the Tx bandwidth requirement is minimized to only be used when reader commands are processed. This reduces the system latency as the USB controller process less data. By arguments unknown this functionality was removed in current revisions as it operates with the standard usrp_std.v provided by Ettus. The author invokes this concept with an extended functionality.

In the initial custom FPGA binary Verilog implementation a CW transmitter implemented in the FPGA, transmitted the CW with maximum power. Here an alternative implementation with the possibility of controlling the CW amplitude from python, is implemented. This feature assist in the case of a multi-carrier reader, to enable independent control without using external attenuation devices. Hence the following changes/additions to the FPGA binary is made.

From the RFID package earlier repository the CW functionality is identified as the following listing from tx.buffer.v

```
else if(tx_empty)
    begin
       case(phase)
         4'd0 : tx_i_0 <= tx_amp;
         4'd1 : tx_q_0 <= 16'd0;
         4'd2 : tx_i_1 <= tx_amp;
         4'd3 : tx_q_1 <= 16'd0;
       endcase // case(phase)
       phase <= phase + 4'd1;
end
```

From this it is clear that if the Tx buffer is empty, the used case function is initiated, inducing a variable tx_amp directly into the Tx buffer for transmission. This is then cycled through, until Tx buffer receives actual data. The extended version here is then to make the variable "tx_amp", a register that is set at application runtime. As the proposed multi-carrier system operates with dual Tx, two variables are created to control them independently. usrp_std.v is therefor altered by firstly initializing wires for input_reg

```
#Line 121
wire [15:0] input_regA;
wire [15:0] input_regB;
```

and further linking input_reg with registers FR_USER_"1/2" accessible via pointers directly specified in the python source code.

```
#Line 136
setting_reg #(`FR_USER_1)
setting_reg #(`FR_USER_2)
```

The I/O definition for tx_buffer is expanded to latch new variables "txA_amp" and "txB_amp, taking input_reg_"A/B" as arguments.

```
tx_buffer tx_buffer( ....., .txA_amp(input_regA), .txB_amp(input_regB);
```

Furthermore tx_buffer.v source code, is adapted to handle the input from usrp_std.v with first defining the input wire

```
input wire [15:0] txA_amp
input wire [15:0] txB_amp
```

and then using the already made function case(phase) by buettner to induce the variable as shown earlier, but with the new variables

```
else if(tx_empty)
    begin
       case(phase)
         4'd0 : tx_i_0 <= txA_amp;
         4'd1 : tx_q_0 <= 16'd0;
         4'd2 : tx_i_1 <= txB_amp;
         4'd3 : tx_q_1 <= 16'd0;
       endcase // case(phase)
       phase <= phase + 4'd1;
end
```

The variables can now be defined directly in python source code via

```
tx._write_fpga_reg(usrp.FR_USER_1, int(txA_amp))
tx._write_fpga_reg(usrp.FR_USER_2, int(txB_amp))
```

Finally the RFID package source code is altered, in terms of silencing the code that process the CW when reader commands are not transmitted. This is done by out-commenting the following lines in rfid_gen2_reader.cc. This is derived by comparing new and old revisions of the package.

```
1  if(FIND_ALL_TAGS){
2        if(NUM_TAGS - STATE.num_tags_found == 0){
3     printf("Found all tags!: %d\n", STATE.round);
4     STATE.round = num_rounds;  //We win. No more rounds
5        }
6      }
7
8      STATE.round++;
9
10 #    int min_cw = 2000; #Continous Wave samples = 2000 (an estimate)
11 #    int num_pkts = ((min_cw / d_us_per_xmit) / 128);
12 #
13 #    for(int i = 0; i < num_pkts; i++){
14 #      gr_message_sptr cw_msg = gr_make_message(0,
15 #                      sizeof(gr_complex),
16 #                      0,
17 #                      (128) * sizeof(gr_complex));
18 #      memcpy(cw_msg->msg(), cw_buffer, 128 * sizeof(gr_complex));
19 #      out_q->insert_tail(cw_msg);
20 #    }
```

Another important parameter for the USRP RFID reader to function properly is to utilize a host computer that provides extensive calculating power. This is seen by the test conducted in appendix B.1, where an outline of the obtained results is presented by table 8.1. Here it can be seen that 4 CPU cores are more or less required to obtain satisfying results. The table shows successful EPC decodings, out of 1000 cycles.

PC3			
# Core	2	3	4
1.8 GHz	0	398	935
2.4 GHz	0	816	933
3.3 GHz	0	929	983
4 GHz	x	x	953

Table 8.1: PC3 test with number of successful decoding out of 1000 Query's at 50 cm, 866.5 MHz and Miller-2

Also the bandwidth of the system is tested in appendix B.1, where tags are trailed for successful readings over a bandwidth of 300 MHz. The test results with no channel con-

trol/shield cabin proved the system to be very susceptible to external noise. However is expected as a 300 MHz span includes occupying restricted frequencies.

A USRP1 with an adopted RFID reader package is utilized and tested with successful results. This creates the basis for the ongoing research and enables the work to progress towards implementing the two proposed methods on top of a fully customisable software defined RFID reader.

9 Multi-carrier reader

This chapter contains the steps taken towards implementing the mutli-carrier reader system. As should be clear from the previous chapters, the implementation is realized by the means of the Ettus USRP1 hardware platform, and will act in extension to the RFID reader package developed by Michael Buettner.

Normally the RFID reader package operates on a single Tx complex chain, by the means of Tx_A in this case. The aim of this implementation is to output the same reader message baseband signal, on both Tx_A and Tx_B, although tuned to different CF. Δf being larger then the channel coherence bandwidth, estimated in chapter 4 as being 10 MHz.

9.1 Multiple command gates

The initial block setup and resulting transmitter structure is depicted in 9.1. When the USRP operates as a dual sink system, the data being processed in the host computer, is interleaved to the USRP and multiplexed out to each channel. To feed the USB host controller with the required data for both channels, the Tx reader_command_gate is duplicated, where both are linked to an interleaver.

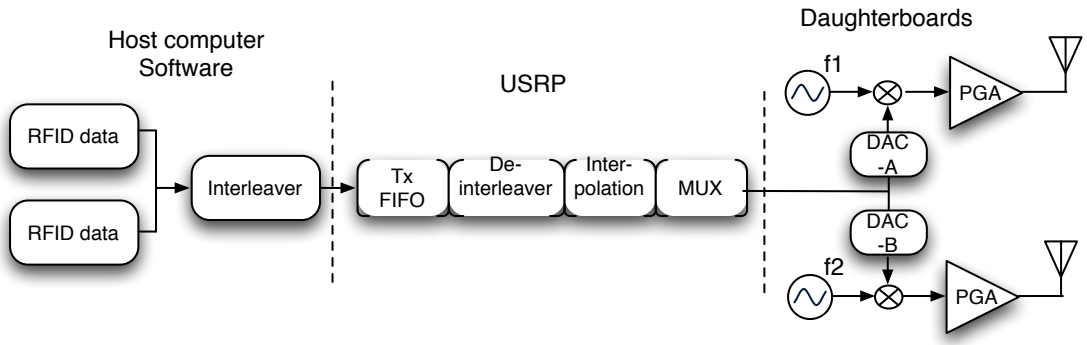

Figure 9.1: Mutlicarrier reader, done with a double Tx reader RFID block and an interleaver

The data is rendered from the same tag response commands, hence the reader_command_gate latches identical data to each channel. This is done, to prevent that each channel gets only

half the number of samples each, due to the interleaver serializing the samples. However this setup may suffer from a slow USB connection, as the data rate is doubled.

Part of the initialization code for instantiating the dual sink USRP in python, is illustrated by the following listing.

```
#HARDWARE SUB-SYSTEM for TX SIDE
    tx = usrp.sink_c(which_usrp, nchan=2, fusb_block_size = 1024, fusb_nblocks=4, ↩
        fpga_filename=fpga) # nchan=2 to initialize dual channel Tx
    tx.set_interp_rate(512) #Interpolation rate = 512
    tx_subdev_A = (0,0) # TX/RX port of RFX900 daugtherboard on side A
      tx_subdeb_B = (1,0) # TX/RX port of RFX900 daughterboard on side B


    t = tx.tune(subdev.which(), subdev_A, freq_A) # Tuning TX_A Daughterboard @ Center ↩
        Frequency

    t = tx.tune(subdev.which(), subdev_B, freq_B) # Tuning TX_B Daughterboard @ Center ↩
        Frequency

    rx = usrp.source_c(which_usrp, dec_rate, nchan = 1, fusb_block_size = 512, fusb_nblocks ↩
        = 16, fpga_filename=fpga)
    rx_reader_subdev_spec = (0,0) # Reader RFX900 daugtherboard on side A
    rx_reader_subdev = rx.selected_subdev(rx_reader_subdev_spec)
    rx_reader_subdev.set_gain(rx_gain)
    rx_reader_subdev.set_auto_tr(False)
    rx_reader_subdev.set_enable(True)
    rx_reader_subdev.select_rx_antenna('RX2')

    r = usrp.tune(rx, 0, rx_reader_subdev, freq) # Tuning READER RX Daughterboard @ Center ↩
        Frequency
```

It is noted how each daughterboard is set to freq_A and freq_B, for different CF.

The system is tested in appendix C.1, with unsuccessful results. The data is verified to be modulated on both Tx_A and Tx_B CF, however no tag responds is evident.

The RFID message signals datarate at miller = 4 is typically of 80 kb/sec. The increased data rate from the two command gates indicates to fail the maximum reader message response time of 500 μs

Furthermore it is noted, that with the current receiver structure the Rx daughterboard is only tuneable to either freq_A or freq_B at a time. Resulting in a limited system, as tag responses on both carriers can not be monitored simultaneously. The maximum decimation rate allows for sampling 2 MHz bandwidth, causing a single Rx channel not to suffice. Finally the system is operating on two independent antenna elements, introducing a channel difference (space diversity), witch is not desired as the main aspect is to cover frequency diversity gain.

The conclusion from this initial implementation is negative, with the system behavior noted for further development.

9.2 FPGA edition

In the implementation procedure conducted in 9.1, timing lead to poor performance of the reader. As the data is being multiplexed trough the FPGA, onto the respective ADC's in the FPGA, another approach is taken in terms of altering the multiplexer behavior directly in the FPGA source code. Altering the path in the FPGA multiplexer makes the RFID package totally unchanged, hence no data structure or format is changed. This creates a more transparent solution as the FPGA handles the information by hard wired circuitry and logic gates, no additional ALU processing is requires from the host, nor the USB host and slave controllers. This is expected to produce the desired output, while still getting successful tag responses.

When the Tx USRP structure is initialized by the command:

```
1  tx = usrp.sink_c(which_usrp, nchan=2, fusb_block_size = 1024, fusb_nblocks=4) # nchan=2 to ↩
       initialize dual channel Tx
```

, a FPGA binary is latched directly from the software code, when it is executed.

However as noted earlier, the initialization of the tx sink enables for a custom FPGA binary to be defined.

The FPGA source code is being expanded by an alternative multiplexer, to force data that is being feed to Tx_A, to also enter Tx_B.

Essentially changing the pointer registers that are processed by the existing MUX controller, to hard wire Tx_A and Tx_B DAC inputs. This is done by the Verilog code illustrated by the following listing. The changes are made in usrp_std.v.

```
1    setting_reg #(`FR_TX_MUX)
2      sr_txmux(.clock(clk64),.reset(tx_dsp_reset),.strobe(serial_strobe),.addr(serial_addr),.↩
           in(serial_data),
3          .out({dac3mux,dac2mux,dac1mux,dac0mux,tx_realsignals,tx_numchan}));
4
5    wire [15:0] tx_a_a = dac0mux[3] ? (dac0mux[1] ? (dac0mux[0] ? q_out_1 : i_out_1) : (↩
         dac0mux[0] ? q_out_0 : i_out_0)) : 16'b0;
6    wire [15:0] tx_b_a = dac1mux[3] ? (dac1mux[1] ? (dac1mux[0] ? q_out_1 : i_out_1) : (↩
         dac1mux[0] ? q_out_0 : i_out_0)) : 16'b0;
```

```
7    wire [15:0] tx_a_b = dac0mux[3] ? (dac0mux[1] ? (dac0mux[0] ? q_out_1 : i_out_1) : (↩
         dac0mux[0] ? q_out_0 : i_out_0)) : 16'b0;
8    wire [15:0] tx_b_b = dac1mux[3] ? (dac1mux[1] ? (dac1mux[0] ? q_out_1 : i_out_1) : (↩
         dac1mux[0] ? q_out_0 : i_out_0)) : 16'b0;
```

The multi-reader is tested in appendix C and proved to output the baseband signal on both carriers and still successfully decode tag responses, with the changed FPGA structure, when RX_A is tuned to one of the two frequencies. Still the system is not capable of decoding both tag responses simultaneously, and still two Tx elements are used.

9.3 Dual decoding

To extend the reader capabilities to process both tag responses on both frequencies, although Δf is more than 2 MHz, an alternative solution is introduced. The RFID reader processes the tag commands in modules, therefor these modules can be used separately, to process incoming data, without responding. Hence the reader_command_gate is used to decode both tag responses captured by Rx_A and Rx_B, tuned to each carrier center frequency. This renders the system indifferent of the frequency spacing between the two interrogation carriers, thus making the system more versatile. A toplevel figure of the I/O is illustrated by figure 9.2. Both the full reader and the decoder outputs RSSI and the number of successful decodings.

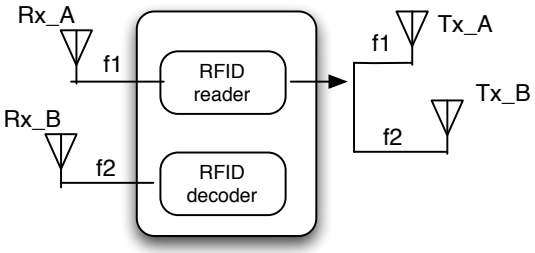

Figure 9.2: Mutli-carrier reader transmitting on Tx_A and Tx_B, and receiving on Rx_A, with a decoder also enabled for Rx_B

The system is tested in appendix C, and proves to run satisfyingly, with the capability of decoding tag responses on both carriers.

Finally the system need to be operating on single antenna elements on both Rx and Tx side, hence a solution needs to be considered and implemented.

Available splitters/combiners, are utilized to join the two Rx ports to one antenna ele-

ments, as well as the two Tx ports to one element. A circulator could be used to reduce the system to a single element, however no such device was available for testing. Hence the final system is noted to be bi-static.

The hole system with splitters/combiners is tested in appendix C, where a short performance illustration is presented by table 9.1 where each Tx chain transmission power is shown,

Chain	level
Tx_A	22.2 dBm
Tx_B	21.1 dBm

Table 9.1: Verification of Tx_A and Tx_B output levels

and further the EPC decoding performance in 9.2.

Reader	Decoder
Freq_A = 865.5 MHz	Freq_B = 876.5 MHz
Out of 1000 cycles	Out of 1000 cycles
949	958
826	608
915	967
901	876
959	911

Table 9.2: Verification of the dual Tx and Rx, on difference frequencies

The USRP outputs both modulated carriers, as was the goal. Furthermore the decoding the the tag responses proved functional, thus the desired functionality of the multi-carrier reader is implemented with success. Although the reader operates as a bi-static system, this is seen as minor detail. The implementation of the deliberate interference reader follows.

10 Deliberate Interference Reader

The Deliberate interference concept is addressed in the following chapter. The steps are documented, and shot notes about the method performance are highlighted. It is noted that the multi-carrier and deliberate interference concepts are implemented separately.

10.1 Baseband noise addition

As an initial test setup to investigate the deliberate interference concept, a commercial reader was tested with an interference signal, in appendix A.3. In the setup, the used interference signal, was a unmodulated pure sinusoid, added to the modulated RFID reader signal, at the same frequency as the carrier. This proved to work as expected, with a reduction in the interrogation zone. However the USRP, using frequency ranged daughterboards, is not equipped with the required number of oscillators to mix the signals at the RFID center frequency. The approach to gain a limited interrogation zone is hence expressed by an interference signal added to the RFID reader message signal, already in digital baseband.

To both specify and verify the output to each antenna element, and how they react in air, the numerical data branches is presented in terms of figure 10.1 and 10.2.

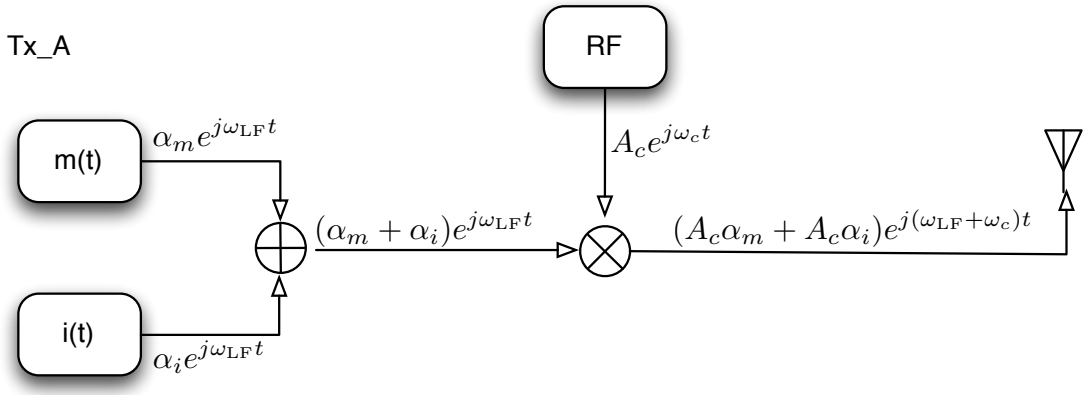

Figure 10.1: The numerical data structure for transmission in branch A

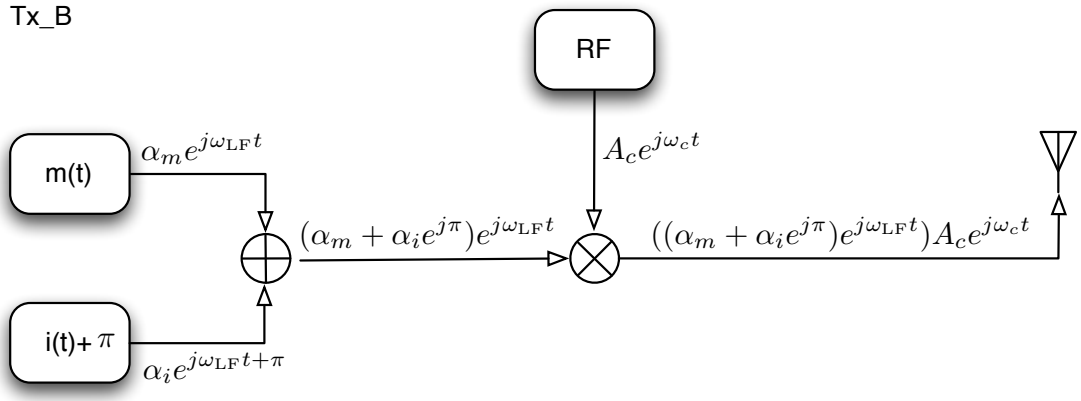

Figure 10.2: The data structure for transmission in branch B, where the interference signal is rotated with π degrees

The output from branch A is given by

$$A_c\alpha_m e^{j(\omega_{\mathrm{LF}}+\omega_c)t} + A_c\alpha_i e^{j(\omega_{\mathrm{LF}}+\omega_c)t}$$

and from B,

$$A_c\alpha_m e^{j(\omega_{\mathrm{LF}}+\omega_c)t} + A_c\alpha_i e^{j(\omega_{\mathrm{LF}}+\omega_c)t+\pi}$$

The interference is factorized in branch B

$$A_c\alpha_m e^{j(\omega_{\mathrm{LF}}+\omega_c)t} + A_c\alpha_i e^{j(\omega_{\mathrm{LF}}+\omega_c)t} e^{j\pi}$$

and the identity $e^{j\pi} = -1$ is used. Thus, derives as

$$A_c\alpha_m e^{j(\omega_{\mathrm{LF}}+\omega_c)t} - A_c\alpha_i e^{j(\omega_{\mathrm{LF}}+\omega_c)t}$$

.

The resulting output addition in air (broadside), when the element spacing is assumed to be $\frac{\lambda}{2}$, creates the expected effect, with a noise cancellation in broadside due to the preprocessing combined with the antenna spacing, as shown by equation (10.1)

$$Tx\_A + Tx\_B = A_c\alpha_m e^{j(\omega_{\mathrm{LF}}+\omega_c)t} + A_c\alpha_i e^{j(\omega_{\mathrm{LF}}+\omega_c)t} +$$
$$A_c\alpha_m e^{j(\omega_{\mathrm{LF}}+\omega_c)t} - A_c\alpha_i e^{j(\omega_{\mathrm{LF}}+\omega_c)t} = 2A_c\alpha_m e^{j(\omega_{\mathrm{LF}}+\omega_c)t} \quad (10.1)$$

Implementation wise the block element structure becomes as shown in figure 10.3, where a pure sinusoid is inserted as the interference source. In digital complex baseband a 180 phase turn is a complex multiplication of $-1 + j0$. As the noise addition is made already in baseband, the system operates with a modulated interference.

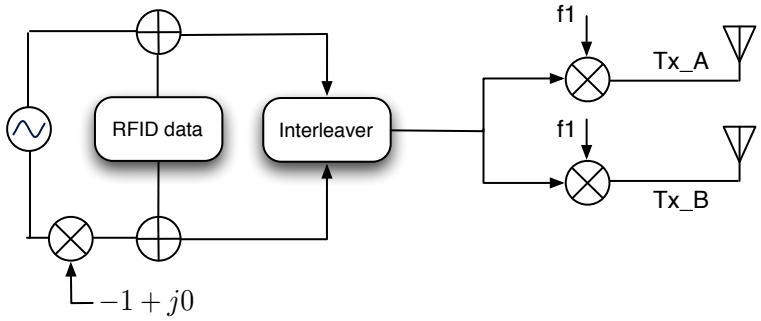

Figure 10.3: Noise addition to create deliberate interference, with a pure sinusoid signal added to the reader message signal

Pseudocode for this implementation is listed in the following:

```
#Instantiate required blocks:

    usrp = usrp.sink_c()

    RFID_reader = rfid.cmd_gate(dec_rate * sw_dec, reader.STATE_PTR)

    interferer = gr.sig_source_c(44000, gr.GR_SIN_WAVE, 100e3, 0.5, 0) #(sample_rate, gr.↩
         GR_SIN_WAVE, Freq, amplitude, offset)

    interleaver = gr.interleave (gr.sizeof_gr_complex)

    sum_A = gr.summation()

    sum_B = gr.summation()

    multiply = gr.multiply_const_cc(complex(1,0))

# Connect them

fg.connect(RFID_Reader, sum_A(0))
fg.conncet(RFID_Reader, sum_B(0))
fg.connect(interferer, sum_A(1), interleaver(0))
fg.connect(interferer, multiply, sum_B(1), interleaver(1))
fg.connect(interleaver, USRP)
```

A key element to this implementation is the verification of actually having the expected phase difference of the interference, gaining a perfect cancellation to limit unwanted com-

ponents in the message signal. Hence before implementing the full system for testing, a partial verification test of phase coherence between the two transmit branches is to be addressed.

Phase offset control

Two system parameters are to be determined, in terms of phase offset repeatabelity and phase stability. In normal operation mode, the daughterboards operate with independent local oscillators, to generate the requested carrier frequency. Phase coherence between Tx_A and Tx_B is therefore not available by default. A hardware modification is therefor necessary. By bypassing the local oscillators in the daugterboards and rerouting the design, a common clock can be provided by the FPGA on the motherboard, to synchronize the carriers. Each daughterboard is therefore hardware modified to disable there local oscillators, and connect them to the FPGA clock.

As the USRP is created under a open source licence, the schematics for every hardware piece designed by Ettus is available to the public [19]. Only board layouts/Gerber files are restricted by Ettus. The Tx daughterboard VCO is illustrated by figure 10.4, where it is evident that R117 populates the clock output. A AD4360-3 upconverter receives this clock and handles the upconvertion to the requested frequency. R117 is removed and R116 is populated, to connect io_tx_0 to AD4360-3, feeding the FPGA clock. Finally to disable the VCO altogether R142 is moved to R153.

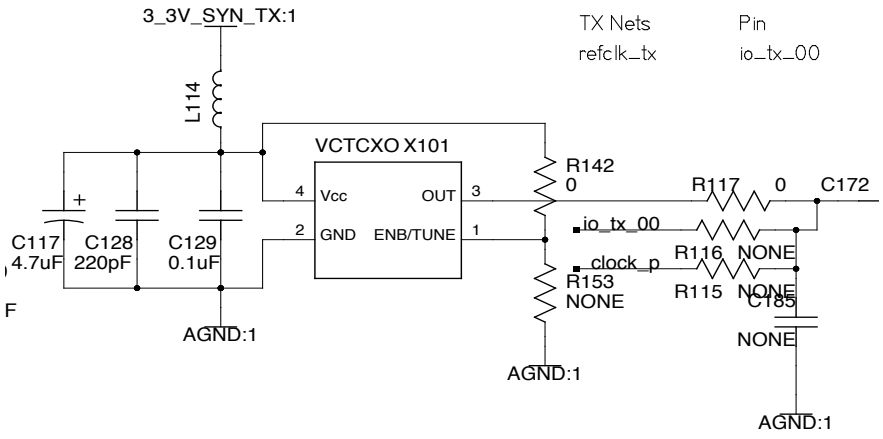

Figure 10.4: RFX900 daughterboard schematic crop out, illustrating the TX local oscillator (VCTCXO) with clock output [19]

In a similar fashion the Rx clock chain is altered by moving R35 to R34, and disable the VCO by moving R64 to R84. It is noted that the hardware modifications done to the Rx chain, is only to obtain a completely coherent Rx and Tx system. Also this is of course performed on both daughterboards.

With this procedure done, it is expected that oscillator coherence leading to phase repeatabelity and stability, is achieved, so the phase of the noise signal is steady and as specified through the application under the hole tag interrogation. A partial system test is conducted with a sinusoid noise signal as the only signal source for the two Tx outputs. The test is documented in appendix D.1, from where it is concluded that the wanted effect of transmit coherence between the two TX daughterboards, is not obtained. The system is able to run without frequency drift, indicating a successful common base clock, however the phase difference of the two outputs change with every runtime. This causes an unpredictable behavior of the system as the constructive and destructive radiation summation then becomes a random process.

Ettus developers are consulted to gain clarification of the system behavior. Response clarified that due to the AD4360-3 upconverters, phase coherence can not be achieved by the means of the executed procedure, although they are fed with a common clock. It is noted by Ettus that as they are classified as Fractional-N frequency synthesizers, they produce a uniformly distributed random phase offset, whenever reset.

It is estimated that the AD4360 synthesizers are initiated by a running variable. Hence the generated random phase offset could be seen as a pseudo random variable. Knowing the variable state at the moment of synthesizing the carrier, may provide a priori knowledge at the application runtime, creating the possibility of taking counter measures in software. Although this could present an apparent solution to this problem, another aspect of the random phase, is the difference in phase offsets induced by using non identical cables. These differences also rise a need for calibration, however are static for every runtime.

With the proposed method of phase cancellation and summation proven to be unsuccessful due to USRP hardware limitations, a solution with phase independency is proposed in the following section.

10.2 Data negation

As a direct phase shift in the baseband is proven to be unusable, another approach is considered. Instead of introducing a noise signal on the message signal, the data signal

itself is being used to alter the modulation index. The reader_command_gate then needs to be modified to output two data signals. The ordinary modulated and encoded data symbol, and the negated encoded symbol, as shown on figure 10.5. It is noted that due to the PIE used in EPC Gen2 protocol, the negation is not a data-0 -> data-1, but reversed amplitude level of the given data symbol outputted by the reader_command_gate. Instead of creating an interrogation zone governed by the SNIR, this creates zones with different modulation index, where only a limited area fulfilles the modulation index requirements of the tag, for it to respond.

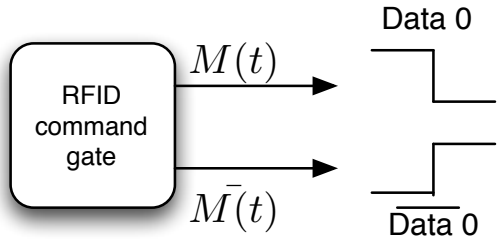

Figure 10.5: RFID command gate with two outputs; Normal and negated data symbol, with Data-0 as an example

The transmit structure will then be as illustrated in figure 10.6

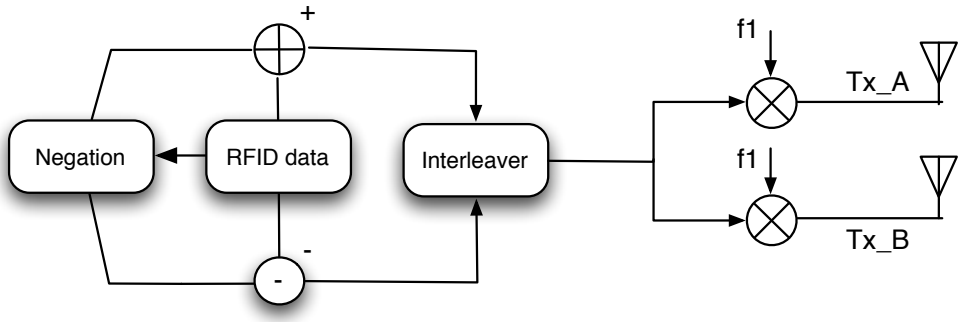

Figure 10.6: RFID command gate with the negation added in Tx_A and subtracted in Tx_B

The proposed method for deliberate interference, firstly by utilising a preset phase offset interference signal and later, a interrogation zone controlled by the modulation index via Data negation, proved to be more comprehensive than the time limit of this project allows. The focus is therefore directed towards the multi-carrier functionality.

Part III

Closing

11 Discussion

With the implementation of a fully operational multi-carrier reader, and partially a reader with an interrogation zone control functionality, the project is rounded of with a discussion. Here reflections on some of the interesting results obtained through the conducted work is noted and also some thoughts about the USRP hardware platform as a tool used for researching into areas like the ones constituting this report. The discussion is divided into three sections, in terms of the Multi-carrier reader, the deliberate interference system and lastly the USRP platform and GNU Radio toolkit.

11.1 Multi-carrier system

When considering the multi-carrier system, one of the interesting aspects to investigate was how the two modulated carriers impact each other and the tag. An initial setup was to interrogate a tag with both carriers active, with one transmitting at a constant level, and the other was varied in power. The expected relation when each receiver chain was monitored would then be as the graph illustrates in 11.1, if no correlation between the carriers is evident.

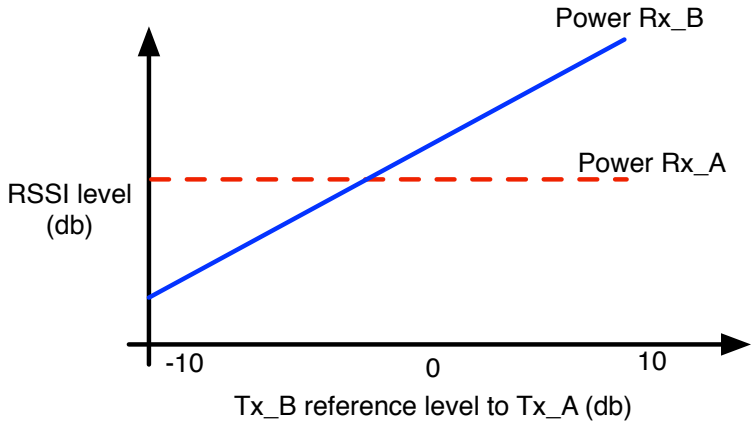

Figure 11.1: Illustration of the expected relations between Rx_A and Rx_B

With the CRC success rate results, nearly the expected tendency rises, although when Tx_B is amplified, the success rate drops at an instant. This could be argued by the

required modulation index relation between the two carriers, highlighted in section 5.2.

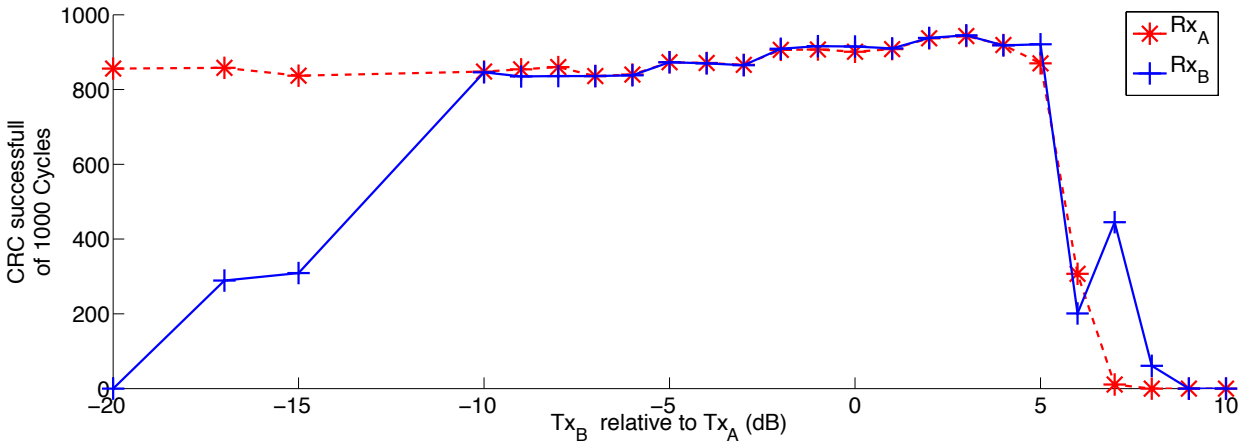

Figure 11.2: Illustrates the successful tag decoding of 1000 reader cycles for both Rx_A and Rx_B, for varying Tx_B transmit power in a anechoic compartment

However when the RSSI levels where monitored, the obtained results showed a high correlation between the two carriers, as seen from figure 11.3.

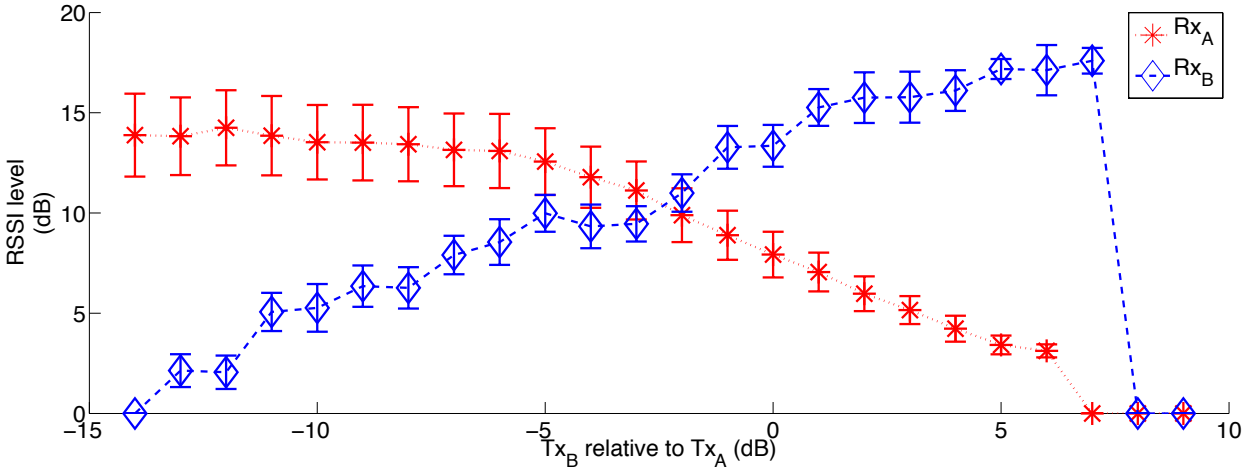

Figure 11.3: Multicarrier interrogation with Tx_B power varied, and RSSI levels on Rx_B and Rx_A, conducted in a anechoic shield device. Tag/reader distance = 55 cm

The results presented by figure 11.3, nearly resembles a selection diversity scheme in the tag, as the one illustrated by figure 11.4

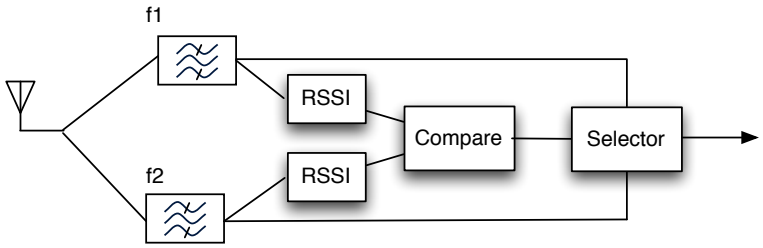

Figure 11.4: RSSI controlled selection diversity

As the tag responds via modulating an antenna reflection coefficient, and does not contain any such device as show in 11.4, the results are unexpected.

Recalled the diversity gain graph from section 5.2, where the distribution compression increases with the diversity order. In the dual carrier reader the order is two, however from the results it is not clear if the tag gains from the second carrier, more than it is evident that the energy from the weakest signal apparently does not get fully reflected by the tag.

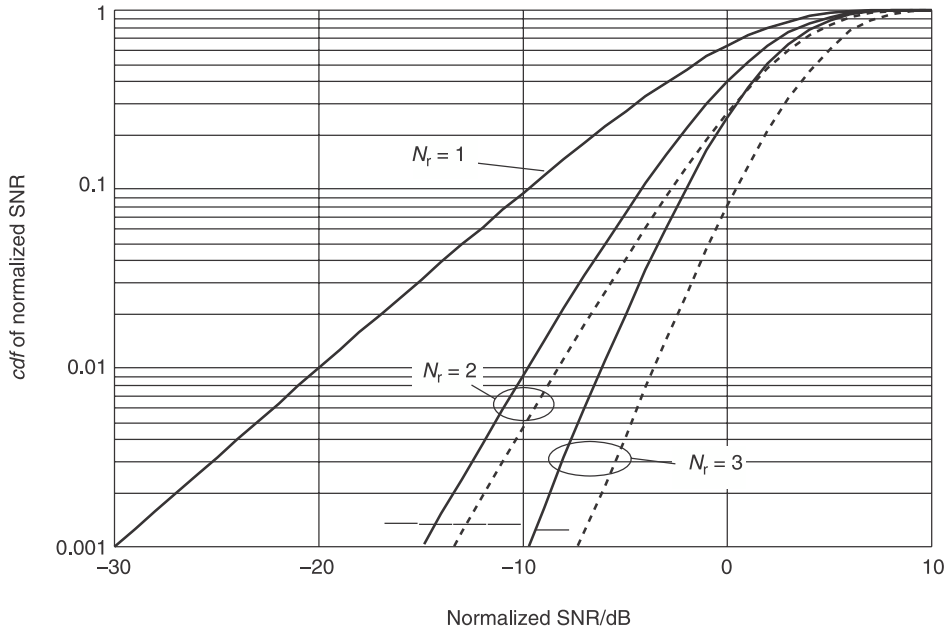

Figure 11.5: Illustration of the cdf of the normalized SNR ratio for selection diversity as the solid lines and MRC as a dashed line [16,p. 255]

In the reader bandwidth investigated in appendix B.2, the results shown in 11.6, illustrates the CRC reader performance of the entire bandwidth, with fairly good results. At 50 cm the entire communication has a success rate of approx. 85 %, hence the SISO does not provide an indication of the MIMO tendencies from 11.3.

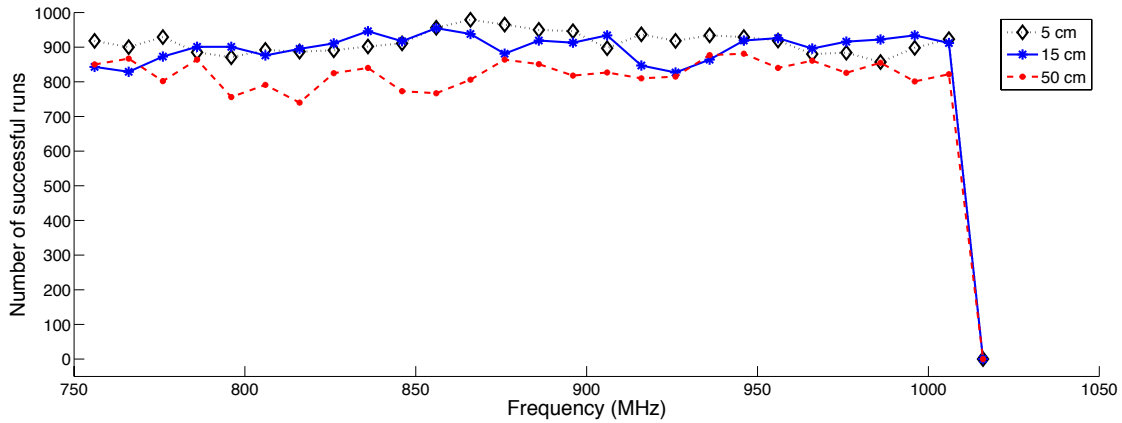

Figure 11.6: Frequency response chart of the system at different spacing from tag to reader Rx/Tx antennas, measured in a RF shielded cabin

When consulting the signal model theory presented in section 5.2, it is evident that it may not be fulfilling, in describing the signal processing inside the tag. No apparent arguments can be given towards explaining the tag response behavior, in terms of expanding the model. However it may indicate that the tag receiver front end consists of more than assumed in the signal model. As tag structural complexity is a field of competition, the actual hardware structure is not accessible.

11.2 Delibrate interference system

The implementation of the deliberate interference concept on the USRP was not completed, as the USRP hardware proved insufficient, regarding a required phase coherence between the two transmitting chains. Therefore little reflections can be made, on behalf of the limited results. The system was tested with the RFX900 front end daughterboards, but could be replaced by LF boards, with a external front end. This would allow for full control of the relevant parts. However as the theme of this project is SDR, this solution is not seen as an option. In the last part of the project period a concept of utilizing the modulation index for limiting the interrogation zone was presented. However this was not implemented. The deliberate interference concept was though successfully implemented as an external device on a commercial RFID reader, hence proven as a working concept.

11.3 USRP Platform

The USRP1 was used as the hardware platform for the implementations made in the project. The USRP as a tool for concept development is very powerful, however has its limits. As many blocks are developed and shared by USRP users, they may be error pron. As an example the saturation level of the USRP was tested by a direct Rx coupling with a signal generator. In a test conducted in appendix C, the dynamic range was evaluated to be 10 dB. This result is highly unlikely, thus is argued to be faulty. Much documentation is provided by the online community supporting GNU Radio and the USRP interface, however the platform is comprehensive with a steep learning curve.

12 Conclusion

The aim of this project, was to implement extended features to a UHF EPC Gen2 reader system in efforts to reach documentation towards new concepts for RFID communication. Two objectives was set; A synchronous multi-carrier reader and a reader with interrogation zone control. These goals where partially reached through utilizing GNU Radio and the USRP hardware platform as well as an adopted RFID reader package, that created the basis for the further development of the proposed features.

A fully functional Multi-carrier reader was obtained, that provided the necessary equipment for researching the field of tag diversity, by exposing a tag to multiple frequencies. The system proved capable of independent decoding of tag responses on separate channels, with a frequency separation of up to 300 MHz. Due to the limited frequency spectrum available, especially in Europe (2 MHz), the tests in this work was conducted with a frequency separation of 10 MHz. The tests proved inconclusive as to whether the tag was able to exploit the information redundancy. From measurements conducted with changing power ratios between Tx_A and Tx_B, it was evident that this ratio was an important factor, as it influences the modulation index at the tag. Also from the results presented in appendix C by figure C.6, an indication of possible reader diversity may act as a challenge for future work, in terms of implementing a suitable diversity gain receiver structure.

The USRP proved to be incapable of handling the necessary preprocessing for a successful deliberate interference implementation, for obtaining the objective of a reader capable of interrogation zone control. However the idea was tested successful on a commercial RFID reader, thus it can be concluded, that the concept has potential of being implemented on a custom build RFID reader.

Bibliography

[1] *EPC Class-1 Generation-2 UHF RFID*. EPCglobal Inc., 2008.

[2] **[Constantine A Balanis]**. *Antenna Theory: Analysis and Design, 3rd Edition*. John Wiley & Sons, 2005.

[3] **[USRP1 block diagram]**. URL `http://wiki.oz9aec.net/images/thumb/1/1a/USRP1_Arch.png/600px-USRP1_Arch.png`.

[4] **[Michael buettner]**. An empirical study of uhf rfid performance. *Mobicom*, 2008.

[5] **[Alien Technology Corporation.]**. Aln-9640 squiggle. Technical report, 2012.

[6] [Daniel M. Dobkin]. *The RF in RFID - Passive UHF RFID in Practice*. Newnes, 1. edition, 2008. ISBN 978-0-7506-8209-1.

[7] **[A Flexible Software Radio Transceiver for UHD RFID Experimenttation]**. Michael buettner and david wetherall. *University of Washington*.

[8] **[Yi-Fan Chen Hsin-chin Liu] and [Young-Ting Chen]**. A frequency diverse gen2 rfid system with isolated continius wave emitters. *Journal of networks*, Vol 2 Nr 05, 2007.

[9] **[Young-Ting Chen & Wen-Shin Tzeng Hsin-Chin Liu]**. A multi-carrier uhf passive rfid system. *IEEE*, 2007.

[10] [Rasmus Melchior Jacobsen] and [Karsten Fyhn Nielsen]. Tag receiver model and collision recovery in rfid networks. Master's thesis, AAU - Wireless Communication, 2010.

[11] **[Rasmus Krigslund]**. Interference helps to equalize the read range and reduce false positives of passive rfid tags. *AAU*, 2012.

[12] **[A. Lazaro]**. Radio link budgets for uhf rfid on multipath environments. *Antennas and Propagation, IEEE Transactions on*, 57, 2009.

[13] **[Harvey Lehpamer]**. *RFID Design Principles*. Artech house, Inc., 2008.

[14] **[Robert J. Mailoux]**. *Phased Array Antenna Handbook - second edition*. Artech House, Incorporated, 2005.

[15] **[Andreas F. Molisch]**. Online appendix - wireless communcations. URL `http://www.wiley.com/legacy/wileychi/molisch/supp/appendices/Chapter_13_Appendix.pdf`.

[16] **[Andreas F. Molisch]**. *Wireless Communcation*. Wiley, 2010.

[17] **[Simon Haykin & Michael More]**. *Communication Systems*. John Wiley & Son Inc, 2005.

[18] **[Fawwaz T. Ulaby Eric Michielssen Umberto Ravaioli]**. *Fundamentals of Applied Electromagnetics*. Number ISBN-10: 0132139316 ISBN-13: 9780132139311. Prentice Hall, 2010.

[19] **[Ettus RFX900 Schematic]**. URL `http://code.ettus.com/redmine/ettus/attachments/download/10/rfx900.pdf`.

Part IV

Appendix

Preliminary method trails A

This appendix serves to document the tests conducted, as a result of the preliminary solution space, and theory deducted in the introduction analysis in chapter 5.2. All preliminary tests are constructed with a commercial RFID reader.

The theory subsections in appendix measurement journals serves to make each appendix independent. They may be skipped if read in extension to the main report.

A.1 Unmodualted Carrier Assistance

Aim

In this measurement a tag is exposed to an additional signal while being interrogated by the commercial reader, to determine if the read range can be improved. Both a modulated and unmodulated secondary carrier is to be tested, thus the documentation is divided in two parts. The unmodulated carrier trail is presented first.

Theory

When the reader is interrogating the tag, two parameters are required to be fulfilled for the tag to respond. The SNR/SNIR and the minimum dBm requirement of the tag, must be sufficient for both powering the tag and enabling the tag to decode the reader to tag commands. A secondary carrier at a adjacent frequency is to be tested, for the investigation of a reading range extension. This second carrier will cause the modulation index to alter, leaving the tag decoding unsuccessful, if an incorrect power ration and frequency spacing is chosen.

Equipment

The equipment used for the unmodulated secondary carrier, is listed in table A.1

Type	equipment	AAU ID number
RFID reader	Impinj Speedway Revolution R420 UHF	-
Signal generator	Rohde Schwarz SMP22 RF	A6-215-F3
Antenna	Three Intermec RFID patch	1415-02
Spectrum analyser	Rohde Schwarz FSL	56915
Tag	Alien Squiggle 9640	-
PC	DELL Optiplex sx260	57347
Software	Multireader 6.6.2	-

Table A.1: Equipment used for measurement

Setup

The physical setup for the measurement is illustrated by figure A.1, where a spectrum analyser is utilised to monitor the correct output from the reader and signal generator.

Figure A.1: The trail setup of the commercial reader, influenced by an interfering signal.

Static parameters of the reader is set as follows:

Parameter	Setting
RFID reader freq.	866.5 MHz
RFID reader Tx power	15 dBm
Q value	0
Reader - Tag distance	1.6 m

Table A.2: Static parameters for the reader

Dynamic parameters will be:

Parameter	Setting
Signal generator Tx power	8 dBm - 15 dBm
Signal generator freq.	800 MHz - 870 MHz

Table A.3: Dynamic parameters for testing increased interrogation range

Procedure

The reader is set to make a continuous reading of a single tag, placed close to the reader. The tag is then moved away from the reader, to determine the readable zone. The signal generator is then enabled, to investigate a possible increase in read range, due to the increase in energy delivered from the second carrier. The reader is held at a fixed center frequency and Tx power, where as the signal generator sweeps in both frequency and power. The spectrum analyser is utilized to verify the transmit power off both reader and signal generator. It is found that a 3 dB difference is evident between the reader and the signal generator, when both set to 15 dBm. This factor is corrected in the presented results. At 15 dBm, the tag is readable at 1.5 m. Hence the tag is placed 1.6 meters from the reader antenna.

Results

The result is represented as a frequency sweep at each power level from 8 dBm to 15 dBm. $\surd$ indicates a tag is being read, at the extended range, $*$ indicates not readable.

Signal gen. Tx Power (dBm)	8	9	10	11	12	13	14	15
Freq sweep 800-870 MHz	*	*	*	*	*	*	*	*

Table A.4: RFID read results on 1.6 m, with unmodulated interference

As it is seen in table A.4, the second unmodulated signal applied, apparently does not assist the tag in getting powered up or else the tag response is disturbed by the second carrier.

If the tag is being moved to 1.5 m, with the assisted signal turned of, the reader continuous to receive the EPC. However when the assisted signal is reapplied, in the same manner as before, the results are as follows:

Signal gen. Tx Power (dBm)	8	9	10	11	12	13	14	15
Freq. Sweep 800-870 MHz	√	√	*	*	*	*	*	*

Table A.5: RFID read results on 1.6 m, with unmodulated interference

This indicates that the second carrier interfere with the reader signal, causing the tag not to be readable.

The next setup is trailed with a second carrier which is now modualted by same reader output.

A.2 Modulated Carrier Assistance

Setup

A setup with the second carrier that is modulated with the same data, as the original signal is tested in the following set up. A simple schematic is shown in figure A.2

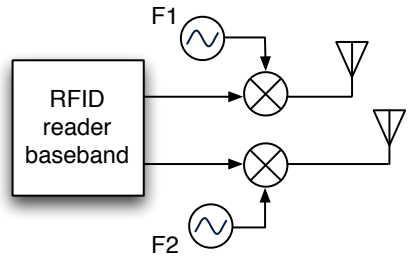

Figure A.2: The double modulated carrier interrogation setup

As the setup is trailed with the commercial reader, the baseband signal is not available for splitting and modulating on each carrier. This leads to an external setup, tasked to detect the envelope of the reader signal, and then ASK modulate it, making it possible to mix it with the second carrier in a signal generator. Such a system is illustrated in figure A.3.

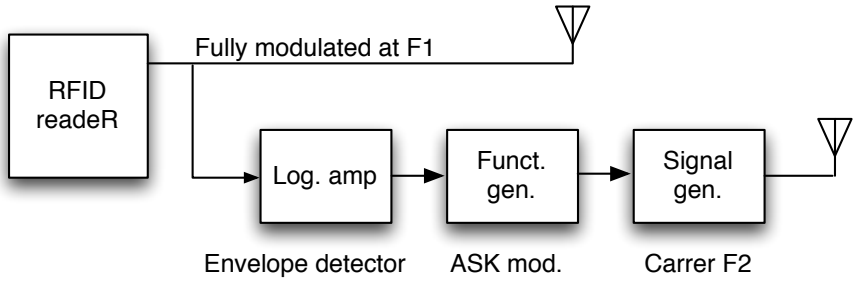

Figure A.3: The lab setup to rebuild the data signal for modulating it on to the second carrier frequency

Additional equipment

For the modulated second carrier additional hardware is used.

Type	equipment	AAU ID number
Amplifier	AAU Log. Amp.	AD8307
Func. gen.	Agilent	33250A

Table A.6: Additional equipment used for measurement

Results

It proved to be an unsuccessfully way of extracting the baseband signal of the commercial reader, for modulating it on a second carrier. The reader utilities PIE encoding, and the function generator used, tend to have a fixed duty cycle for every trigger. Resulting in two non-identical signals being modulated on each carrier, making the setup unusable.

Conclusion

The conducted trails, did not conclude that a second carrier assists the tags reading distance, however the modulated case proved to be unobtainable from the commercial reader. The multi-carrier reader is therefor still targeted for implementation, although the results in this test, may indicate that the system does not work as expected.

A.3 Deliberate Interference concept test

An initial setup is created by the use of a commercial reader.

Aim

The aim for this lab experiment is to verify the theory behind the deliberate interference concept, presented in section 5.1. This is tested by extending a commercial RFID reader with the necessary hardware to gain deliberate interference. The expected outcome is to gain a narrowed interrogation zone, by the use two antenna elements and the concept of signal vector summation.

Theory

The theory behind this concept is described in 5.1, however to make this journal independent a shot summery is presented.

By the means of two antenna elements, a RFID reader and a signal generator, the SIR can be controlled in the radiation field of the two antenna elements. This is done by inputting an interference signal with a carefully set phase offset, to create a narrow null at broadside, that leaves a small area in which the SIR requirements of the tag is fulfilled. The mathematical derivation result from 5.1 is presented by (A.1)

$$\mathrm{SIR}(\phi) = \frac{P_{r-s}(\phi)}{P_{r-i}(\phi)}$$

$$\mathrm{SIR}(\phi) = \frac{\left(\frac{\lambda}{4\pi R}\right)^2 G_{t-s}(\phi) G_r P_t}{\left(\frac{\lambda}{4\pi R}\right)^2 G_{t-i}(\phi) G_r P_t} \tag{A.1}$$

where $P_{r-s}(\phi)$ is the power received from the interrogation signal, $P_{r-i}(\phi)$ is the power received from the interference signal at the angle ϕ.

Equipment

Type	equipment	AAU ID number
RFID reader	Speedway Revolution	
Antennas	Two Omni antenna 900 MHz	OEU 19808
Cables	Two N-Male 4 m	1215-05-E6/E4
2-1	Three 0°	A6-21304
1-2	One 90°	A6-21130
Airline	Adjustable 20 cm	E-4-833
Signal gen.	Rohde Schwarz SMP22	A6-215-F3
Tag	Four Alien Squiggle 9640	-
PC	Dell Optiplex sx260	57347
PC software	Multireader 6.6.2	-

Table A.7: Equipment required for setup

Setup

The wiring of the components is illustrated by the following figure A.4. R_{x° and I_{x° represents the reader and interference signals phase offset as they are entering the next component. It should be clear from the figure, how both elements are feed with a 0° reader signal, where as element 1 is fed with a 0° interference signal and element 2 with a 180° off set interference component. Also as each cable used to interconnect the different components introduce different phase, an airline is used to calibrate the hole system from input to the output of the last combiners. The calibration is done with a network analyzer.

Further more an illustration of the environmental setup is illustrated in figure A.5, to show how the measurement is conducted. The antenna spacing is set carefully to $\lambda/2$.

Procedure

The measurements are conducted in a $9\text{m} \cdot 6\text{m}$ lab room, where two antenna elements are coupled to the reader and interference source signal, as specified by figure A.4. A spectrum analyzer is connected with a dipole antenna, and set for a 12 sec measurement time span, at the RFID reader center frequency. The dipole is then moved 3 m perpendicular to the two antenna elements. Firstly radiating the reader signal, and then the interfere

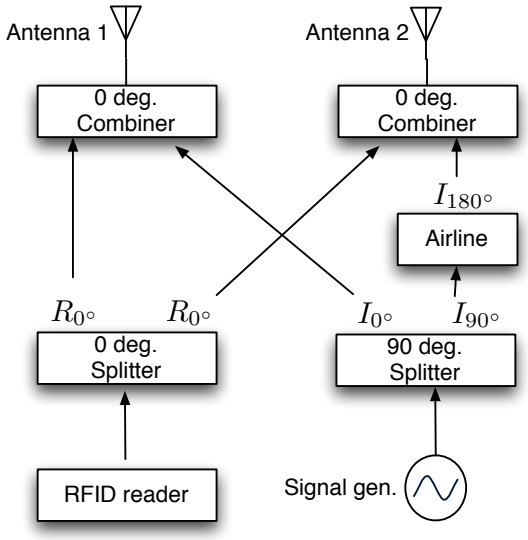

Figure A.4: Illustration of how the reader and signal generator is connected to the elements.

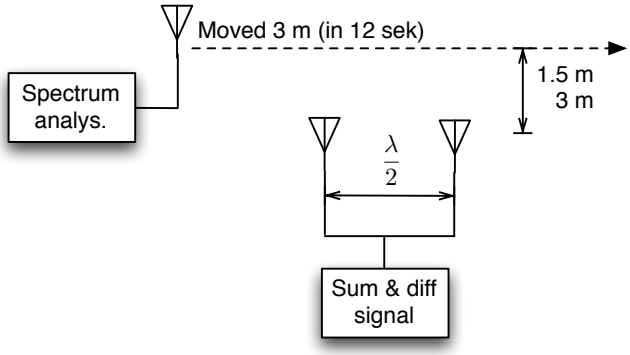

Figure A.5: Illustration of the components wiring and setup

signals. The measurements are done at 1.5 m and 3 m from the radiating elements.

It is expected that the reader signal adds constructively in the broadside center point, where as the interference signal adds destructively at the broadside center point. Also the distance to which these summations are vivid, is an important factor to clarify.

If the expected results are evident, a procedure with live tag measurements is conducted. Here multiple tags are aligned perpendicular to the radiating antenna elements at 0.5 m. Measurements both with and without the interference signal is then executed, with the expected outcome of a decreased interrogation zone, revealed by the amount of tags that are detected.

Results

The results of the transmitted power measurement is illustrated by figure A.6, at 1.5 m. As noted under the procedure description, the reader signal and the interference signal is enabled one at a time, however they are plotted together, to compare the behavior.

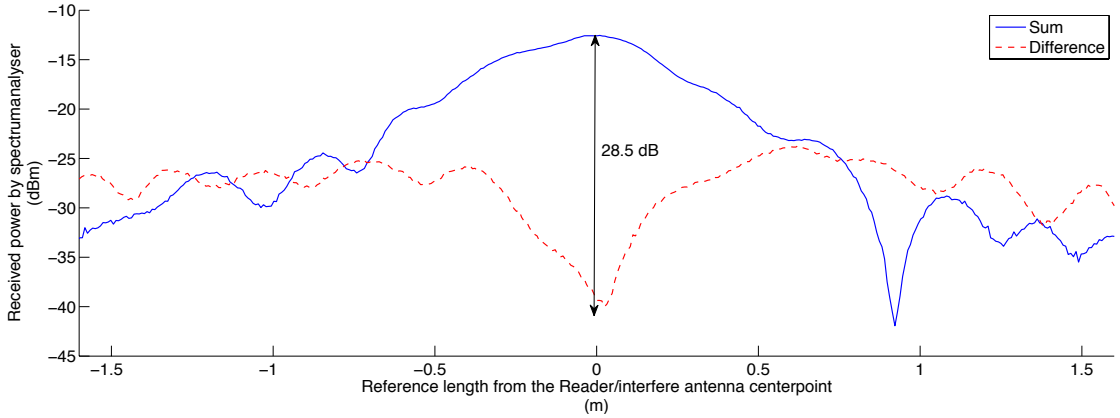

Figure A.6: The sum and difference signal measured individually at 1.5 m, and plotted together.

The expected results are evident for both sum and difference signal, and the dynamic range of the broadside radiation is approx. 28.5 dB.

The same measurement at 3 m is presented by figure A.7.

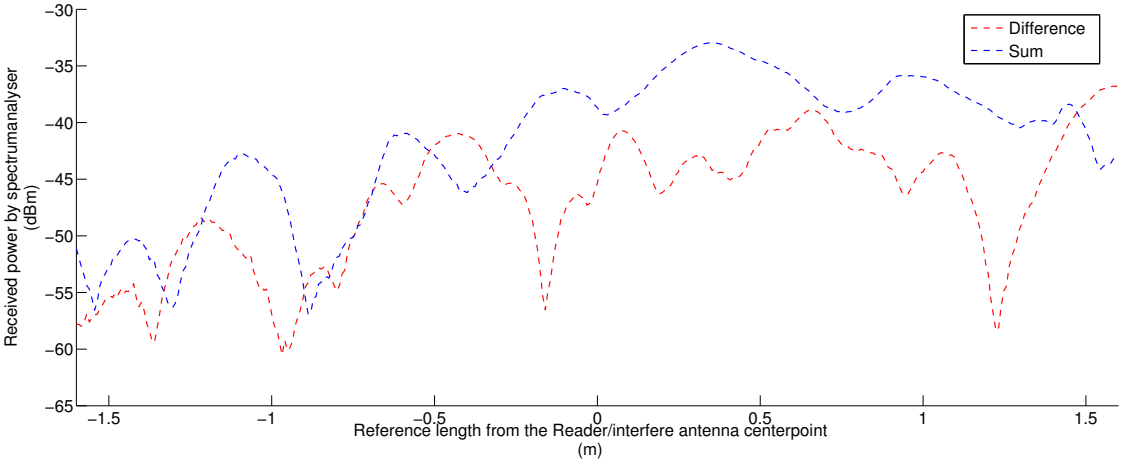

Figure A.7: The sum and difference signals measured 3 m from the radiating antennas. It is clear that the null becomes less sharp.

The clear sum and difference effects in the measurement from 1.5 m, becomes undefined when the reading is made from a distance of 3 m. This is expected as a natural cause of multipath effects.

As the deliberate interference effects has shown to be as expected, tests with live tags is commenced.

Live tag test

As described in the the procedure, a test with multiple tags set on a row is to be made. The setup is illustrated by figure A.8

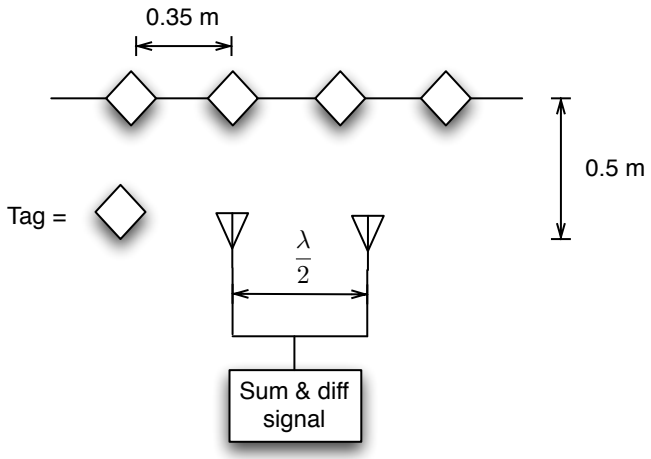

Figure A.8: Multiple tags set on a row, to determine the interrogation zone with the live RFID system

First the test is setup with no interference signal to verify the broad interrogation zone, by how meany of the four tags that are detected by the reader. Afterwards the interference signal is applied, and the number of tags are noted. One tag is moved along a perpendicular line of the transmit antennas, to determine how wide the interrogation zone actually is.

Results

The results from the initial test with the interference signal disabled is shown in figure A.9.

It is seen that only 3 of 4 tags are readable by the commercial RFID reader. Thus the interrogation zone without interference signal is a minimum om 70 cm, 0.5 m from the antennas.

The results with the interference signal enabled is presented by figure A.10. Clearly the interference signal indeed effects the interrogation zone of the reader, hence the objective

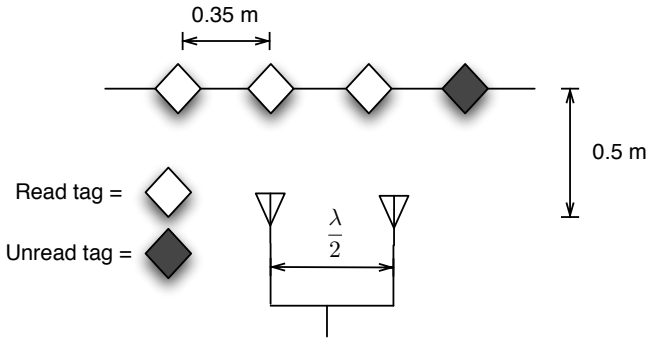

Figure A.9: Tag reading with the reader (sum) signal enabled, proven to read 3 out of 4 tags, indicating a width readability of min 70 cm.

is successfully obtained. It is noted that the readable tag was not centered completely between the two antenna elements, indicating some offset is in effect. However this is tune able.

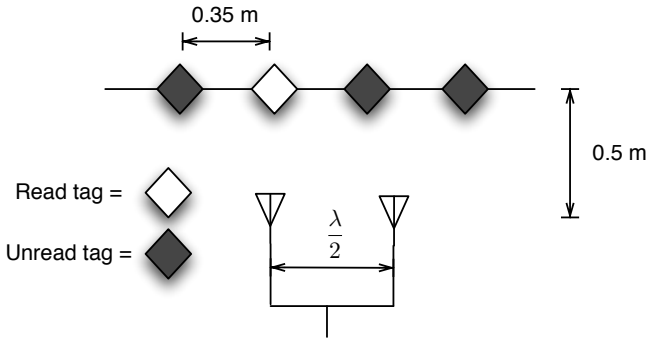

Figure A.10: The final result with the interference signal causing a limited read area.

By moving a tag from the center of the two antennas to each side, the interrogation zone width is determined to be approx 6 cm or 7 $^\circ$ at 0.5 m.

Conclusion

The presented results indicates an operative concept, with the expected behavior. A max. reader distance with this setup can be concluded to be more than 1.5 m, and less then 3 m. The interrogation zone is minimized from above 70 cm to 6 cm in the 0.5 m range.

B USRP RFID Reader Performance

This chapter contains the results obtained by testing the RFID reader package developed by Michael Buettner, to get an indication of the performance, both in successful decoding rates and bandwidth of the system and used tags.

B.1 EPC Decoding Performance

Aim

The objective of this measurement is to test the used USRP1 RFID reader application, to verify its operation and gain a reference point for the further development of the system.

Theory

Every tag in reader vicinity receives a Query command, containing the Q value. The tag then selects a slot between 0 and 2^Q, where tag at slot 0 responds with a random 16 bit number. The reader decodes and reply the same number in an "ACK" command. If the two numbers match, the tag reply its EPC and a CRC check. The correspondence is shown in figure B.1.

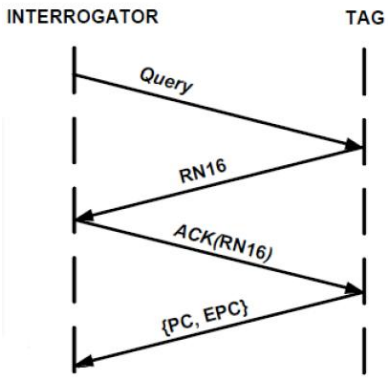

Figure B.1: Reader - Tag communication according to EPC Gen2 standard, for EPC extraction [1]

This communication is handled by the RFID reader package adopted and used on the USRP, and is expected to function with live EPC Gen2 tags.

Equipment

The equipment used for the reader performance test is listed in table B.1, where three PC systems are noted as central elements in the testings.

Type	equipment	AAU ID number
RFID reader	Ettus URSP1	-
D-boards	Two RFX900* 750-1050 MHz Rx/Tx	-
Antenna	Two OMNI Antenna 900-/1710-2170 MHz	AU-8050
Cables	Two SMA-Male to N-Male	-
Tag	Alien Squiggle 9640	-
PC1	Apple MBP - C2 Duo 2.4 GHz - 4 GB 1067 Mhz DDR3	-
PC2	Intel C2 Duo 3.0 GHz - 4 GB 1067 MHz DDR3	-
PC3	Intel i5 Quad Core 3.7 GHz - 8 GB PC3 10700 DDR3	-
USRP software	USRP RFID software package	-
PC software	Gnuradio 3.3	-
OS (PC 1,2,3)	Ubuntu 10.4 LTS (2.6.32-38 generic)	-

Table B.1: Equipment used for measurement

*) The RFX900 daughterboards has been modified at the TX port. The ISM band filter is removed and C204 is populated with a 100pF capacitor. This is required as the ISM filter may be damaged from the CW emitted. Also this increases the possible output form 200 mW to $\approx$ 500 mW.

Setup

The reader and antennas are set up as shown on figure B.2, as a bi-static system. The tag is placed directly in front of the receiver antenna, to increase the probability of the reader being able to decode tag reply.

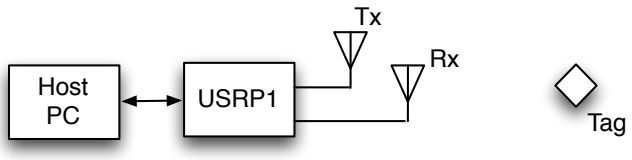

Figure B.2: Generic USRP1 RFID reader test setup

Static parameters of the reader is set as follows:

Parameter	Setting
Tag uplink (BLF) frequency	41.667 kHz
R->T cal	72 μs
USRP decimation factor	32
Software decimation factor	4
Samples per pulse (tag signal)	6
Q value	0
Center freq.	866.5 MHz

Table B.2: Static parameters for the reader

Dynamic parameters will be the encoding, shifting between subcarrier levels, from Miller 2 to 8.

Parameter	Setting
Encoding level	Miller-2,-4,-8

Table B.3: Dynamic parameters for testing

Procedure

A single tag is placed perpendicular to the Rx antenna in a distance of 20 cm. The antenna spacing is $\lambda/2 \approx$ 16cm. The reader is tested by three runs, where each run consists of 10 power ups, making the success rate 10 successfully EPC extractions on each run. Each of the three PC systems are tested with all three Miller encodings, to indicate the apparent success rate of each system. A tag reply package can be undetected, corruptly detected/CRC error, or successfully detected.

Results

The results are denoted in the order [Received frame / Successful EPC / CRC Error]

Preliminary results of the three systems:

PC1			
run	Miller-2	Miller-4	Miller-8
1	1/0/1	3/0/3	0/0/0
2	0/0/0	4/0/4	2/0/2
3	3/0/3	1/0/1	0/0/0

Table B.4: Reader tested with PC1

PC2			
run	Miller-2	Miller-4	Miller-8
1	5/0/5	3/0/3	2/0/2
2	1/0/1	4/0/4	0/0/0
3	3/0/3	0/0/0	0/0/0

Table B.5: Reader tested with PC2

PC3			
run	Miller-2	Miller-4	Miller-8
1	8/7/1	6/4/2	8/4/4
2	10/6/4	10/6/4	9/6/3
3	10/10/0	9/8/1	10/9/1

Table B.6: Reader tested with PC3

The results indicate that PC3 is the only system that meets the requirements to enable successful package detection and decoding. Thus this system is further investigated to give an indication of why PC3 is successful.

The RFID package is evaluated on PC3, by regulating the number of cores enabled and the CPU clock frequency. The results are listed in table B.7.

PC3			
Number of Cores	2	3	4
1.8 GHz	0	398	935
2.4 GHz	0	816	933
3.3 GHz	0	929	983
4 GHz	x	x	953

Table B.7: PC3 test with number of successfull decoding out of 1000 Query's at 50 cm, 866.5 MHz and Miller-2 with varying enabled cores and CPU frequency

The data is plotted in figure B.3

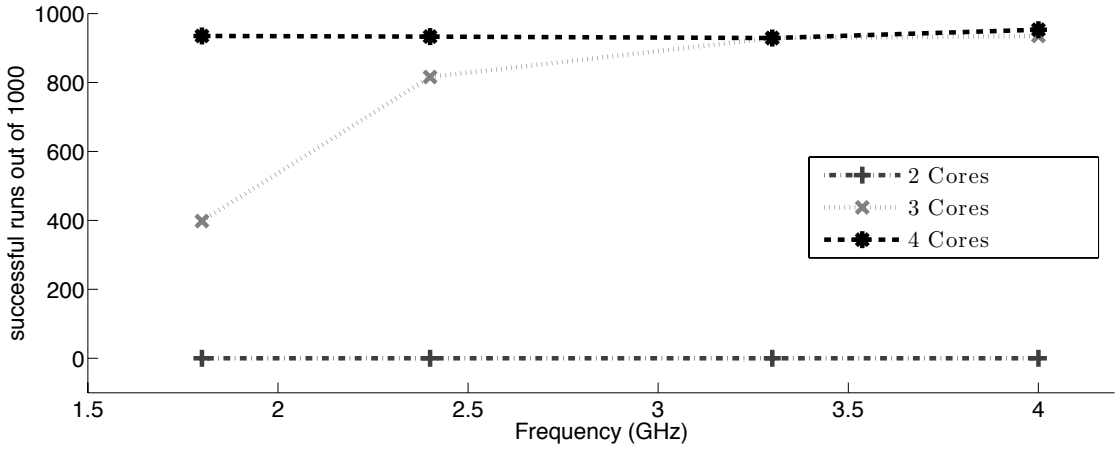

Figure B.3: USRP RFID reader package tested at different CPU settings, 1000 readings at 50 cm, 866.5 MHz and Miller-2

Discussion

The preliminary results executed on three different computers indicates that a fast processor is required for the RFID reader package to successfully interrogate tags, with no or little errors. This lead to additional measurements with different CPU clock frequency and Core settings, to gain less ambiguity in the conclusion drawn from the measurements. It is evident that at least 3 cores are needed to obtain a satisfying result, with the success rate increasing along with the clock frequency. At 4 cores the processor clock speed seams to have no influence on the success rate. It is noted that 4 cores clocked at 4 GHz does not tend to perform superior of a 3.3 GHz system.

To further argue towards clarifying the results, it is noted that the RFID USRP transmitter

needs to radiate the CW, to power the tag even when no reader commands are to be transmitted. This complicates the reader to tag timing constraints, as the Tx buffer is latched with CW samples through the OS kernel. These samples are processed by the CPU, hence are determined by the processing power and clock frequency. As the CW samples are processed by different number of cores and speed, the number of CW samples between reader commands becomes a variable that is system dependent. This causes a mismatch between Rx and Tx timing in the RFID software subroutines, as it is unknown exactly how many CW samples are queued in the Tx buffer, when a reader command is initiated.

Conclusion

By the means of the conducted measurements and derived results, a conclusion is drawn, towards the performance of the RFID reader at different hardware specifications. It is evident that the timing constraints are not being fulfilled, when a CPU with a number of cores below 3 is utilized. Furthermore the clock frequency is required to be in the 3 GHz range. An increase in clock frequency can not be concluded to benefit the success rate, when reaching 4 GHz.

B.2 USRP RFID reader bandwidth

Aim

The aim of this measurement is to investigate the bandwidth of the RFID reader system. Hence derive a frequency response chart, to define the reader and tag performance when frequency and distance are the variables.

Theory

The tag used in this setup is an Alien Squiggle 9640 UHF EPC Gen2 tag. From the datasheet the bandwidth of the tag is defined to be between 840-960 MHz. A frequency responds chart from the datasheet is illustrated in figure B.4.

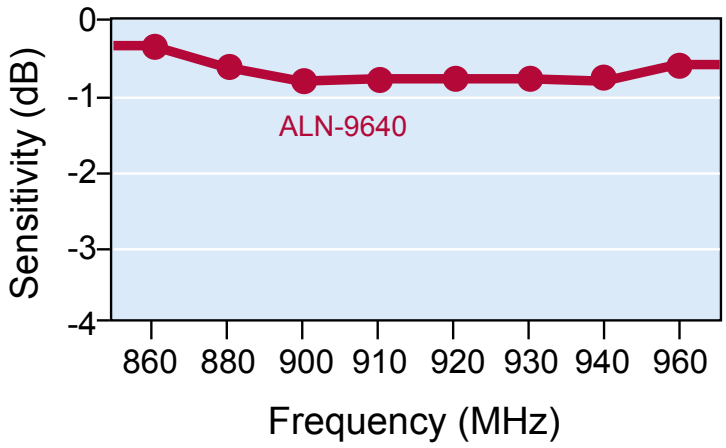

Figure B.4: Frequency response chart of Alien Squiggle 9640 tag [5,p. 3]

Furthermore the USRP is equipped with two RFX-900 daughterboard front-ends, that limits the reader from 750 to 1050 MHz.

The Rx and Tx antennas used are Intermecs RFID circular polarized patch antennas, with a frequency range specification of 865 - 928 MHz. Hence the apparent bottleneck would be the Intermec antennas.

The maximum read distance between the tag and reader can be evaluated by a simplified friis equation as

$$P_{tag} = P_{rx}\left(\frac{\lambda}{4\pi d_{max}}\right)^2 G_{rx}G_{tag} \tag{B.1}$$

P_{tag} is the minimum power required for the tag to operate, P_{rx} is the power transmitted by the reader, $\lambda = {}^{c}/_{f_c}$ is the wavelength of the carrier frequency, G_{rx} and G_{tag} is the tag and reader antenna gains, and finally d_{max} is the distance between the tag and reader antennas.

Simplifying the expression in B.1 for directly deriving the distance, and inserting the variables listed in table B.8 the maximum distance evaluated at the European RFID center frequency $f_c = 866.5$ MHz as shown in (B.3)

$$d_{max} = \frac{10^{(P_{rx}+G_{rx}+G_{tag}-P_{tag})/20}}{41.88 f_c} \tag{B.2}$$

Parameter	Value
P_{tag}	-10 dBm
P_{rx}	27 dBm
f_c	866.5 MHz
G_{rx}	8 dBi
G_{tag}	1 dBi

Table B.8: Parameters of the system, to evaluate max read distance

$$d_{max} = \frac{10^{(27+6+1-(-10))/20}}{41.88 \cdot 866.5}, \rightarrow d_{max} = 4.36\text{m} \tag{B.3}$$

It is noted that the gain of the tag antenna is not known from the datasheet, but is estimated to be 1 dBi.

Equipment

The used equipment for evaluating the reader and tag bandwidth, is listed in table B.9.

Type	equipment	AAU ID number
RFID reader	Ettus URSP1	-
D-boards	RFX900 750-1050 MHz Rx/Tx	-
Antennas	Two Intermec RFID patch Antenna 865-928 MHz	AU-8050
Cables	Two SMA-Male to N-Male	-
Tag	Alien Squiggle 9640	-
PC	Intel i5 Quad Core 3.3 GHz - 8 GB PC3 10700 DDR3	-
USRP software	USRP RFID software package	-
PC software	Gnuradio 3.3	-
OS	Ubuntu 10.4 LTS (2.6.32-38 generic)	-

Table B.9: Equipment used for measurement

Setup

The system setup is illustrated by figure B.5, where the Tag/Reader distance is denoted by d.

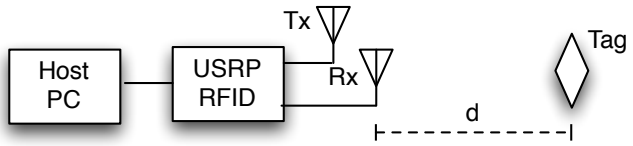

Figure B.5: Illustration of the trail setup, with the tag being exposed to a range of frequencies at different distance

Static parameters of the reader is as chosen as follows:

Parameter	Setting
Tag uplink (BLF) frequency	41.667 kHz
R->T cal	72 μs
USRP decimation factor	32
Software decimation factor	4
Samples per pulse (tag signal)	6
Q value	0
Number of Query rounds	1000

Table B.10: Static parameters for the reader

Dynamic parameters in the test is shown in B.11.

Parameter	Setting
R-T distance (d)	5, 15 and 50 cm
Frequency	756 to 1016 MHz, 10 MHz step

Table B.11: Dynamic parameters for testing

Procedure

To determine the bandwidth of the USRP reader, a tag is held at a fixed distance, and then exposed to reader commands, modulated at different CF, spanning from 756 MHz to 1016

MHz. This is then done for three different Reader/Tag distances. It is expected that the reader successfully decodes the tag at all three distances, when inside the European RFID communication frequency band. However the total bandwidth of the system, and what is the bottleneck is unpreductable from the presented hardware specifications, although the Intermec antennas are the bandwidth limiters by specification details.

Results

Figure B.6 illustrates the frequency response of the system, when the tag is read at frequencies from 756-1016 MHz range in steps of 10 MHz. The RFID reader is not able to function properly when set to 750 MHz, nor above 1018 MHz.

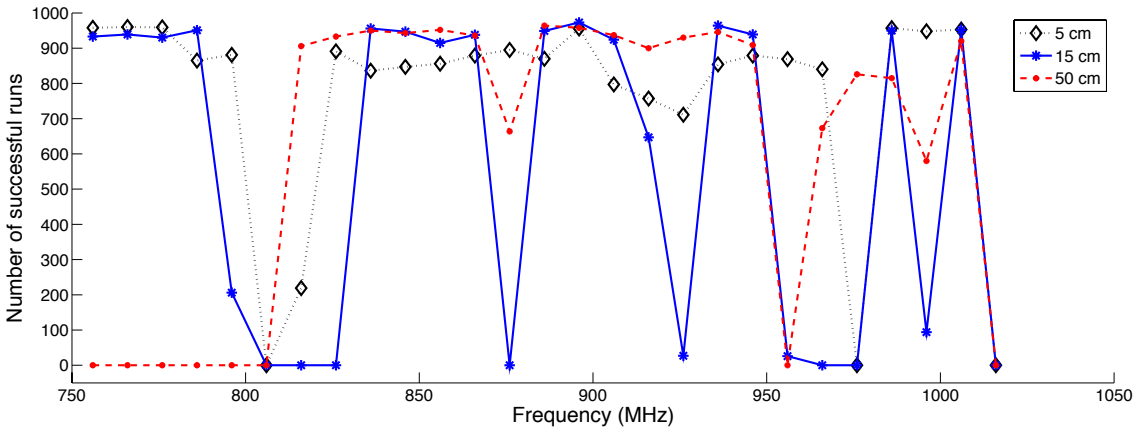

Figure B.6: Frequency response chart of the system at different spacing from tag to reader Rx/Tx antennas

As the results from the measurements indicates strong interference dropouts, the test is also conducted in a RF shielded cabin, with the results presented in figure B.7

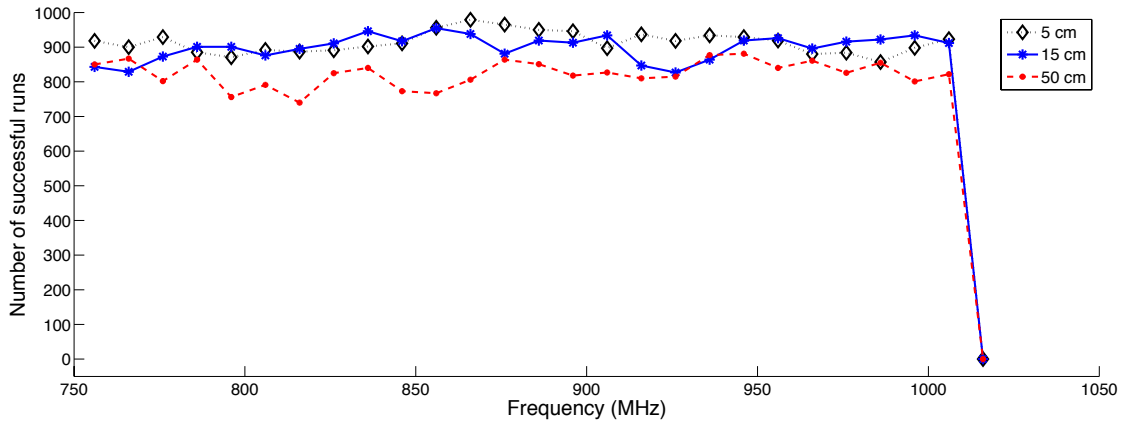

Figure B.7: Frequency response chart of the system at different spacing from tag to reader Rx/Tx antennas, measured in a RF shielded cabin

Discussion

By the initial hardware system limitations, from the tag, and especially from the Intermec RFID patch antennas, the system outperform the specifications, well above what was expected. A bandwidth of nearly 300 MHz was evident, however deep fades occurred at all trailed distances, at nearly the same frequencies. However these where expected to be interference and fading patterns, thus the experiment showed much better results when conducted in a shield cabin. The RFX900 daughterboards proved to be the system limiter, as no sign of degradation appeared before reaching the RFX900 boards upper and lower frequency boundaries.

Conclusion

The USRP RFID reader is tested, and from the results it is evident that the reader is highly susceptible to channel noise, however the system performed well above and below the European UHF frequency band. Thus, the large operational spectrum makes the reader suitable for frequency diversity, enabling extended frequency spacing.

C Multi-carrier measurements

This appendix serves to present the measurements made, of the proposed and implemented solutions to obtain a functional multi-carrier reader. Furthermore to classify how the two carriers influence the tag and each others performance. This is done with RSSI level and successful CRC cycles logging.

C.1 Multiple command gate test

In section 9.1 on page 61 a Multiple reader_command_gate setup was presented in terms of the system illustrated by C.1.

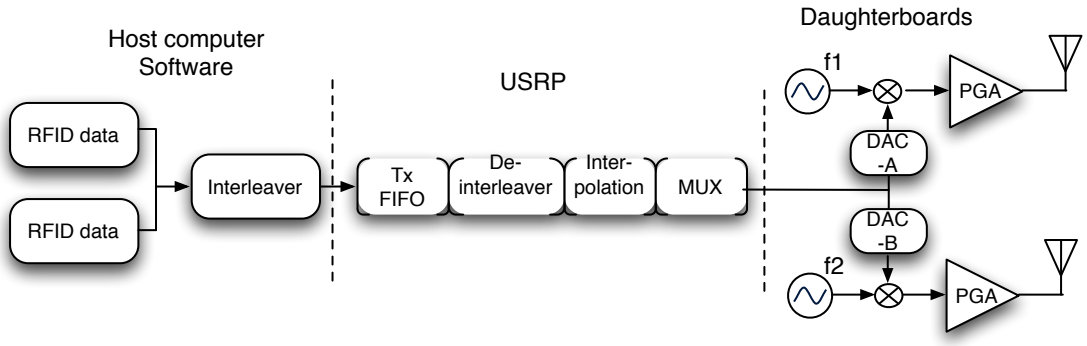

Figure C.1: Mutli-carrier reader, done with a double Tx reader_command_gate block and an interleaver

The system is implemented and ready for testing, hence the following equipment is required for testing.

Equipment

The used equipment for the test is listed in table C.1

Type	equipment	AAU ID number
RFID Multi-reader	Ettus URSP1	-
D-boards	RFX900 750-1050 MHz Rx/Tx	-
Cables	Two SMA-Male to N-Male	-
Antennas	Two Intermec RFID patch	1415-02
Spectrum analyzer	R/D FSEM30	57634
PC software	GNU Radio 3.3	-

Table C.1: Equipment used for measurement

Procedure

Firstly the USRP Tx_A and Tx_B is connected to the spectrum analyser, to verify the dual carrier output. Then the USRP is connected to the Intermec antennas to read live tags. It is expected that both carriers are modulated with the same reader signal. Furthermore the tag responses are expected to be received on both CF, enabling the USRP reader to decode tag responses on either frequencies.

Results

The output from Tx_A and Tx_B is verified to be as expected on both CF, with a spectrum analyzer. However the live tag readings had no success as show in table C.2

Tx_A(866.5 MHz)	Tx_B (876.5 MHz)
0	0
0	0
0	0
0	0
0	0

Table C.2: Results for live tag readings with multiple CF in the air, success out of 100 readings, trailed 5 times

Conclusion

The system proved unsuccessful, although the data was measured to be modulated on to both CF, the tag responds was negative.

The RFID message signals datarate at miller = 4 is typically of 80 kb/sec. The increase in data rate from the two command gates is expected to have caused the system to fail the maximum reader message response time of 500 us

C.2 FPGA MUX test

As the results from the Multi reader_command_gate proved to be unsuccessful, the test for the proposed changes in the FPGA MUX routing is conducted and presented in the following.

Aim

The aim of this measurement is to verify the correct multi-carrier modulation output, and correct tag response on both carriers. The decoding is also to be tested on both carriers.

Equipment

The required equipment of the measurements is listed in table C.3

Type	equipment	AAU ID number
RFID Multi-reader	Ettus URSP1	-
D-boards	RFX900* 750-1050 MHz Rx/Tx	-
Cables	Two SMA-Male to N-Male	-
Antennas	Two Intermec RFID patch	1415-02
2-1 Splitter	MCL ZAPDQ-2	1130-01
2-1 combiner	MCL ZAPD-1	1304-00
Spectrum analyser	R/D FSEM30	57634
PC software	Gnuradio 3.3	-

Table C.3: Equipment used for measurement

Due to limited access to fully compatible hardware, it is noted that the lower frequency bound of the MCL ZAPDQ-2 2-1 splitter is 1 GHz. As the reader carrier is set at 865.5 MHz and 876.5 MHz, they are not within the component specifications. However the trail continues.

Setup

The system is setup as shown in figure C.2, where both transmissions are monitored on a spectrum analyzer, to verify that both carriers are transmitting and at the same level. All measurements are conducted in a RF shielded room.

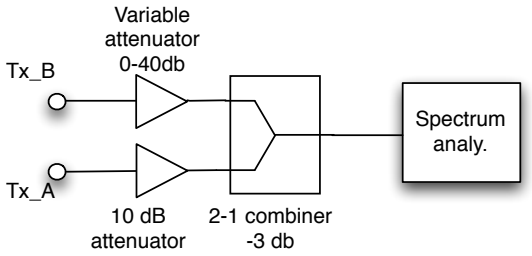

Figure C.2: Multi-carrier reader transmitting on both channels. Tx_A damped 10 dB and Tx_B connected to a variable attenuator, combiner to the spectrum analyser input

The next setup is to verify the actual reader operation on both frequencies, thus connects as illustrated by C.3.

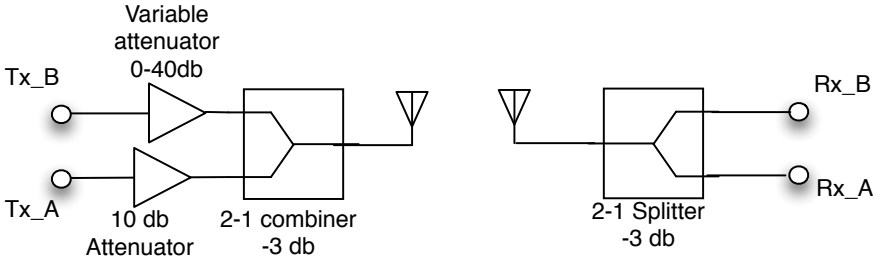

Figure C.3: Mutlicarrier reader transmitting on Tx_A and Tx_B and receiving on Rx_A and Rx_B

It is noted that due to the 2-1 splitter in the receiver chain, the resulting reception levels of Rx_A and Rx_B differs from a SISO setup as each chain in this MIMO setup experience $1/2 mathrm Tx_A + 1/2$Tx_B

Regarding the physical setup, the tag and reader antennas are 120 cm above ground.

Procedure

With the described setup, the initial test is expected to output the message signal on the preset carrier frequencies, at a level that is 13 dB attenuated relative to maximum output (25 dBm). Further it is expected that both carriers are responding the tag message signal, thus providing successful tag respond decoding in both receiver blocks. The final aspect in the measurement, being the Tx_B transmission power variation relative to Tx_A from -10 dB to +10 dB, is expected to reveal that little or no difference in the decoding quality of Tx_A at Rx_A, where as Rx_B RSSI levels are expected to be directly influenced by Tx_B levels.

Results

The carrier levels are verified with the spectrum analyser as show in table C.4

Chain	level
Tx_A	12.2 dBm
Tx_B	11.1 dBm

Table C.4: Verification of Tx_A and Tx_B output levels

Next measurement is to verify the operation of the implemented dual Tx and Dual Rx, with equal gain in both branches.

Reader	Decoder
Freq_A = 865.5 MHz	Freq_B = 876.5 MHz
Out of 1000 cycles	Out of 1000 cycles
949	958
826	608
915	967
901	876
959	911

Table C.5: Verification of the dual Tx and Rx, on difference frequencies

Measurement of the RSSI levels on Rx_A and Rx_B, when Tx_B transmission power is

altered, is show in the following figures. It is noted that Tx_A is attenuated 10 dB, to gain a suitable reference level, as only an attenuator is used.

The results with a tag to reader distance of 55 cm is presented in figure C.4. The Tx_B transmission power is altered with steps of 1 dB. The measurement is conducted in an RF shielded container.

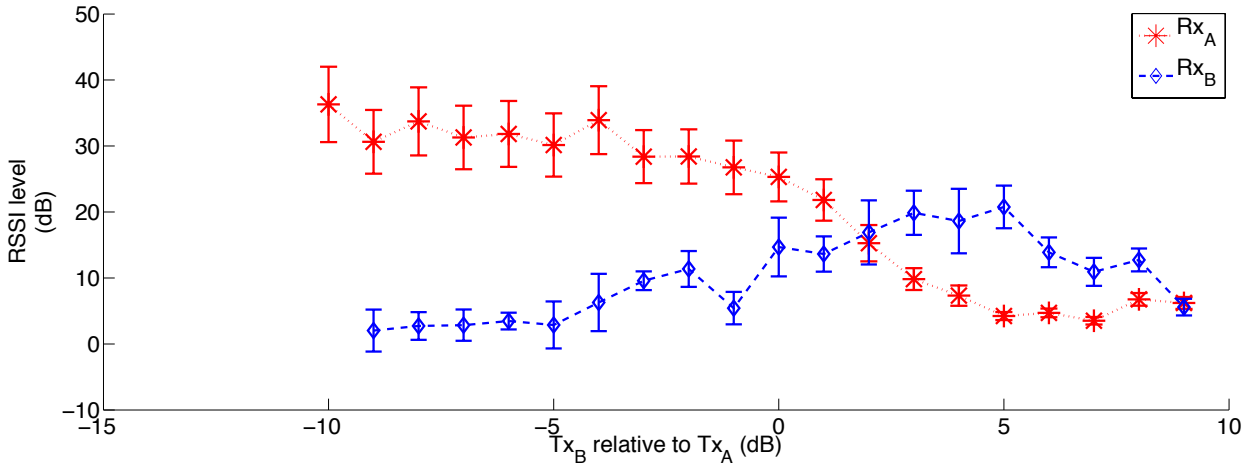

Figure C.4: Multicarrier interrogation with Tx_B power varied, and RSSI levels on Rx_B and Rx_A with a tag/reader distance of 55 cm

A measurement with the tag/reader distance increased to 125 cm, is presented in figure C.5. Less data is provided, as the measurements are done with steps of 5 dB, however the same tendency is evident.

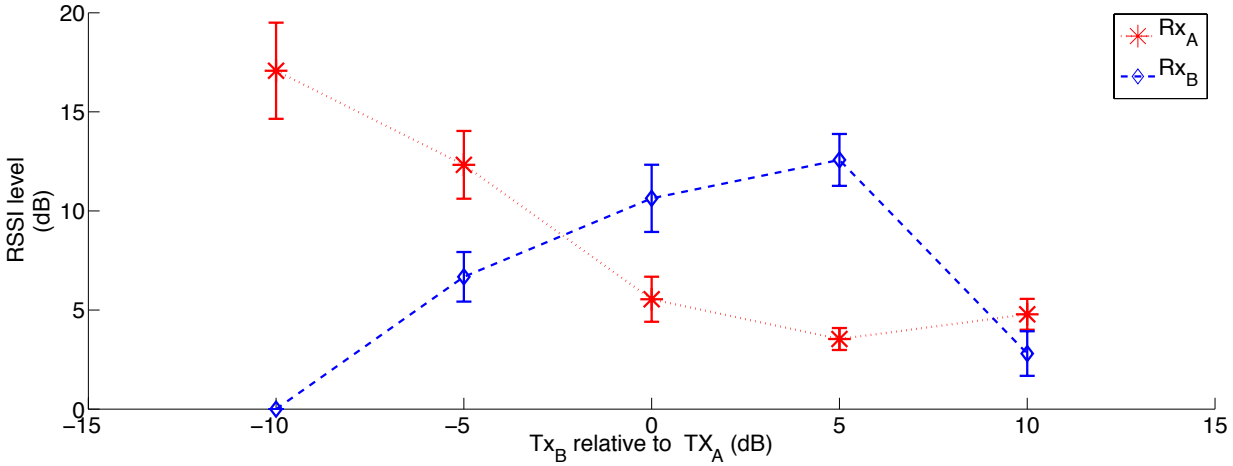

Figure C.5: Multicarrier interrogation with Tx_B power varied, and RSSI levels on Rx_B and Rx_A. Tag/reader distance = 125 cm

As noted all data presented is measured from a electromagnetic shielded room. Although

shielded from external noise, the reflections from the reader itself cause some dispersion. An actual measurement of these effects are not addressed, however the measurements are repeated in an anechoic shield device, that minimizes such implications.

Thus a 55 cm measurement is presented by figure C.6, measured in an anechoic shield device.

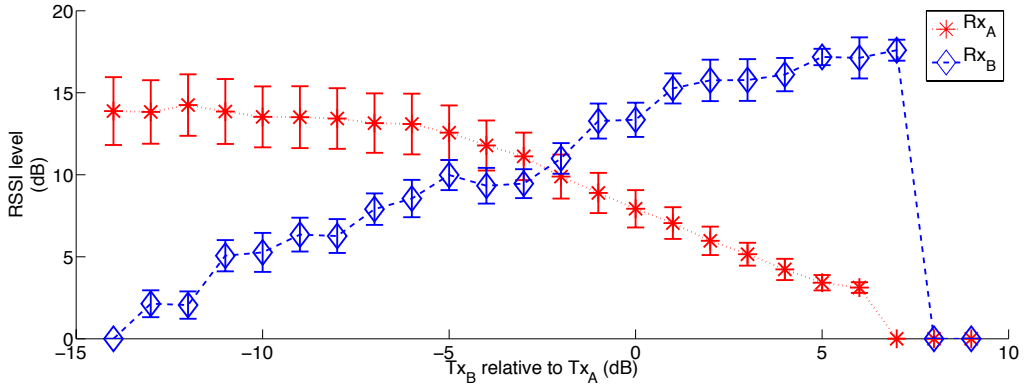

Figure C.6: Multicarrier interrogation with Tx_B power varied, and RSSI levels on Rx_B and Rx_A, conducted in a anechoic shield device. Tag/reader distance = 55 cm

With the RSSI level results presented the successful CRC decoding rates are illustrated in the following figures. Again the data is collected from trails done in the RF shielded compartment, and the anechoic cabin.

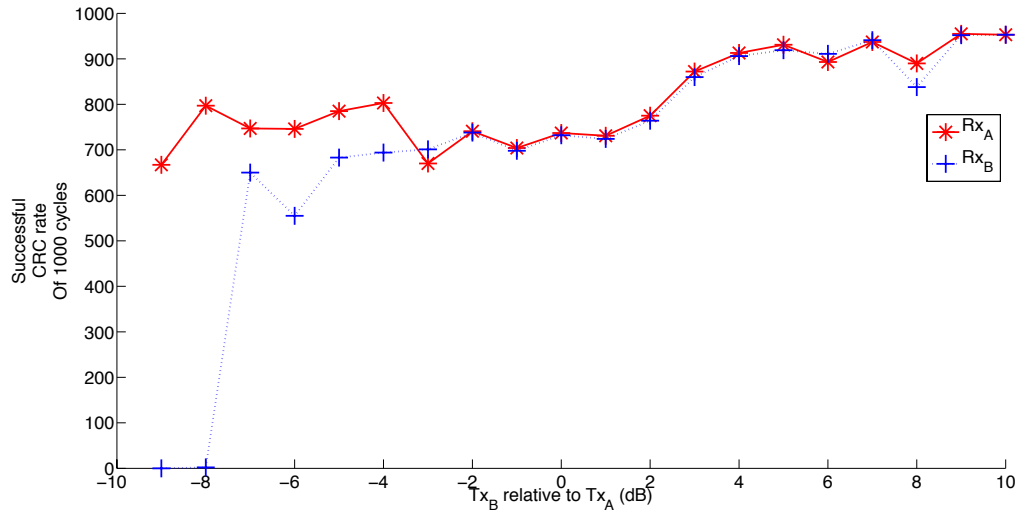

Figure C.7: Illustrates the successful tag decoding of 1000 reader cycles for both Rx_A and Rx_B, for varying Tx_B transmit power in a RF shielded compartment

Finally the results from the anechoic compartment at 55 cm:

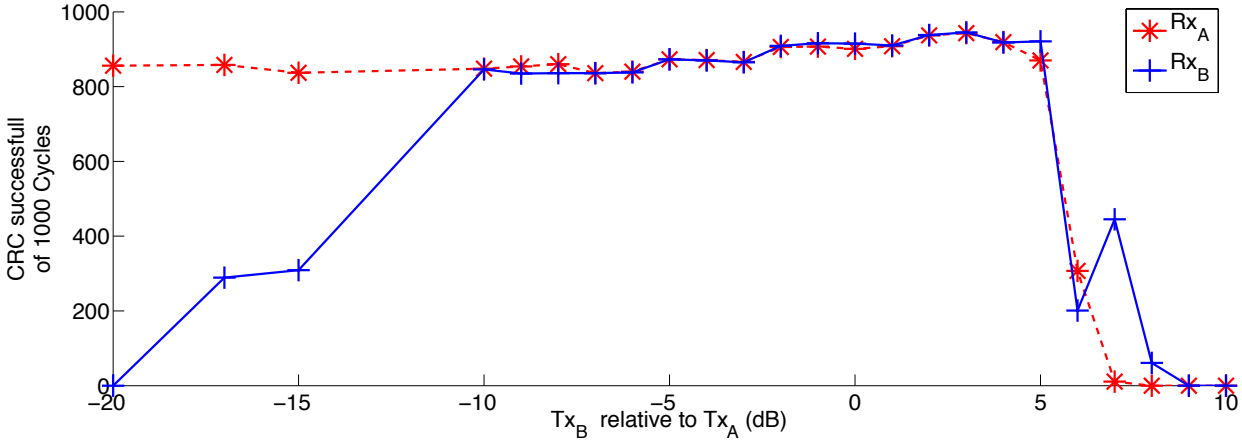

Figure C.8: Illustrates the successful tag decoding of 1000 reader cycles for both Rx_A and Rx_B, for varying Tx_B transmit power in a anechoic compartment

Further measurements

From the results obtained so far it is evident, that the Tx_B power level influences the reader capabilities of Rx_A, although only the Tx_B power level is varied, for instance as seen in figure C.6. The RSSI level drop at Rx_A when Tx_B is amplified is of no obvious cause, therefor further measurements needs to be conducted towards an unambiguous conclusion. A "strip to minimum system" approach is used, to derive a possible cause.

The cause of the obtained results may be hidden in the three basic parts, constituting the system; The transmitter, receiver and the tag. By the nature of the tags construction, it is difficult to verify its exact behavior, in other ways then information gained form external empirical "cause and effect" measures. However the transmitter and receiver is directly measurable. Hence further measurements are made towards verifying the actual I/O performance characteristics of the USRP, to rule out any abnormal behavior in terms of the transmitter and receiver chain, when exposed to different power levels.

Setup

The setup is two folded. Firstly Tx_A and Tx_B is connected directly to Rx_A and Rx_B, with a digital attenuator via combiners/splitters. Tx_B is not enabled to transmit. Secondly Rx_A and Rx_B is connected to a signal generator, to verify the RSSI levels. The two setups are illustrated by figure C.9 and C.10.

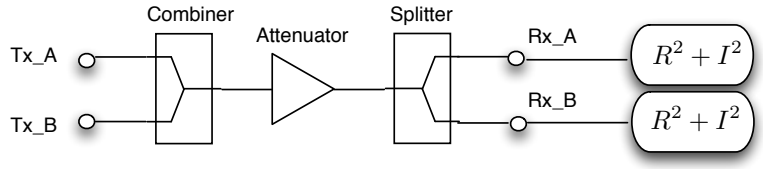

Figure C.9: Tx_A transmitting directly into Rx_A and Rx_B. Tx_B is not enabled

The second setup, in terms of a signal generator directly coupled to the Rx inputs of the USRP.

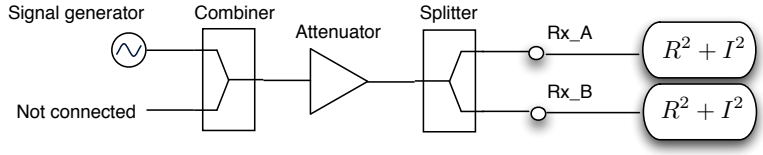

Figure C.10: A signal generator connected to Rx_A and Rx_B via combiner/splitters and attenuater

Procedure

The Tx_A output is held constant at maximum output (25 dBm), as done in the previous measurements. A digital attenuator is then swiped from a starting point attenuation level of -50 dB. The actual range from minimum to saturation is then tested by varying the attenuation level.

Results

The results from the direct connection between Rx and Tx is presented in figure C.11. It is noted that the signal levels presented in the results are corrected for the - 3 dB attenuation pr combiner/splitter.

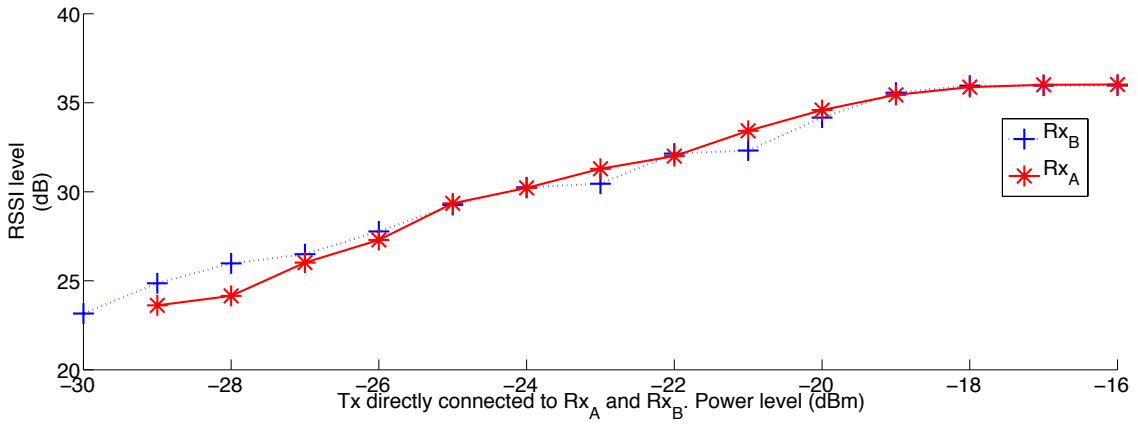

Figure C.11: The RSSI level measured with the attenuation level as a variable

Is is clear that the saturation level is obtained at approx. - 18 dBm, where the level hits a flad curve at 38 dB. The minimum level is reached at -28 dBm output power from Tx, indicating a dynamic range of 10 dB. This is rather surprising, that the lowest and highest level is reach within 10 dB. This is a result that is not expected, however indicates a possible fault in the software, being GNU Radio or the module used to extract I and Q values. This is not investigated further. The test continues with the signal generator coupled directly to Rx ports.

The results of the setup with the signal generator is illustrated by figure C.12, where the receivers tend to have the same behavior as with the USRP Tx as input.

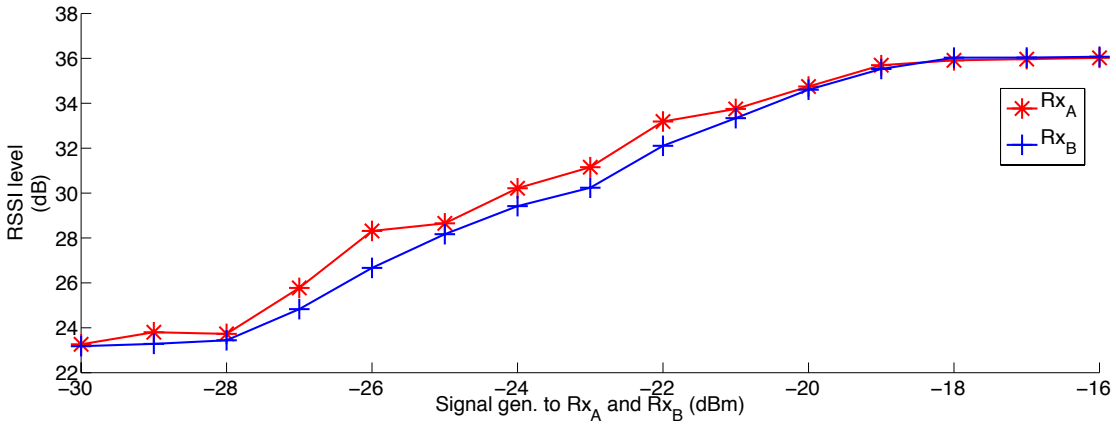

Figure C.12: The RSSI level measured with the attenuation level as a variable

With the direct Tx/Rx coupling and a external signal generator tested to verify a linear tendency in both receiver and transmitter a SISO measurement is made, to verify the system behavior when actual tag communication takes place with only one active carrier.

C.2.1 SISO setup

In the MIMO case the Tx_A and Tx_B is combined with a 2-1 ZAPD-1 to a single antenna element. As this is a SISO setup only the splitter used in the receiver for Rx_A and Rx_B, is connected to a single element via the ZAPD-1 splitter. The setup is illustrated by figure C.13 and is conducted at 55 cm R/T distance, in an anechoich cabin.

Figure C.13: Test setup with a splitter at the receiver

The results are illustrated in C.14

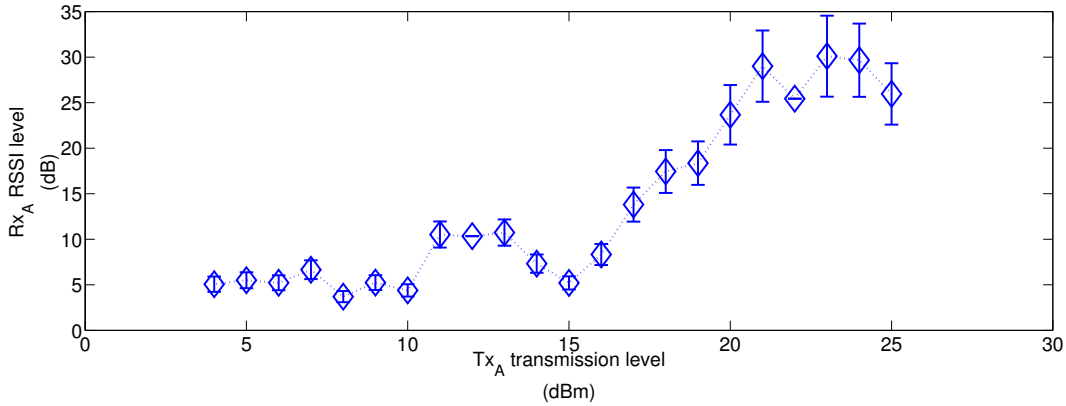

Figure C.14: Test results with the ZAPD-1 splitter at differenct Tx_A transmission power. R/T distance: 55 cm

The RSSI level is as expected when the signals travel in free air.

With the transmitter and receiver chanins tested to verify the linarity, and the presented SISO measurement a conclusion can be drawn.

Conclusion

A multi-carrier system with a frequency spacing of 10 MHz (866.5 - 876.5 MHz) is tested, to clarify the system behavior when the tag is exposed to two modulated carriers. The initial setup proved a tendency not expected, thus further measurements where conducted.

On behalf of the presented results, no apparent cause can be identified to why the attenuation level of one carrier effects the other. The USRP transmitter and receiver is tested, to exclude the cause of non-linearity in either chains. It is therefore concluded that the behavior may be caused by an unknown effect in the RFID tag.

Deliberate Interference tests

D.1 Phase coherence

This measurement journal contains the efforts made towards determining phase coherence and oscillator drift of the two transmission chains Tx_A and Tx_B.

Equipment

Type	equipment	AAU ID number
RFID reader	Ettus URSP1	-
D-boards	RFX900* 750-1050 MHz Rx/Tx	-
Cables	Two SMA-Male to N-Male	-
Network analyser	R/D ZVB-8	56984
PC software	Gnuradio 3.3	-

Table D.1: Equipment used for measurement

Setup

The software application created for this test is illustrated by the schematic shown in figure D.1.

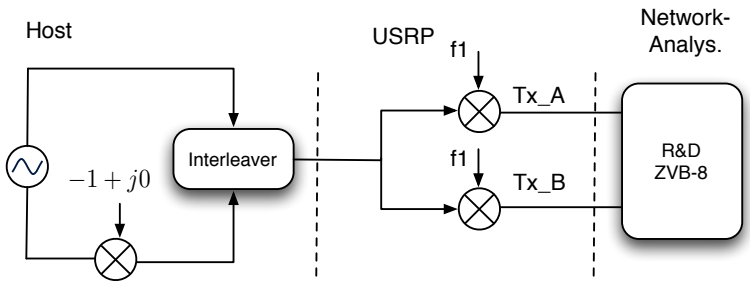

Figure D.1: Deliberate interference partial test schematic, with a sinusoidal noise signal, as the only signal source

The pseudo code of the test is listed in the following:

```
#Create blocks that are used

   usrp = usrp.sink_c()

   interferer = gr.sig_source_c(44000, gr.GR_SIN_WAVE, 250*1e3, 0.5, 0) #(sample_rate, gr.↩
        GR_SIN_WAVE, Freq, amplitude, offset)

   interleaver = gr.interleave (gr.sizeof_gr_complex)

   multiply = gr.multiply_const_cc(complex(1,0))

#Connect blocks to sink

fg.connect(interferer, interleaver(0))
fg.connect(interfere, multiply, interleaver(1))
fg.connect(interleaver, usrp)
```

Results

The obtained results are presented in table D.2

trails	Phase difference	Drift (after 4 min)
1	26°	0°
2	176°	0°
3	-86°	0°
4	55°	0°
5	41°	0°
6	-19°	0°
7	-133°	0°
8	124°	0°
9	-179°	0°

Table D.2: Results for the phase coherence test

Conclusion

The results indicate that the system does not perform the expected phase coherence, as the phase difference is argued to be random at any given time the application is executed.

Antenna radiation

This appendix serves to specify the relevant theory behind multi-antenna systems, as is utilized by the deliberate interference concept.

A two-element array setup is illustrated by figure E.1, where the two elements are lined on the x-axis. The figure illustrates both Cartesian (x, y, z) and Spherical (r, θ, ϕ) coordinates, both used throughout this section. The spacing between the elements is an important factor, when considering the desired functionality, as it influences how the two elements interact when radiating. An element spacing of no more than $\lambda/2$ is in many cases used to limit the degrading effects of grading loops, where λ denotes the wavelength. The frequency regulations of RFID operation in Europe is set for a bandwidth of 2 MHz, in the span from 865 to 867 MHz.

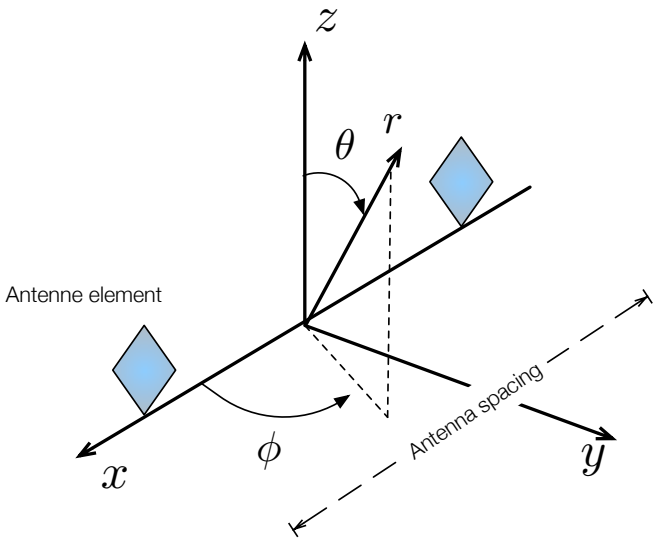

Figure E.1: Illustration of the two-element antenna array setup

The wavelength is derived by $c/f = \lambda$, where c equals the speed of light ($c \approx 300 * 10^6$ m/s). Thus for $f = 866$ MHz the wavelength $\lambda = 34.6$ cm, concluding an element spacing Δ of 17.3 cm

The antenna elements illustrated in figure E.1 are assumed to be identical dipoles. There are several control aspects that can be used to form the effective pattern of such an array. The relative displacement between the elements, the individual amplitude and phase and radiation patterns are parameters used to control the total radiation pattern form the array.

These parameters can serve in the solution towards a controllable interrogation zone.

By the effects of the elements being identical, the total field of the array is essentially a vector addition of all the individual radiations. This principle is illustrated in figure E.2 a). With equal phase excitation and by using the element spacing $d = \lambda/2$, phase accumulation occurs at $\phi = \theta = \pi/2$. Hence in the direction orthogonal to the array line, also refereed to as a broadside radiation pattern. In E.2 b), waves propagating parallel to the array line is considered. Here the signal propagates a half wavelength distance between the elements, introducing a 180° phase turn causing the two vectors to reduce to a theoretical zero.

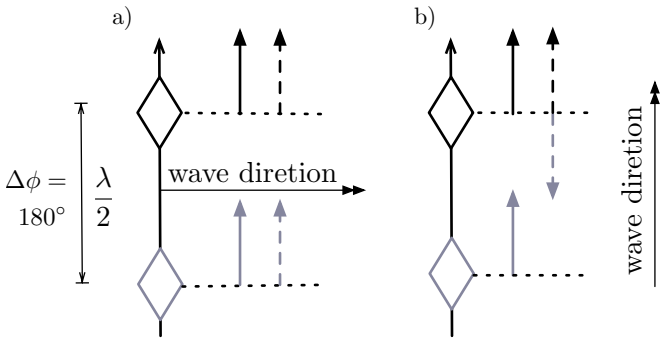

Figure E.2: a) Waves propagating in the $\phi = \theta = \pi/2$ direction experience signal accumulation. b) Waves in $\phi = 0$ and $\phi = \pi$ direction experience phase cancellation

If a single element pattern is denoted by E_i, then the total field radiated by the two elements is given by

$$E_{total} = E_1 + E_2$$

, if it is assumed that there is no coupling between the elements [2,p. 284]. A more general theoretical approach is however introduced by the pattern multiplication theorem, denoted by

$$E_{total} = E_{element} \cdot AF \tag{E.1}$$

where AF is the Array Factor (AF) being the far-field radiation of N elements, had they been isotopic radiators. The AF is defined [18,p. 449] as

$$AF(\theta, \phi, \omega) = \sum_{i=0}^{N-1} A_i \exp\left(i^{(k\Delta)/2} \sin\theta \cos\phi\right) \tag{E.2}$$

where N is the total number of elements, $k = \omega/c$ is the wave number, Δ is the element spacing and A_i is the feeding coefficient to the i'th element, composed of the amplitude factor a_i and the phase ψ_i as

$$A_i = a_i \exp(i\psi_i)$$

. The array elements orientation in the plane leads to the following mapping in the AF exponential operator

$$\begin{aligned} \sin(\theta)\cos(\phi) &\rightarrow \text{Array along the x axis} \\ \sin(\theta)\sin(\phi) &\rightarrow \text{Array along the y axis} \\ \cos(\theta) &\rightarrow \text{Array along the z axis} \end{aligned} \tag{E.3}$$

Hence the pattern multiplication theorem is now easily illustrated in the following. The single element radiation pattern of a dipole and the array factor of the two-element array is illustrated by figure E.3

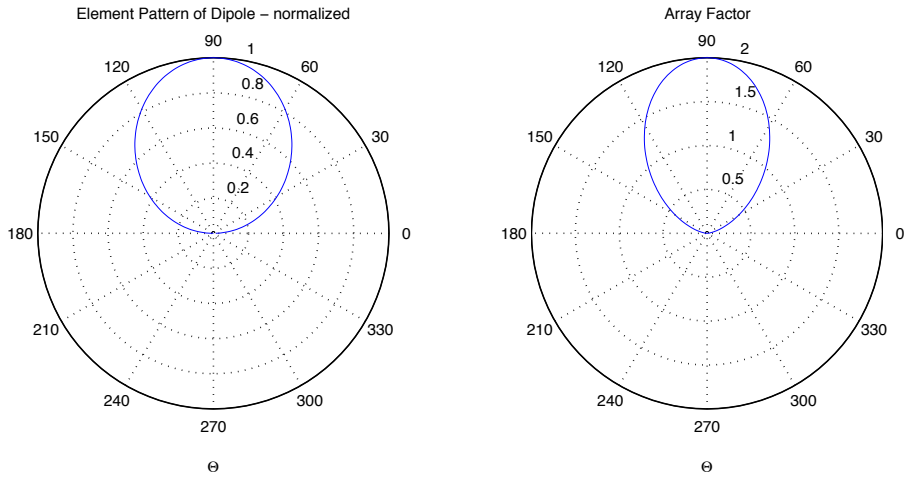

Figure E.3: Illustration of a typical dipole radiation pattern and the Array Factor instantiated by a Two-element array

The resulting total radiated pattern is achieved by multiplying the single element pattern with AF, thus resulting in the pattern illustrated by figure E.4.

When considering the pattern multiplication theorem denoted by equation E.1, it is noted that E_i is not fully capable of describing the far-field pattern. Thus it is expanded by

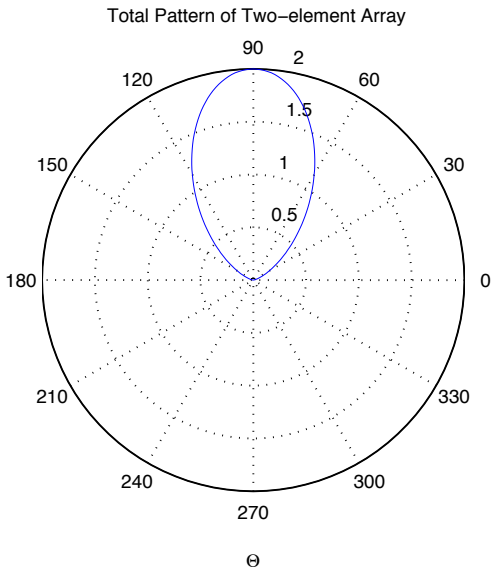

Figure E.4: Illustration of the total pattern, derived from the pattern multiplication theorem

$$E_i(r,\theta,\phi) = F_i(\theta,\phi)\exp(-ikR_i)/R_i \tag{E.4}$$

for

$$R_i = [(x-x_i)^2 + (y-y_i)^2 + (z-z_i)^2]^{1/2} \tag{E.5}$$

Where (x,y,z) is an arbitrary point in the far-field, and (x_i,y_i,z_i) is the location of the i'th element. A valid far-field approximation of R_i can be made [14,p. 13] in terms of

$$R_i = R$$

if the following inequality is satisfied

$$R \geq \frac{2l^2}{\lambda} \tag{E.6}$$

where l is the largest array dimension.

The total far-field array pattern can now be denoted by

$$E(r,\omega) = AF(\theta,\phi,\omega)F(\theta,\phi)\exp(-ikR)/R \tag{E.7}$$

It should be clear from equation E.2 that the AF is dependent on the excitation of the elements, witch leads to the considerations of the feeding coefficients A_1 and A_2. Let each coefficient be a combination of two signals, thus denoted by

$$A_1(\omega) = [G_s\ s(\omega) + G_g\ g(\omega)]\exp(i\psi_1) \tag{E.8}$$

and

$$A_2(\omega) = [G_s\ s(\omega) - G_g\ g(\omega)]\exp(i\psi_2) \tag{E.9}$$

where $s(\omega)$ is an interrogation signal, $g(\omega)$ is a interference signal and $G_{s/g}$ is the gain factor of the interrogation and interference signal. As the coefficient G_s figure with identical sign in both expressions the interrogation signal $s(\omega)$ will act as a sum signal, where as G_g figures with opposite sign, arguing a difference signal.

With the input signals to the two antenna elements defined, the resulting AF can be deduced as

$$\begin{aligned} AF(\theta,\phi,\omega) = & \\ & [G_s\ s(\omega) + G_g\ g(\omega)]\exp(i\psi_1)\exp(i^{(k\Delta)}/_2\sin\theta\cos\phi) \\ & + \\ & [G_s\ s(\omega) + G_g\ g(\omega)]\exp(i\psi_2)\exp(-i^{(k\Delta)}/_2\sin\theta\cos\phi) \end{aligned} \tag{E.10}$$

For the sake of simplicity $\psi_1 = \psi_2 = 0$, this can then be reduced by using Euler's identity

$$\exp(ix) = \cos(x) + i\sin(x)$$

$$AF(\theta,\phi,\omega) = \tag{E.11}$$

$$2G_s s(\omega)\cos(^{(k\Delta)}/_2 \sin\theta\cos\phi)$$

$$+$$

$$2iG_g g(\omega)\sin(^{(k\Delta)}/_2 \sin\theta\cos\phi) \tag{E.12}$$

It should now be evident that the AF consists of two elements

$$AF(\theta,\phi,\omega) = AF_s(\theta,\phi,\omega) + AF_g(\theta,\phi,\omega)$$

where $AF_s(\theta,\phi,\omega)$ is the AF of the sum pattern, thus controlling the radiation of the interrogation signal while $AF_g(\theta,\phi,\omega)$ is the difference pattern, controlling the radiation of the interference signal. The gain factors $G_{s/g}$ introduces the ratio between the two signals, hence the SIR can be controlled by tuning them, leading to controlling the area in which the interrogation is possible.

Nomenclature F

Acronym	Description
ASK	Amplitude Shift Keying
BLF	Backscatter Link Frequency
CIR	Channel Impulse Response
CF	Carrier Frequency
CW	Continuous Wave
DSB	Double Side Band
DDC	Direct Down Conversion
DUC	Direct Up Conversion
EPC C1G2	Electronic Product Code Class 1 Gen. 2
EGC	Equal Gain Combining
FM0	Bi-phase space
FPGA	Field Programmable Gate Array
GRC	GNU Radio Companion
HDL	Hardware Descriptive Language
HPBW	Half-Power Beamwidth
LOS	Line Of Sight
MAC	Medium Access Control
MIMO	Multiple Input Multiple Output
MRC	Maximum Ratio Combining
NLOS	No Line Of Sight
PDP	Power Delay Profile
PDF	Probability Density Function
PIE	Pulse Interval Encoding
PSK	Phase Shift Keying
R/T	Reader to Tag
RFID	Radio Frequency IDentification
RN16	Pseudo Random 16 Bit
RSSI	Received Signal Strength Indication
SCF	Sub-Carrier Frequency
SNR	Signal to Noise Ratio
SIMO	Single Input Multiple Output

SNIR	Signal to Noise and Interference Ratio
SSB	Single Side Band
TR	Tag to Reader
UHD	Universal Hardware Driver
UHF	Ultra High Frequency
USRP	Universal Software Radio Peripheral
USS	Uncorrelated Scatter
WSS	Wide Sense Stationary
WSSUS	Wide Sense Stationary Uncorrelated Scatter

Table F.1: List of acronyms