**ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL OF SCIENCE ENGINEERING AND TECHNOLOGY**

# DESIGN AND IMPLEMENTATION OF A LOW-COST, COMPACT AND LONG RANGE MONOSTATIC UHF RFiD READER WITH READ POINT EXTENSION

**M.Sc. THESIS**

**Özgür BOSTAN**

**Department of Electronics and Communications Engineering**

**Electronics Engineering Program**

**Thesis Advisor: Prof. Dr. Osman PALAMUTÇUOĞULLARI**

**JANUARY 2014**

**ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL OF SCIENCE ENGINEERING AND TECHNOLOGY**

# DESIGN AND IMPLEMENTATION OF A LOW-COST, COMPACT AND LONG RANGE MONOSTATIC UHF RFiD READER WITH READ POINT EXTENSION

**M.Sc. THESIS**

**Özgür BOSTAN**
**(504101221)**

**Department of Electronics and Communications Engineering**

**Electronics Engineering Program**

**Thesis Advisor: Prof. Dr. Osman PALAMUTÇUOĞULLARI**

**JANUARY 2014**

**İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ**

# OKUMA NOKTASI ARTIRILMIŞ, DÜŞÜK MALİYETLİ, KOMPAKT VE UZUN MENZİLLİ MONOSTATİK UHF RFiD OKUYUCU TASARIMI VE UYGULANMASI

**YÜKSEK LİSANS TEZİ**

**Özgür BOSTAN**
**(504101221)**

**Elektronik ve Haberleşme Mühendisliği Anabilim Dalı**

**Elektronik Mühendisliği Programı**

**Tez Danışmanı: Prof. Dr. Osman PALAMUTÇUOĞULLARI**

**OCAK 2014**

**Özgür BOSTAN**, a **M.Sc.** student of ITU **Graduate School of Science Engineering and Technology** student ID 504101221, successfully defended the **thesis** entitled "**DESIGN AND IMPLEMENTATION OF A LOW-COST, COMPACT AND LONG RANGE MONOSTATIC UHF RFiD READER WITH READ POINT EXTENSION**", which he prepared after fulfilling the requirements specified in the associated legislations, before the jury whose signatures are below.

| | | |
|---|---|---|
| **Thesis Advisor:** | **Prof. Dr. Osman PALAMUTÇUOĞULLARI**<br>Istanbul Technical University | ...................... |
| **Co-advisor:** | **Asst. Prof. Dr. Serkan TOPALOĞLU**<br>TRON Elektronik Sistemler A.S. | .............................. |
| **Jury Members:** | **Prof. Dr. Selçuk PAKER**<br>Istanbul Technical University | ............................. |
| | **Prof. Dr. Burak POLAT**<br>Beykent University | .............................. |
| | **Oğuzhan KIZILBEY, Ph.D.**<br>TUBITAK | .............................. |

**Date of Submission : 27 January 2014**
**Date of Defense : 31 January 2014**

***To my family,***

## FOREWORD

I would like to express my gratitude to the many people who have made my graduate studies possible and who have made it such a rewarding experience. First, I would like to thank Prof. Dr. Osman PALAMUTÇUOĞULLARI, my research advisor, and Asst. Prof. Dr. Serkan TOPALOĞLU, my research co-advisor, for their guidance and encouragement throughout my graduate study at ITU.

I am also indebted to the many professional and friendly staff members in a defense industry company who have helped me in manufacture and measurement process. I would particularly like to thank CTO of that company for his encouragement and great support. Another person that I would like to give my appreciation for helping me in measurement process is Res. Asst. Osman CEYLAN at ITU RF Lab.

I would also like to thank Hüseyin Ulvi AYDOĞMUŞ, my friend, colleague and partner at RFtek Electronics, for his efficient and excellent technical support on the hardware and software design process.

Last but not the least; I would like to thank my family and friends who have supported me through the years. Without them, I could not overcome the obstacles and finish my degree. Thanks to my mother, father and sister, who have always encouraged me to do my best. They have always been there to share in my times of trial and times of joy. A special acknowledgment goes to my grandfather and grandmother. They encouraged me in school from the start. I am very grateful for all they have done for me.

January 2014

Özgür BOSTAN
(Electronics Engineer)

**TABLE OF CONTENTS**

**Page**

## ABBREVIATIONS

**ADC** : Analog Digital Converter
**AMS** : Austria Microsystems
**ASK** : Amplitude-Shift Keying
**B2B** : Business-to-Business
**CMOS** : Complementary Metal Oxide Semiconductor
**CW** : Continuous Wave
**CompTIA** : Computer Technology Industry Association
**CDMA** : Code-Division Multiple Access
**CRM** : Customer Relationship Management
**DAC** : Digital Analog Converter
**DC** : Direct Current
**DTC** : Digital Tunable Capacitor
**EAS** : Electronic Article Surveillance
**EM** : Electromagnetic
**EPC** : Electronic Product Code
**ERP** : Enterprise Resource Planning
**ETSI** : European Telecommunications Standards Institute
**FCC** : Federal Communications Commission
**FIFO** : First In, First Out
**FPGA** : Field-Programmable Gate Array
**FSK** : Frequency-Shift Keying
**FSTC** : Financial Services Technology Consortium
**HF** : High Frequency
**HTTP** : Hypertext Transfer Protocol
**IATA** : International Airlines Transport Association
**IC** : Integrated Circuit
**IEC** : International Electrotechnical Commission
**IEEE** : Institute of Electrical and Electronics Engineers
**IF** : Intermediate Frequency
**I/O** : Input/Output
**ISM** : Industrial Scientific and Medical
**ISO** : International Organization for Standardization
**ITF** : Interrogator Talks First
**LED** : Light-Emitting Diode
**LF** : Low Frequency
**LLRP** : Low-Level Reader Protocol
**LO** : Local Oscillator
**LPF** : Low Pass Filter
**MCU** : Microcontroller Unit
**MPHPT** : Ministry of Public Management, Home Affairs, Post and Tel.
**MTB** : Messaging/Transport Bindings
**OOK** : On-Off Keying

**PA** : Power Amplifier
**PCB** : Printed Circuit Board
**PIE** : Pulse-Interval Encoding
**PLC** : Programmable Logic Controller
**PSK** : Phase-Shift Keying
**RF** : Radio Frequency
**RFiD** : Radio Frequency Identification
**SAC** : Standardization Administration of China
**SCM** : **S**upply-Chain Management
**SPDT** : Single Pole Double Throw
**TCP** : Transmission Control Protocol
**TCXO** : Temperature Compensated Crystal
**UART** : Universal Asynchronous Receiver/Transmitter
**UHF** : Ultra High Frequency
**VCO** : Voltage Controlled Oscillator
**WMS** : Warehouse Management
**XTAL** : Crystal

## LIST OF TABLES

**Page**

## LIST OF FIGURES

**Page**

## LIST OF SYMBOLS

**fF** **:** Femtofarad
**m** **:** Meter
**MHz** **:** Megahertz
**Kbit/s** **:** Kilobit per second
**pF** **:** Picofarad
**Ω** **:** Ohm
**V** **:** Volt

**DESIGN AND IMPLEMENTATION OF A LOW-COST, COMPACT AND LONG RANGE MONOSTATIC UHF RFiD READER WITH READ POINT EXTENSION**

## SUMMARY


RFiD systems have an increasing popularity in various kinds of applications. Necessities are rising for the manufacture of new RFiD readers in industry especially at UHF band. Based on this concept, a new UHF RFiD reader design with extended read point capability has been presented within the scope of this thesis. Designed reader has attractive features required by some industrial RFiD applications.

Before the hardware design part of the study, first, the background of RFiD and its key standards have been introduced in the first two chapters. In the third chapter, the hardware design process has been covered in detail and simulation and measurement results have been presented.

The designed hardware is a low-cost, compact and long-range Gen2 compliant UHF RFiD reader with extended read point capability. The reader has up to 30 dBm (1 Watt) output RF power at two selectable antenna ports. The reader has an antenna tuning circuit, a novel feature, to reduce reflected RF power from antennas. This is achieved by tuning output impedance of the reader to the impedance of antenna. The reader can also tune the antenna impedance during operation in case the environment of the antenna changes. A power detector is used to control and limit the output power to regulatory requirements. While designing the hardware, several technical skills within a wide spectrum of disciplines were used like PCB design in high frequency, radio frequency, physics of RF, digital and analog design.

Extended read point capability is provided with another hardware design called RF multiplexer circuit. This product has been designed in order to increase the number of antenna output ports of UHF RFiD reader to reduce the system implementation cost in dense antenna applications.

This hardware design is also a part of another Research & Development project funded by the Ministry of Science, Industry and Technology of Turkey. As a part of this project and this thesis, the UHF RFiD reader has been designed as a domestic product to lower the cost of manufacture.

As a result of this project, all the objectives have been achieved and a prototype of UHF RFiD reader, which has a control unit and a graphical user interface, and an RF multiplexer have been manufactured to be used in any desired UHF RFiD application.

**OKUMA NOKTASI ARTIRILMIŞ,**
**DÜŞÜK MALİYETLİ, KOMPAKT VE UZUN MENZİLLİ MONOSTATİK**
**UHF RFiD OKUYUCU TASARIMI VE UYGULANMASI**

## ÖZET

RFiD sistemlerinin çeşitli uygulama alanlarında artan popülerliği neticesinde, özelikle UHF bandında çalışacak olan RFiD okuyucu üretimine dair ihtiyaçlar gittikçe artan bir eğilim göstermektedir. Bahsedilen ihtiyaçlar göz önüne alınarak, bu tez kapsamında yeni bir okuyucu tasarımı gerçekleştirilmiştir. Tasarlanan okuyucu, endüstriyel RFiD uygulamaları için gerekli görülen birçok ilgi çekici özelliği bünyesinde barındırmaktadır.

RFiD sistemleri, kısaca radyo frekanslı kimliklendirme diye tanımlanabilmektedir. Elektromanyetik dalgaları kullanarak (kablosuz iletişim), üzerlerine RFiD etiketleri iliştirilmiş olan nesne, hayvan ve insanlardan verilerin transfer edilmesini sağlarlar. Takip, gözlem, kontrol vb. amaçlı kullanılabilmektedir. Genel itibari ile barkod sistemi gibi otomatik tanımlama teknolojileri ailesinin bir üyesidir.

Tez kapsamındaki ilk iki bölümde, RFiD sisteminin detaylarına ve temel standartlarına dair bilgilere yer verilmiştir. Üçüncü bölümde, donanım sistem tasarımına ait süreçler detaylı bir şekilde ele alınmış ve simülasyon ile ölçüm sonuçlarına yer verilmiştir.

Tasarlanan okuyucu; okuma noktası artırılmış, düşük maliyetli, kompakt, uzun menzilli ve Gen2 uyumlu olacak şekilde UHF bandında geliştirilmiştir. Aynı zamanda, birden fazla okuyucunun aynı anda çalıştığı yoğun ortamlarda çalışabilme özelliğine sahiptir. Okuyucu, anten çıkış gücü 30-dBm olan iki adet anten çıkış portu barındırmaktadır. Ayrıca, yenilikçi bir özellik olarak, geri yansıyan RF gücünü azaltmak için anten uydurma devresi tasarlanmıştır. Bu işlem, okuyucunun çıkış empedansının antenin empedansına uydurulması ile gerçekleştirilmektedir. Bununla birlikte, okuyucu, işlem anında antenin empedansını olası çevresel faktörlere karşı kararlı bir yapıda tutabilme kabiliyetine de sahiptir. Bunların yanı sıra, bir güç algılayıcı devresi vasıtasıyla, okuyucu için var olan yasal koşulları sağlamak adına, çıkış gücünü sınırlandırma ve kontrol etme özellikleri de mevcuttur. Donanım tasarımı esnasında, yüksek frekansta PCB tasarım teknikleri, radyo frekansı ve fizik temelleri, dijital ve analog devre tasarım teknikleri gibi farklı disiplinlerden çeşitli teknik bilgiler ve kabiliyetler kullanılmıştır.

Artırılmış okuma noktası özelliği, tasarlanan bir başka donanım, RF çoklayıcı devresi, vasıtası ile sağlanmaktadır. Bu ürün sayesinde, UHF RFiD okuyucunun anten çıkışları artırılarak sistem kurulum maliyeti azaltılmaktadır. Bu cihazın amacı, çoklu anten ihtiyacı olan uygulamalarda okuyucu sayısını sabit tutarak, anten çıkış

sayısını artırmaktır. Bu sayede sistemin uygulanma maliyetinde avantaj sağlanmaktadır. Ürün dahilindeki anahtarlama entegrelerinin araya girme kayıplarının az olması ve entegrelerin kontrolünü sağlayan denetleyici yapısı, okuyucuların marka modelinden bağımsız tak-çalıştır sistem modeli ürüne ait katma değerli nitelikleridir.

Bu tez dahilinde tasarımı gerçekleştirilen UHF RFiD okuyucu, aynı zamanda Bilim, Sanayi ve Teknoloji Bakanlığı'nın sağlamış olduğu Ar-Ge proje destekleri kapsamında desteklenmiştir. Bu proje ve tez neticesinde, imalat masraflarını düşürmek adına okuyucu tasarımı ve üretimi yerli olarak gerçekleştirilmiş ve yurt içinde milli bir cihaz geliştirilmiştir.

Proje sonucunda, başlangıçta belirlenen tüm kıstaslar başarıyla sağlanmış ve birer adet RF çoklayıcı devresi ve UHF RFiD okuyucu devresi, kontrol ünitesi ve grafiksel arayüz yazılımı ile birlikte, istenen herhangi bir RFiD uygulamasında kullanılmak üzere prototip olarak üretilmiştir.

# 1. INTRODUCTION

## 1.1 Purpose of Thesis

The main objective of this study is to design a low cost UHF RFiD reader for passive UHF RFiD systems and applications that have an increasing popularity in various industries like manufacturing, supply chain management, inventory control, smart shelves, etc. Besides this, for modular and long range applications this UHF RFiD reader has been manufactured as a compact design and with a high output power feature.

Another hardware, which has the capability of increasing the number of antenna outputs of UHF RFiD reader, has also been designed. With the design of this RF multiplexer circuit, it is possible not only to use the UHF RFiD reader in the dense antenna applications but also to reduce the system implementation cost.

This hardware design is also a part of another Research & Development project funded by the Ministry of Science, Industry and Technology of Turkey. As a part of this project and this thesis, the UHF RFiD reader has been designed as a domestic product to lower the cost of manufacture.

As a purpose of thesis to design a UHF RFiD reader, several technical skills within a wide spectrum of disciplines were used like PCB design in high frequency, radio frequency, physics of RF, digital and analog design.

## 1.2 Literature Review

In this part of thesis, some previous academic researches have been reviewed. Most of the studies started after the year 2005 on the subject of UHF RFiD reader design. After reviewing the literature, it has been realized that, since 2008 the academic researches began to focus on this subject with increasing popularity of UHF RFiD systems in automatic identification sector.

In 2008, a UHF band (840 MHz – 925 MHz) RFiD reader transceiver design for the protocol of EPC Class-1 Gen-2 and ISO/IEC 18000-6C was presented. As an innovative solution, to suppress the leakage signal from transmitter to receiver, directional coupler and leakage cancellation circuit were introduced in the transceiver (Ye, et al., 2008). In the same year, a single chip UHF RFiD reader that integrates all building blocks, including an RF transceiver, IQ data converters and a digital baseband, was implemented in a 0.18 μm CMOS process. A high linearity RX front-end and a low phase noise synthesizer were proposed to handle the large self interferer, which is a key challenge in the reader RX design (Wang, et al., 2008). As a module based solution, a highly integrated UHF RFiD reader based on the RFiD transceiver chip (Intel R100 Chip) was designed also in 2008. It has the advantages of small size, high integration and reliability as well as low cost (Pang et al., 2008). Ying and Fu-hong (2008) introduced a system design for RFiD reader, which includes RF analog front end, the base band design and clock control. The base band contains the FPGA chip, which inseted NiosII soft core. This architecture is an advantage for implementing various kinds of RFiD standards by changing the soft of NiosII core in FPGA, and efficiently reduces the design and development time and cost. Again, in the same year, a UHF/HF multi-band RFiD reader was proposed and implemented into SiP with Package-on-Package technology. The proposed SiP RFiD reader was designed to support both for EPCgloabal Class1 Generation 2 protocol of UHF band and 13.56MHz RFiD protocols of ISO14443 A/B type and ISO15693 standards. The operating mode is controlled by embedded 32-bit RISC core, and the mode can be selected by users (Yi, et al., 2008).

Developments on UHF RFiD reader design proceeded in the year 2009. According to Park (2009) the spread of RFiD application need IC-based solution to reduce the size and cost of reader. As a result, a UHF band passive RFiD reader system on chip was presented. The chip includes processor core, flash memory, RFiD digital baseband, DAC/ADC, RF based on direct-conversion architecture, user interface block. In the same year, a new UHF RFiD reader which baseband module is based on ARM processor and FPGA chip was designed and implemented. The reader consists of three parts: baseband signal processing board, radio frequency transceiver and interface board. 90-degree phase-shift microstrip line was used in the radio frequency board to achieve the IQ conversion, saving the power divider component compared to the conventional homodyne scheme (Li et al., 2009). Another based on ARM work was presented in the year 2009. The hardware and software designs were described, and the hardware includes the RF sending circuit and the RF receiving circuit. Especially in the receiving system, it uses integrated circuit and the direct demodulation signal reception programme to achieve hardware optimized receiver circuit design. Using the sensitive amplification filter technology, the system can effectively detect and receive weak signal modulation and improve the recognition from the readers (Guo & Ting-lei, 2009). Other new improvements added some innovative features to the UHF RFiD readers in the same year, which are high linearity, mobility, high output power and canceller for reflected power. A Mobile UHF RFiD Reader made up of RF front end, phase lock loop, analog baseband and digital baseband was designed and implemented in a 0.18um CMOS process. An RX configuration without LNA was adopted in this design for high linearity purpose (Feng, et al., 2009). Another work presented a long-range RF identification (RFiD) reader that has proven to work at up to 5 m with 2W effective radiated transmit power at 868 MHz. For the validation, a phase-shift keying backscatter modulator was implemented, thus complementing the reader to form a complete passive RFiD system focused on backscattering communication (Mayordomo et al., 2009). As reflected power imposes severe linearity problems to the receiver in radio frequency identification (RFiD) readers, the design and realization of an ultra high frequency RFiD reader with a reflected power canceller circuit based on quadrature feedback was presented. Theory and measurements of the signal and noise in the receiver were presented as a function of incident carrier power (Pursula, Kiviranta, & Seppa, 2009).

There are some low power and low cost designs in the year 2010. A low power low cost fully integrated single chip UHF radio frequency identification (RFiD) reader for short distance handheld applications was presented. The IC integrates all building blocks, including an RF transceiver, a PLL frequency synthesizer, a digital baseband, and a MCU, in a 0.18 μm CMOS process. A high linearity RX front end and a low phase noise synthesizer were designed to handle the large self-interferer. A class-E power amplifier with high power efficiency was also integrated to fulfill the function of a UHF passive RFiD reader (Wnag et al., 2010). As UHF RFiD is becoming the main stream of passive RFiD applications, reader is a key component of an RFiD application system. Based on the ARM9 chip S3C2440, the UHF reader ASIC AS3990 and a battery charger 9-channel programmable DC-DC power management chip SMB122, a low power handheld UHF RFiD reader was designed and implemented (Li et al., 2010). Later in 2010, as an innovative solution a blocking reader and a reader based on mobile phone were designed. A low-cost privacy protection device that prevents unauthorized reading of RFiD tags was presented. This low-cost blocking reader was implemented based upon the Chipcon CC1101 chip and its basic read and privacy preserving performance was characterized. Using a monopole antenna, the Blocking Reader prevents unauthorized tag reads within 1m of it (Narayanaswamy et al., 2010). As to the features that of current mobile phone RF system operating frequency range about 900 – 2400 MHz UHF band, and the logic control core has a strong ability of controlling and data processing capability for consisting of dual kernel ARM9xx and DSP C55X. On this basis, by modifying the mobile phone operating system, set the mobile phone operating at max power 0.25w, an RFiD reader was realized to read the passive UHF tag supplied with the radiated energy from mobile phone (Zhang & Ma, 2010).

Internet of Things is a key component of next generation information technology. In addition, the key of Internet of Things is RFiD. Now Internet of Things brings new requirements to handheld UHF RFiD reader. In the year 2011 there was a work that proposed a complete solution of handheld UHF RFiD reader based on AS3991 and AM3517 for The Internet of Things. This reader uses the MPU chip of TI AM3517 as main controller, which provides excellent multimedia performance (Lei et al., 2011). Another work was a prototype UHF RFiD reader chip for mobile-phone applications. The reader architecture was designed for passive tags in compliance with the ISO/IEC 18000-6 Type C and the EPCglobal Class-1 Generation-2 protocols for UHF RFiD air interface. The reader also supports communication with active tags (Nakao, et al., 2011).

In 2012, a fully integrated single-chip RFiD reader consisting of zero-IF receiver, direct up-conversion transmitter, sigma-delta phase-locked loop synthesizer, and modulation/demodulation (MODEM) module was developed using a 0.18μm CMOS process. The RFiD reader operates from 860-960 MHz in steps of 100/200 kHz, supporting a multi-band global standard suitable for USA, Europe and Korea for both passive and active communications. It was specifically designed to achieve small size, low spur levels, low power consumption, and complete integration while meeting requirements for short-range applications (Lee, et al., 2012). In the same year, a complete solution of UHF RFiD reader system based on S3C2440 microprocessor and AS3992 UHF Reader chip was proposed. By designing the automatic gain control (AGC) circuit and the antenna impedance automatic matching circuit, the transmit power was increased up to 33 dBm and the receiver SNR was improved at the same time. The reader system was transplanted into the embedded Linux OS, which greatly facilitates the system development and maintenance (Song et al., 2012).

There are also some other related researches based on the UHF RFiD Reader ICs of AMS, one of the best companies that develops and manufactures high performance semiconductors, on the subject of UHF RFiD reader design. Devices were designed with AS3990, AS3991, and AS3992 in 2011, 2010, and 2012 respectively. Li and Wu (2011) designed a radio frequency circuit of reader. According to the ISO18000-6B/C air interface protocol and the FCC standard, considering the application of the tag test, the radio frequency module of RFiD reader and the filter of PLL circuit were designed in this study. Another study introduces a design solution of UHF reader based on AS3991. Using the internal PA and internal VCO, which integrated on the RF chip, the reader has the advantages of small size, high integration and low cost (Tang et al., 2010). Design and realization of UHF RFiD reader system based on ARM9 microprocessor as the controller and austriamicrosystems' UHF RFiD reader IC AS3992 for the RF front-end processing was introduced in 2012. With designing of the external power amplifier circuit, the external RF power detector circuit and the reader antenna impedance matching digital tuning circuit in the hardware system, the transmitter output power level was increased up to +33dBm, and the receiver S/N ratio was improved. The reader software system implemented high speed identification of ISO/IEC18000-6C tags and multi-tags inventory anti-collision algorithms, it has also solved the existing crosstalk problems between readers in the industrial site through the IP multicast technology based on embedded Linux operating system. The designed UHF RFiD reader system had been already applied effectively in the RFID management system of a certain power plant vehicle, and the operation result showed that it had successfully realized purposes to identify and process the information of vehicles' tag in the distance of 10 meters with stable performance (Xia et al., 2012).

### 1.3 Introduction to RFiD

Radio frequency identification is a generic term that is used to transfer data, for the purpose of automatically identifying and tracking tags attached to objects, humans or animals in the form of wireless non-contact use of radio frequency electromagnetic fields.

Basically, RFiD systems consist of small transponders, or tags, attached to physical objects. When in the field of electromagnetic wave provided by RFiD transceiver, or readers, tags respond with some identifying information associated with data records. Thus, RFiD systems are one of the sub-branchs of automatic identification systems like barcodes.

There are many kinds of applications that use RFiD systems in industry. These systems have different functionalities based on operating frequencies and regulatory restrictions. While RFiD has many benefits, it still faces several hurdles. Besides the typical implementation challenges faced in any information technology system and economic barriers, there are major concerns over security and privacy in RFiD systems. All these mentioned subjects will be covered in the following sub-sections.

#### 1.3.1 RFiD Origins

Although RFiD became popular only in recent years, the fact is that it has been used for a long time. The historical background goes back to the 19$^{th}$ century when the study of the electromagnetic waves were started; this was the keystone in the development of this technology.

The most important milestones since the 19$^{th}$ century are summarized as follows:

- 1864: James Clerk Maxwell asserted that electric and magnetic fields travel through space in the form of waves and published his theory about electromagnetism.
- 1887: Heinrich Rudolf Hertz carried out experiments with radio waves (transmission and reception) in his laboratory and verified Maxwell’s theory.

- 1897: Guglielmo Marconi succeeded in transmitting a message over a distance of 6 km without any cable across the Bristol Channel (Landt, 2005).

But it was not until the $20^{th}$ century that the development of the modern radio communication was a fact, thanks to the development of the Radar.

- 1904 is considered as the year when the Radar was invented. Christian Hülsmeyer, who detected a ship in the fog, realized one of the first experiments with the Radar.

- By the 1930s, the Radar was employed during the World War II by the allies as a form of intercepting the enemies' planes (Finkenzeller, 2003). Its function has not changed with the years since it is possible to determine the position and distance of an object by the reflection of radio waves.

The world had to wait several years till 1948 to see the true "birth" of the RFiD technology. In this year, Engineer Harry Stockman published the first work known about the study of RFiD, called "Communication by Means of Reflected Power" (Landt, 2005).

The study of RFiD did not stop, but it continued to evolve based on the other epoch inventions such as the transistor (1947), the integrated circuit (1958), the microprocessor (1971) and the development of communication networks.

- The 1960s were the prelude to the takeoff of RFiD because it was used in commercial activities. It was promoted by such companies as Sensormatic, Checkpoint and Knogo. They developed the Electronic Article Surveillance (EAS) to prevent shoplifting, which is still being used.

- In 1975, Alfred Koelle, Steven Depp, and Robert Freyman published their work "Short Range Radio Telemetry for Electronic Identification Using Modulated Backscatter". They carried out this study at Los Alamos Scientific Laboratory, and their findings were the beginning of short range passive tags (tens of meters).

- In 1980s, the RFiD technology was implanted in products after the invention of the personal computer. The computer enabled the harvesting and management of the data in RFiD systems.

- In 1990s, the use of RFiD was introduced in motorway tolls and the rail sector. In addition, the first standards started to emerge and RFiD became a part of everyday life (Landt, 2005).

In the $21^{st}$ century, the design of tags has advanced due to miniaturization (it is limited by the constraints of the antenna). A tag can now be manufactured using only two components: a single CMOS integrated circuit and an antenna. Nowadays the development of systems based on RFiD continues its global expansion.

## 1.4 Components of an RFiD System

After reviewing the history of RFiD, the system is investigated in detail based on the parts that compose it.

RFiD, as the term indicates, is an identification, or communication, system uses radio waves with the purpose of identifying objects (a physical thing, a person or an animal). In the following sections, the components of the system are presented.

### 1.4.1 Reader, Transceiver or Interrogator

The reader is the most important part of the system. Basically, it is a radio frequency transmitter and receiver controlled by a microprocessor. The reader, using an antenna or more, captures data from RFiD enabled tags attached to the objects, and then directs the data to a host computer for processing. Since the purpose of this thesis is to design a UHF RFiD reader, it will later be discussed in further detail in chapter four.

### 1.4.2 Transponder or Tag

The transponder consists of a coupling element (an integrated antenna) and at least one integrated circuit (IC). This IC contains the EPC (Electronic Product Code) and the logic necessary to understand the communication protocol between the tag and reader. As per the tag characteristics, they can be classified in three groups: Passive, Semi-Passive and Active. Each tag group is explained in more detail below.

Passive Tags:

Passive tags do not have their own source of power (without battery). The tag uses the power supplied by the reader to activate the IC tag. That is, the power is obtained through the tag antenna when it enters in the interrogation zone of the reader. In other words, the tag is powered by rectification of the received power. Moreover, the tag returns a modified signal (signal backscatter) to the reader (tag's information). Passive tags have a maximum reading distance of 5-10 meters depends on the output power of the reader, the antenna gain and the sensitivity of the tag (Dobkin, 2008). Figure 1.1 illustrates how passive tags are built.

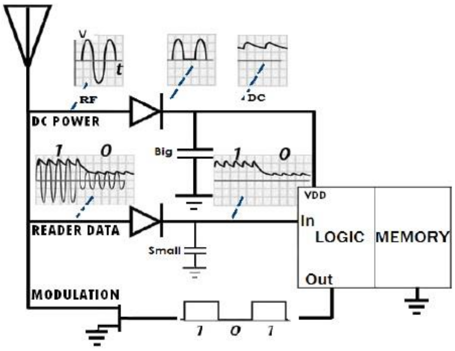


**Figure 1.1 :** Schematic of a simple passive RFiD tag (Dobkin, 2008).

As seen in Figure 1.1, a high-frequency signal (RF) is picked up when the antenna is influenced by an electromagnetic field of a nearby reader. This RF voltage that will be rectified by the diode and then smoothed by the capacitor to get a constant voltage is able to power the tag's memory and logic circuitry.

A similar rectification is carried out, at the same time, with a smaller capacitor, with the aim of demodulating the information from the reader. This is done with an envelope detector that allows varying the voltage in the timescale of the reader data. Finally, to transmit the information back, the tag has to change the electrical characteristic of the antenna to modify the signal received. In Figure 1.1, this has been represented with a FET although in a real tag but the process is a bit more complex (Dobkin, 2008).

Semi-Passive Tags:

Unlike passives tags, semi-passive tags have a battery for the power supply but still use the backscatter for the communication with the reader (see Figure 1.2). Semi-passive tags have a better operating range (from tens of meters to as much as 100 m) and give a better response to a valid interrogation than passive tags. Nevertheless, they are bigger due to the battery, cost more and are harder to maintain. Their applications are mainly oriented to automobile tolls and to tracking of high-value pieces, for example airplane parts (Dobkin, 2008).

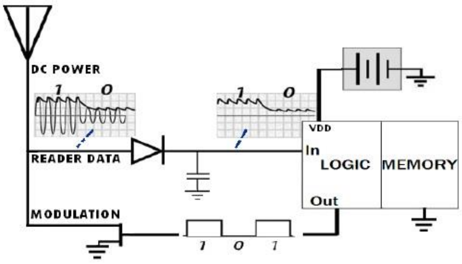


**Figure 1.2 :** Schematic of a simple semi-passive RFiD tag (Dobkin, 2008).

<u>Active Tags:</u>

Active tags, not only have batteries but also a transmitter, can be configured as a conventional bidirectional radio communication device. These tags can cover distances of more than 100 meters even kilometers.

Figure 1.3 illustrates the complexity of these tags. Active tags can use frequency division multiplexing or different frequency channels when they want to communicate in the presence of other tags. In addition, an active tag can communicate within a specific frequency band by the means of a Local Oscillator (LO) and a crystal reference (XTAL).

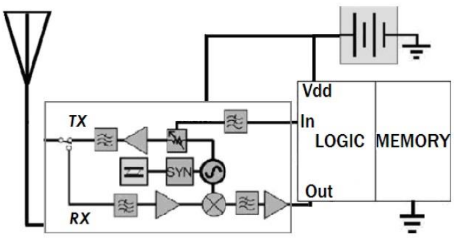


**Figure 1.3 :** Schematic of a simple active RFiD tag (Dobkin, 2008).

By the use of Code-Division Multiple Access (CDMA) it is possible to reuse the same frequency band by multiple tags. So the active RFiD tag can be successfully used in environments where the tag-reader path is significantly obstructed. One example is metal shipping containers that are stacked near each other without having a visual line from the reader to the tag (Dobkin, 2008).

### 1.4.3 Antenna

Both tags and readers have their own antennas because they are both radio devices. A tag antenna, which is only a few centimeters (or less) long, is attached to the integrated circuit (IC, or just chip) to absorb a signal and then transmit out a slightly modified signal. The reader antennas range in size but are generally about the size of a computer flat screen and are specially tuned to transmit and receive RF signals (Sweeney II, 2005).

Antennas are how readers communicate with the outside world. Reader antennas send radio signals into the air to activate a tag, listen for an echo (or backscatter) from the tag, read the data transmitted by a tag, and, in some cases, write data onto a tag. Antennas act as conduits between the tag and the transceiver and can function continuously or on demand (Sweeney II, 2005).

### 1.4.4 Middleware or Reader Interface Layer

An interface is necessary between the reader and the mainframe or host. Its function is to 'translate' the tags' signals into single identification data. In addition, it acts as a link between the RFiD hardware and the client's application.

The interface is often a software that runs on computers or servers and consists of middleware, which contains the logic of the RFiD application and a backend database system (e.g. Oracle, SQL Server, MySQL, etc.) for storing information about the tags (typically, the identification number and perhaps some item-specific information) (Thornton & Haines, 2006).

### 1.4.5 Middleware Circuits

A device or a circuit used for communication between main components of an RFiD system and enterprise applications. Middleware circuits enhance the compatibility of the RFiD systems within the environment they used, provide extended capabilities for applications like multiplexing antenna outputs, compensating RF losses etc.

## 1.5 RFiD Frequency Ranges

Low Frequency (LF) – [30 kHz - 300 kHz]:

The typical frequencies used in RFiD are 125 - 134.2 kHz and 140 - 148.5 kHz. LF is used in animal ID (standard ISO 14223/1) or in car applications. At this frequency, both the read range (less than 0.5 meter) and the data transfer rate (less than 1Kbit/s) are low.

High Frequency (HF) – [3 MHz - 30 MHz]:

Typically, the HF value used for RFiD is 13.56 MHz. Usually it is applied in smart tags (standard ISO 15693). The read range is higher than that of LF (up to 1.5 meter), but its data transfer rate is low (less than 25Kbit/s).

Ultra High Frequency (UHF) – [300 MHz - 3 GHz]:

The frequency bands used in RFiD are 433 MHz, 865 - 960 MHz and 2,5GHz. Generally, these frequencies are employed for animal tracking or in logistic applications. The read range is 0.5 - 10 meters for 865-960 MHz, but it can go up to the 100 meters to 433 MHz. Moreover, this frequency band has a data transfer rate larger than that of HF (30Kbit/s to 433 - 956 MHz).

Microwave – [2 GHz - 30 GHz]:

The typical frequencies used in RFiD are 2.45GHz and 5.8 GHz. It is used mainly in vehicle tolls because the read range is up to 10 meters. Moreover, it has a bigger data transfer rate than UHF (up to 100Kbit/s) (Finkenzeller, 2003).

## 1.6 Operating Principle of RFiD

As it is has been explained in the former sub-sections, both tags and readers have their own antennas. When the transmitting antenna of the reader emits a radio frequency field, the nearby tags are interrogated when they pass through the RF field. The distance of this emitted field depends on the frequency and the power output used by the system.

After the passive tag is activated, it sends (backscatters) the programmed information into its memory back. Next, the reader antenna receives and detects this response.

Then the backscatter signal is decoded with the purpose of sending the data to the host.

Sometimes, the reader can also broadcast special signals to a tag (e.g. to synchronize a tag with the reader for interrogating all or part of the tag's contents). Once the reader sends the data to the middleware software, the data are stored on the host. In other words, the middleware software handles the interface between the RFiD hardware operations and the flow of data (e.g. different electronic product codes in a database).

The Middleware software includes the following elements:

- Reader and device management: With a common interface, it is possible to configure, monitor or execute commands directly to reader.
- Data management: It is able to filter the captured information from readers (EPC or other data) and route it to its destination.
- Applications integration: It provides solutions for messaging, routing and connectivity. The RFiD data can be integrated into a supply-chain management (SCM), enterprise resource planning (ERP), warehouse management (WMS), or customer relationship management (CRM) systems.
- Partner integration: It provides collaborative solutions like business-to-business (B2B) (Sweeney II, 2005).

In brief, an RFiD network can be defined as a peer-to-peer architecture able to send data to a central host by the middleware. The middleware is responsible for linking the data between different networks.

### 1.7 Applications and Common Benefits of RFiD

Early commercial examples of RFiD applications include automatic tracking of train cars, shipping containers, and automobiles. Railroad cars were originally labeled with optical barcode labels for tracking. These labels began to deteriorate and be obscured by dirt, causing reads to fail. As a solution, railroad companies began to tag railcars with RFiD devices. By 1994, these devices were mandatory and nearly every railcar in the United States was tagged.

RFiD devices began to be used for automated toll collection in the late 1980s and early 1990s. Electronic toll systems have since been adopted around the world. Like railway and shipping applications, electronic toll systems may use sturdy, self-powered RFiD devices. Automobiles, railcars, and shipping containers are all high-value items, with ample physical space that can accommodate more expensive and bulky RFiD devices. These types of tags could offer much more functionality than simple identification. For example, shipping containers might have accelerometer sensors, tamper alarms, or satellite tracking integrated into an identification device.

As manufacturing costs dropped, RFiD systems began to be used for lower-value items in industries besides transport. An example is in animal identification of both pets and livestock. Glass-encapsulated RFiD devices have been implanted in millions of pets throughout the United States. These tags allow lost animals to be identified and returned to their rightful owners. These tags have a very short read range.

Livestock, particularly cattle, are often labeled with an RFiD device that is clamped or pierced through their ear, attached to a collar, or swallowed. Unlike implanted pet tags, these RFiD devices are rugged and able to be read from greater distances. Concerns over Bovine Spongiform Encephalopathy (mad cow) disease have motivated proposals for universal tracking of livestock with these types of RFiD systems. Like transport applications, animal tracking is still essentially a low-volume, high-value market that may justify relatively expensive RFiD systems.

Other widespread applications of RFiD systems include contactless payment, access control, or stored-value systems. Since 1997, ExxonMobil gasoline stations have offered a system called SpeedPass that allows customers to make purchases with an RFiD “fob”, typically a keychain-sized form factor (Speedpass). In 2005, American Express launched a credit card enhanced with RFiD that allows customers to make purchases without swiping a card.

RFiD proximity cards or “prox cards” are commonly used for building access control at many companies and universities throughout the world. Similar systems have been used for ski-lift access control at ski resorts around the world. Many subway and bus systems around the world, for example in Singapore, use stored-value RFiD proximity cards.

There are several applications that use RFiD as an anti-counterfeiting measure. In 2005, the Wynn Casino in Las Vegas first opened and deployed RFiD-integrated gaming tables and gambling tokens. These "chips-in-chips" are designed to frustrate counterfeiting, prevent theft, detect fraud, and to offer enhanced games or service. Besides stored-value tokens like casino chips or event tickets, there have also been proposals to tag currency (Juels & Pappu, 2003). In 2005, a controversial proposal to attach tags carrying biometric identification data to United States passports began to be implemented.

<u>Evolution and innovation in the uses of RFiD:</u>

One adaptation and improvement in the use of RFiD is to combine the tags with different sensors. In this way, the tag delivers the identification information repeatedly, and the current data is picked up by the sensor. An example of this application in the alimentation market would be an RFiD tag attached to a piece of meat that could report on the temperature readings ensuring that the meat is properly kept cool (Collins , 2004).

Other advancements in the RFiD world are:

- The self-scanning technology allows reducing the waiting time in a store checkout line because the items selected will be charged automatically from your bank account.
- Applications in the field of medicine.
- Energy harvesting.

Before investigating a more detailed discussion of various RFiD technologies, several of the present and envisioned future applications of RFiD are summarized below:

- Tracking and identification:
    - Large assets, e.g. railway cars and shipping containers
    - Livestock with rugged tags
    - Pets with implanted tags
    - Supply-chain management with EPC
    - Inventory control with EPC
    - Retail checkout with EPC

    - Recycling and waste disposal

- Payment and stored-value systems:
    - Electronic toll systems
    - Contact-less Credit Cards, e.g. American Express Blue card
    - Stored-valued systems, e.g. ExxonMobil Speedpass
    - Subway and bus passes
    - Casino tokens and concert tickets

- Access control:
    - Building access with proximity cards
    - Ski-lift passes
    - Concert tickets
    - Automobile ignition systems

- Anti-Counterfeiting:
    - Casino tokens, e.g. Wynn Casino Las Vegas
    - High-denomination currency notes,
    - Luxury goods, e.g. Prada

### 1.8 Challenges, Problems and Concerns of RFiD Systems

These applications also exposed some shortcomings of RFiD. For instance, some RFiD technologies do not operate well in proximity to liquids or metals. Each different technology has its own strengths and weaknesses, including variations in cost, size, power requirements, and environmental limits. There is no "one size fits all" RFiD technology. The term actually describes an entire array of technologies, which are each applicable to different types of applications.

While RFiD continues to lower the costs of tracking high-value items, an untapped and lucrative market lies in tracking cheap, everyday consumer goods. Companies like Proctor & Gamble, Coca-Cola, and Wal-Mart have hundreds of billions of products and components in their supply chains. Tracking and managing the flow of goods through these supply chains is a complex and expensive enterprise.

RFiD technology may streamline these supply-chain processes and save billions of dollars, savings that ultimately may be passed on to consumers. Shipping pallets or, ideally, individual items may be tracked and traced from manufacturers, through transport, wholesale, and retail into the hands of the consumer at a point-of-sale. Products could even be tracked post-consumer as they are recycled, refurbished, or disposed. What happens with respect to privacy while RFiD-tagged items are in the hands of a consumer has been an issue of major contention.

Supply chain management and inventory control applications of this scale require an extremely low-cost tag to be economically viable. In settings like animal identification, proximity cards, electronic toll systems, or stored-value systems, RFiD tags costing as much several US dollars could be justified. However, items in consumer supply-chain management and inventory control applications are much cheaper than in traditional settings. Ideally, RFiD tags in these applications should be as simple and cheap as the traditional, UPC optical bar code.

Data flooding:

Not every successful reading of a tag (observation) represents data useful for the purposes of the business. A large amount of data may be generated that is not useful for managing inventory or other applications. For example, a customer moving a product from one shelf to another, or a pallet load of articles that passes several readers while being moved in a warehouse, are events that do not produce data that is meaningful to an inventory control system (Glover & Bhatt, 2006).

Event filtering is required to reduce this data inflow to a meaningful depiction of moving goods passing a threshold. Various concepts have been designed, mainly offered as middleware performing the filtering from noisy and redundant raw data to significant processed data.

Global standardization:

The frequencies used for UHF RFiD in the USA are currently incompatible with those of Europe or Japan. Furthermore, no emerging standard has yet become as universal as the barcode (Radio Silence, 2007). To address international trade concerns, it is necessary to use a tag that is operational within all of the international frequency domains.

Security concerns:

Retailers such as Walmart, which already heavily use RFiD technology for inventory purposes, also use RFiD as an anti-employee-theft and anti-shoplifting technology. If a product with an active RFiD tag passes the exit-scanners at a Walmart outlet, not only does it set off an alarm, but it also tells security personnel exactly what product to look for in the shopper's cart (RFiD Technology Transforming Food Retailers Like Wal-Mart, 2010).

A primary RFiD security concern is the illicit tracking of RFiD tags. Tags, which are world-readable, pose a risk to both personal location privacy and corporate/military security. Such concerns have been raised with respect to the United States Department of Defense's adoption of RFiD tags for supply chain management. More generally, privacy organizations have expressed concerns in the context of ongoing efforts to embed electronic product code (EPC) RFiD tags in consumer products. This is mostly as result of the fact that RFiD tags can be read, and legitimate transactions with readers can be eavesdropped, from non-trivial distances. RFiD technology used in access control, payment and e-ID (e-passport) systems operate at a shorter range than EPC RFiD systems but are also vulnerable to skimming and eavesdropping, albeit at shorter distance (Hancke, 2011).

Security concerns exist in regard to privacy over the unauthorized reading of RFiD tags, as well as security concerns over server security. Unauthorized readers can use the RFiD information to track the package, and so the consumer or carrier, as well as identify the contents of a package (Ahson & Ilyas, 2012). Several prototype systems are being developed to combat unauthorized reading, including RFiD signal interruption (RFiD Privacy and Security), as well as the possibility of legislation, and 700 scientific papers have been published on this matter since 2002 (RFiD Security & Privacy Lounge). There are also concerns that the database structure of servers for the readers may be susceptible to infiltration, similar to denial-of-service attacks, after the EPCglobal Network ONS root servers were shown to be vulnerable (Tedjasaptura, 2007).

Exploitation:

Ars Technica reported in March 2006 an RFiD buffer overflow bug that could infect airport terminal RFiD databases for baggage and also passport databases to obtain confidential information on the passport holder (Anderson, 2006).

Passports:

In an effort to make passports more secure, several countries have implemented RFiD in passports (McCullagh & Broache, 2005). However, the encryption on UK chips was broken in under 48 hours (Sterling, 2006). Since that incident, further efforts have allowed researchers to clone passport data while the passport is being mailed to its owner. Where a criminal used to need to secretly open and then reseal the envelope, now it can be done without detection, adding some degree of insecurity to the passport system (How to clone a biometric passport while it's still in the bag. Mail exposes the postal vulnerability, 2007).

Temperature exposure:

Currently, RFiD tags are created by gluing an integrated circuit (IC) to an inlay. This poses a problem as vibration and high temperatures will loosen the connection. If the IC loses connection with the inlay, the RFiD tag will no longer transmit. A new design was filed for patent (King, 2010) where the IC is soldered to a circuit board and the circuit board is then soldered to the inlay. This process replaces the adhesive with solder, which is much more durable and temperature resistant.

There are also some controversies mentioned as follows.

Privacy:

The use of RFiD technology has engendered considerable controversy and even product boycotts by consumer privacy advocates. Consumer privacy experts Katherine Albrecht and Liz McIntyre are two prominent critics of the "spychip" technology. The two main privacy concerns regarding RFiD are:

- Since the owner of an item will not necessarily be aware of the presence of an RFiD tag and the tag can be read at a distance without the knowledge of the individual, it becomes possible to gather sensitive data about an individual without consent.

- If a tagged item is paid for by credit card or in conjunction with use of a loyalty card, then it would be possible to indirectly deduce the identity of the purchaser by reading the globally unique ID of that item (contained in the RFiD tag). This is only true if the person doing the watching also had access to the loyalty card data and the credit card data, and the person with the equipment knows where you are going to be.

Most concerns revolve around the fact that RFiD tags affixed to products remain functional even after the products have been purchased and taken home and thus can be used for surveillance and other purposes unrelated to their supply chain inventory functions (Hansen & Meissner, 2007).

The RFiD Network proved these fears to be unfounded in the premier episode of their syndicated cable TV series (RFiD Network Launches TV Series, 2012) by having RF engineers show how RFiD technology really works. RF engineers drove an RFiD-enabled van around a building and tried to take an inventory of items inside. They also explored if a passive RFiD tag can be tracked from satellite.

<u>Government control:</u>

With the rise of technology, some individuals have grown to fear the loss of rights due to RFiD human implantation.

By early 2007, Chris Paget of San Francisco, California, showed that RFiD information could be pulled from individuals by using only $250 worth of equipment. This supports the claim that with the information captured, it would be relatively simple to make counterfeit passports (Thomson, 2009).

According to ZDNet, critics believe that this technology will lead to tracking individuals every movement and will be an invasion of privacy. Some conceptualize a future where every movement is tracked by the government.

# 2. KEY STANDARDS AND TECHNOLOGIES

This section introduces the key standards and technologies utilized in this thesis. In the first sub-section, the current status of the RFiD standardization is investigated. Air and device interface standardization is also taken into consideration, moreover, EPCglobal standards, since they are utilized in the developed embedded system. In sub-sections two and three, the low-level interfaces concerning the reader development are examined in detail.

## 2.1 RFiD Standards

Multiple RFiD standardization projects were started during the late 1990's and the most successful were the ones done by the International Organization for Standardization and the Auto-ID Center, currently known as the Auto-ID Labs (McFarlane, 2006). The International Organization of Standardization established the ISO 18000 series of standards that essentially specify how the RFiD reader and the tags communicate. The first initiative was a development of a project called GTAG which resulted ISO/IEC 18000-6 (UHF technology) Type A protocol and later Type B protocol was developed and published (McFarlane, 2006). However, while Europe was leaning towards GTAG, separate development was done by Auto-ID Center in the US. Gradually GTAG was abandoned and most of the key developers became members of the Auto-ID Center. Later more significant development, involving collaboration between ISO experts, the Auto-ID Labs and eventually EPCglobal, resulted the third version of the ISO 18000-6 standard, Type C, which is also known as EPCglobal Class 1 Gen 2 protocol.

### 2.1.1 Current situation of RFiD Standardization

A number of organizations have set standards for RFiD, including the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), ASTM International, the DASH7 Alliance and EPCglobal.

There are also several specific industries that have set guidelines. These industries include the Financial Services Technology Consortium (FSTC) that has set a standard for tracking IT Assets with RFiD, the Computer Technology Industry Association (CompTIA) that has set a standard for certifying RFiD engineers, and the International Airlines Transport Association (IATA) that has set tagging guidelines for luggage in airports.

In principle, every country can set its own rules for frequency allocation for RFiD tags, and not all radio bands are available in all countries. These frequencies are known as the ISM bands (Industrial Scientific and Medical bands). The return signal of the tag may still cause interference for other radio users.

- Low frequency (LF: 125–134.2 kHz and 140–148.5 kHz) (LowFID) tags and high-frequency (HF: 13.56 MHz) (HighFID) tags can be used globally without a license.
- Ultra high frequency (UHF: 868–928 MHz) (Ultra-HighFID or UHFID) tags cannot be used globally as there is no single global standard.

In North America, UHF can be used unlicensed for 902–928 MHz (±13 MHz from the 915 MHz center frequency), but restrictions exist for transmission power. In Europe, RFiD and other low-power radio applications are regulated by ETSI recommendations EN 300 220 and EN 302 208, and ERO recommendation 70 03, allowing RFiD operation with somewhat complex band restrictions from 865 - 868 MHz. Readers are required to monitor a channel before transmitting ("Listen Before Talk"); this requirement has led to some restrictions on performance, the resolution of which is a subject of current research. The North American UHF standard is not accepted in France as it interferes with its military bands. On July 25, 2012, Japan changed its UHF band to 920 MHz, more closely matching the United States’ 915 MHz band.

For China, there is no regulation for the use of UHF. Each application for UHF in these countries needs a site license, which needs to be applied for at the local authorities and can be revoked. For Australia and New Zealand, 918–926 MHz is unlicensed, but restrictions exist for transmission power.

Standards that have been made regarding RFiD technology include:

- ISO 14223: Radio frequency identification of animals - Advanced transponders
- ISO/IEC 14443: This standard is a popular HF (13.56 MHz) standard for HighFIDs that is being used as the basis of RFiD-enabled passports under ICAO 9303. The Near Field Communication standard that lets mobile devices act as RFiD readers/transponders is also based on ISO/IEC 14443.
- ISO/IEC 15693: This is also a popular HF (13.56 MHz) standard for HighFIDs widely used for non-contact smart payment and credit cards.
- ISO/IEC 18000: Information technology - Radio frequency identification for item management:
    - Part 1: Reference architecture and definition of parameters to be standardized
    - Part 2: Parameters for air interface communications below 135 kHz
    - Part 3: Parameters for air interface communications at 13.56 MHz
    - Part 4: Parameters for air interface communications at 2.45 GHz
    - Part 6: Parameters for air interface communications at 860–960 MHz
    - Part 7: Parameters for active air interface communications at 433 MHz
- ISO/IEC 18092 Information technology, telecommunications and information exchange between systems, Near Field Communication - Interface and Protocol (NFCIP-1)
- ISO 18185: This is the industry standard for electronic seals or "e-seals" for tracking cargo containers using the 433 MHz and 2.4 GHz frequencies.
- ISO/IEC 21481 Information technology, telecommunications and information exchange between systems, Near Field Communication - Interface and Protocol-2 (NFCIP-2)

- ASTM D7434, Standard Test Method for Determining the Performance of Passive Radio Frequency Identification (RFiD) Transponders on Palletized or Unitized Loads
- ASTM D7435, Standard Test Method for Determining the Performance of Passive Radio Frequency Identification (RFiD) Transponders on Loaded Containers
- ASTM D7580, Standard Test Method for Rotary Stretch Wrapper Method for Determining the Readability of Passive RFiD Transponders on Homogenous Palletized or Unitized Loads

In order to ensure global interoperability of products, several organizations have set up additional standards for RFiD testing. These standards include conformance, performance and interoperability tests.

Groups concerned with standardization are:

- DASH7 Alliance, an international industry group formed in 2009 to promote standards and interoperability among extensions to ISO/IEC 18000-7 technologies (O'Connar, 2009).
- EPCglobal, this is the standardization framework that is most likely to undergo international standardisation according to ISO rules as with all sound standards in the world, unless residing with limited scope, as customs regulations, air-traffic regulations and others. Currently the big distributors and governmental customers are pushing EPC heavily as a standard well-accepted in their community, but not yet regarded as for salvation to the rest of the world.

Currently, the main air interface protocols used for identifying items are the ISO/EIC 18000 series of standards. Most of them were published in 2004, but since then the enhancements are made. The equivalent standard from EPCglobal for UHF range ISO/EIC 18000-6 Type C is EPCglobal Class 1 Gen 2. Nowadays, EPCglobal is leading the development and presents the standards to the ISO for additional review and further development. This kind of process is likely to be continuing since already new on-going standardization projects exist (McFarlane, 2006).

In addition, in the device interface and management standard development EPCglobal has led the way by the EPCglobal Low-level Reader Protocol (LLRP). The ISO did not start the development of the software system infrastructure, ISO/IEC 24791, until the work of LLRP was published. However, the scope of the device interface standards is currently generally still limited since both LLRP protocol and ISO/IEC 24791 series address only EPCglobal Class 1 Gen 2 and ISO/IEC 18000-6 air interface protocols respectively.

### 2.1.2 EPC Global

EPCglobal Inc. is an organization established to develop the industry-driven standards for the Electronic Product Code (EPC) used for RFiD devices (EPCglobal Inc.) and to achieve the adoption of the EPC Network Architecture. EPCglobal was formed in 2003 by two organizations, currently known as GS1 and GS1 US, to be open, worldwide, non-profit consortium of companies and organizations. Before the establishment of EPCglobal much of the work in standardizing EPC was done by Auto-ID Center of Massachusetts Institute of Technology, nowadays known as Auto-ID Lab. Later much of the work in terms of RFiD standardization done by Auto-ID Center was taken over by EPCglobal.

EPCglobal protocols and standards are developed in specified workgroups in five stages (McFarlane, 2006). Nowadays, the development process includes also coordination with the ISO. Standards specified and defined by EPCglobal are divided into multiple levels. The lowest two level standards are used in the identification. Second level standards are used to capture the information that is gathered. And, finally, the highest layers are used for information exchange.

In this thesis two of the EPCglobal standards, Reader Protocol (RP) and Tag Protocol UHF Class 1 Gen 2 standards are used in the reader interfaces.

## 2.2 EPCglobal Tag Protocol - UHF Class 1 Generation 2

EPCglobal Tag Protocol UHF Class 1 Generation 2 is an air-interface protocol that specifies the communication between EPC-compliant RFiD transponders and readers (EPCglobal Inc., 2008). The standard is developed by EPCglobal Inc. to serve as the second generation RFiD air interface protocol. UHF Class 1 Gen 2 specifications were developed to establish a standard for RFiD tags used in supply chain applications, e.g., tracking inventory (EPCglobal Inc.).

The Class 1 is the base class of RFiD tag classes. While both Class 1 and Class 2 devices are passive RFiD tags, the latter have more sophisticated functionalities, more memory and better access control. Class 3 is dedicated to semi-passive tags and Class 4 to active tags. The EPCglobal UHF Class 1 Gen 2 protocol defines both the physical and logical requirements for the Class 1 tag communication. The specifications can be divided into two different layers – Physical Layer and Tag identification layer. The first takes care of the low-level specifications, e.g. modulation, encoding and frequency, and the latter specifies operation procedure and commands.

The current ratified standard for Class 1 devices operates in the UHF range 860 – 960 MHz and uses backscattering in Tag-to-Reader communication. In addition, while tags being passive also the operating energy of the tags is received from the RF signal transmitted by the reader during both the Tag-to-Reader and Reader-to-Tag communication. Reader and tags are not required to talk simultaneously but the communication is half-duplex. The support for security is only minimal. Static passwords are used to access or kill RFiD tags.

Central to the standard is the electronic product code, Figure 2.1, which is the universal identifier that tags use in the EPC Gen 2 standard. The EPC consists of 96 bits that identify the encoding standard, company information, product type, and unique item identifier. Apart from the EPC number, many tags contain additional memory. The memory can store information such as expiration date, manufacturing date, manufacturing location, etc (Borisenko, 2012).

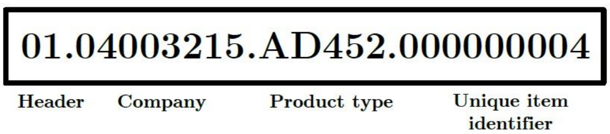


**Figure 2.1 :** Electronic product code (Borisenko, 2012).

### 2.2.1 Air-interface operation overview

In the EPC Gen 2 protocol, all communication is done in the ITF (Interrogator Talks First) mode. It means that the communication is always started by the reader using initializing commands. The communication between EPC-compliant reader and tags has to follow the pattern presented in Figure 2.2.

An EPC Gen 2 compliant reader uses three basic operation classes to manage the tag population in its RF field; select, inventory and access. Select commands are used to choose part of the tags for inventory and access. The commands can be used successively and the selection is based on user-specified criteria. The inventory commands are used to identify tags that are selected during the select phase. Inventory is done using multiple query commands in one of the four sessions. When the tags have been inventoried, the EPC code can be requested and tags can be moved to the access phase. Thereafter, access commands are used to write to or read from a tag. The tag that is accessed must be always identified prior to writing or reading operations. As in the inventory phase, there are also multiple commands used in the access phase.

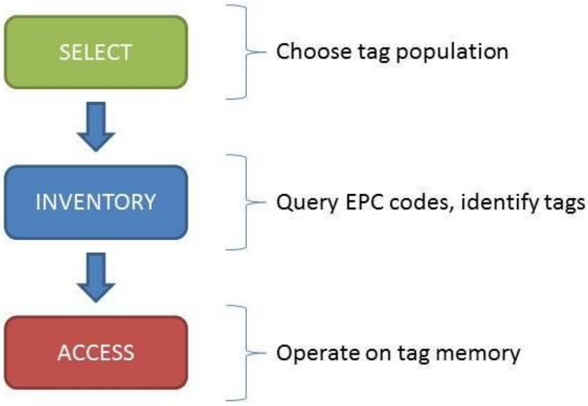


**Figure 2.2 :** Reader operation process in the tag interaction.

Reader-to-Tag communications uses one of the Amplitude-Shift Keying Modulation techniques available with PIE (Pulse-interval Encoding). A fixed modulation format and data rate is used during a single inventory round. The reader sets the format and data rate at the beginning of every query cycle in select commands.

For the Tag-to-Reader communication, tags select the modulation format, the data encoding and the data rate according to the commands sent by the reader during the select and the inventory phases of the communication process. Tag backscatter uses ASK and/or PSK modulation and data is encoded as either FM0 baseband or Miller modulation of a subcarrier at the data rate. The link frequency is chosen from multiple alternatives ranging from 40 kHz to 640 kHz. The transmission order in both Tag-to-Reader and Reader-to-Tag communication is big endian, which means that the most-significant word is transmitted first and, within each word, the most-significant bit is transmitted first.

If errors occur when the tag is executing access commands, it backscatters an error code. However, error code is not transmitted if the command is unknown or the tag communication process is not yet in the access phase.

### 2.2.2 State transitions of an EPC – compliant tag

Tags operating according to the EPCglobal Tag Protocol UHF Class 1 Gen 2 protocol follow the state diagram illustrated in Figure 2.3, a simplified version, following the phases of the tag communication presented in Figure 2.2. The states and state transitions are explained below. To move an EPCcompliant tag from a state to another, the reader uses mandatory air interface commands (EPCglobal Inc., 2008). State machine and operating phases need to be considered when designing and implementing the air interface operation of the EPC-compliant reader.

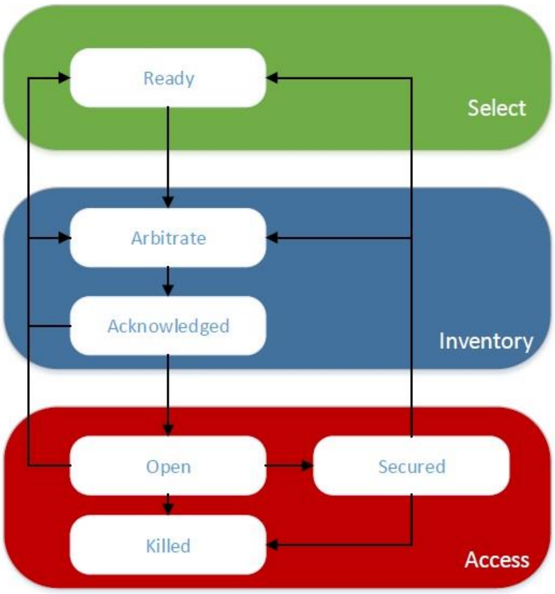


**Figure 2.3 :** Simplified version of the tag state machine.

The Ready state is an initial waiting state of the EPC-compliant tags. Tags that are neither killed nor participating in the inventory action stay in the Ready state. Every time a tag that is not killed loses its power and regains it afterwards it, returns to the Ready state.

The Arbitrate and Acknowledged states are used for inventory. From the Ready state tags move to the next state, Arbitrate, when they receive a *Query* command matching their inventory flags from the reader. The state is a waiting state for the tags that are participating in the inventory action but whose slot counters hold non-zero values. Tags decrease their slot counter value when a *QueryRep* command is received from the reader. When the slot counter value reaches zero the tag backscatters its RN16 random number to the reader. If the tag receives a valid acknowledgement, it transitions to the Acknowledged state and sends its EPC code.

The Open, Secured and Killed states are used when the tags are accessed. A tag can be moved to the Open state from the Acknowledged state by a *Req_RN* command. A new RN16 number, a handle, is sent to the reader. When in the Open state any access commands, except *Lock*, can be used. If the password of the tag is not set, the tag moves directly to the Secured state instead of the Open state when a *Req_RN* command is received. Tags that have a non-zero password can be moved to the Secured state by a valid *Access* command. When in the Secured state any tag commands can be executed. A final state, Killed, is a state where the tag enters when it receives a valid *Kill* command and a kill password while staying in the Open or Secured state. A *Kill* command permanently disables the tag. After a *Kill* command is successfully completed and the tag is powered up again later, it moves directly to the Killed state.

State transitions of an EPC Gen 2 RFiD tag shown in Figure 2.3 are as follows:

- *Query* command is received and the tag's inventory variables match those received with *Query* command.
- Acknowledgement message that contains a valid RN16 number is received from the reader.
- *Req_RN* command including a valid RN16 number sent to the reader during the inventory is received.
- *Access* command that contains a valid access password is received from the reader. If the tag has a zero password, it moves automatically from Open to Secured state.

- *Kill* command including a valid non-zero kill password and a valid handle is received from the reader.
- A command that is neither a query command nor an access command is received.
- *Select* or one of the query commands is received from the reader.
- A command that is neither a query command nor an access command is received.
- *Select* or one of the query commands is received from the reader.
- *Kill* command including a valid non-zero kill password and a valid handle is received from the reader.

### 2.2.3 Protocol conformance

To claim conformance with EPCglobal Tag Protocol UHF Gen 2 Class 1 the devices have to implement all mandatory air interface commands and comply with all the mandatory clauses presented in the specifications of the EPCglobal Class 1 Gen 2 protocol. Moreover, the device has to comply also with the clauses presented in a separate conformance document that is available to EPC subscribers only at the EPCglobal website (EPCglobal Inc.). Finally, all the regarding radio regulations need to be met.

## 2.3 EPCglobal Reader Protocol

The EPCglobal Reader Protocol standard defines how the interaction between the EPC-compliant reader and the reader management unit is performed (EPCglobal, 2006). The aim of the Reader Protocol standard is to hide all details of the air interface and the interaction between the reader and RFiD tags. Reader Protocol does not define the protocol used in the air-interface and, moreover, the host needs to know nothing about it.

The protocol consists of multiple layers to which all necessary operations are divided. The communication between the reader and the host is done using two channels: a Notification Channel and a Command Channel. The first is used to carry messages issued only by the reader and the latter, on contrary, follows request/response pattern in which the host issues all the requests and the reader responses.

### 2.3.1 Reader protocol layers

The Reader Protocol standard specifies three distinct layers: Reader Layer, Messaging Layer and Transport Layer as illustrated in Figure 2.4. Furthermore, the lowest two of the layers define an entity called Messaging/Transport Binding. The EPCglobal Reader Protocol standard defines multiple alternative Messaging/Transport Binding implementations each representing a different transportation medium and messaging protocol combination, e.g. TCP or serial line.

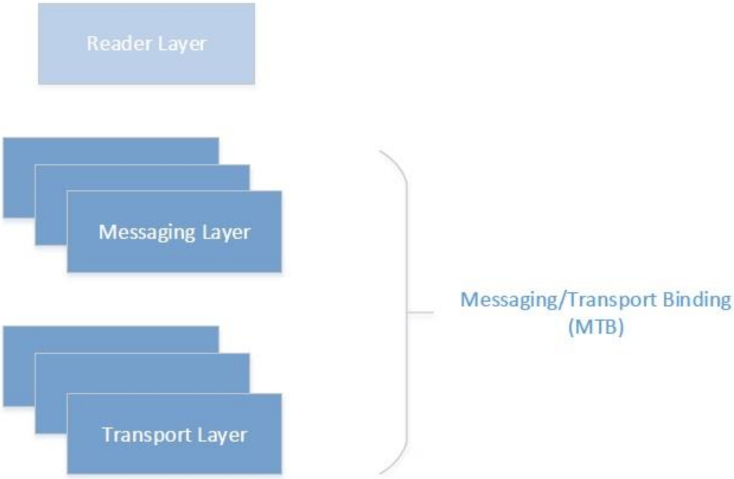


**Figure 2.4 :** EPCglobal reader protocol layer structure.

The highest layer, Reader Layer, is the core of the Reader Protocol. It defines the content of the messages that are sent between the reader and the host. It dictates what operations are implemented and what those operations actually do. Although different Reader Protocol implementations may have very different Messaging/Transport Binding layers, all Reader Protocol implementations have similar Reader Layer operations. Some implementations may have more commands and, consequently, more versatile operation options, but the basis of the Reader Layer is the same.

Messaging/Transport Bindings (MTB) performs the transporting of the encoded EPCglobal Reader Protocol commands between the reader and the reader management unit. There are three different Message/Transport Bindings specified in the EPCglobal Reader Protocol standard; serial line, TCP and HTTP. All bindings can be divided into two layers, which have different, specified tasks.

The higher layer of the Messaging/Transport Binding defines the syntax and format that is used to form the Reader Protocol commands. Two message formats can be used; Text and XML. In addition, the Messaging layer defines the message payload transformation and the framing of the messages. The lower of the Messaging/Transport Binding layers instead defines the networking facilities used in the transportation. In addition, the acknowledgement protocol is defined by the Reader Protocol Transport layer.

Finally, also the handshake procedure used to establish connections is defined by the Messaging/Transport Binding. The handshake is always done in text-based format and it is carried out immediately upon the establishment of a connection. In the EPCglobal Reader Protocol, a similar handshake is used with all different Messaging/Transport Binding options.

### 2.3.2 Reader protocol object layer

In addition to the protocol layer structure, EPCglobal Reader Protocol introduces also an internal object model for EPC-compliant reader. Object model is illustrated in Figure 2.5. Model is similar to the EPCglobal Software Action Group specification Reader Management, although some objects and properties are not relevant in Reader Protocol and, therefore, shown in gray in Figure 2.5. The proposed object model is not mandatory in EPCglobal Reader Protocol, but just illustrates internal relationships between multiple sources, triggers and other components.

The *ReaderDevice* is the base container for most other objects and, also, for most attributes including the management of the network interface. Consequently, it can be considered as the main object of the model. *Source* object, instead, in association with *ReadPoint* object represents a single source for communication input from the transponders. Whereas *ReaderDevice* and *Source* together form the basis for the tag communication, channel objects *CommandChannel* and *NotificationChannel* are used for host communication.

Since the proposed object model is not mandatory, different implementations of Reader Protocol may include different objects of the model. A single reader may contain zero or more read sources and, consequently, a various number of *Source* and

*ReadPoint* objects. Similarly, *ReaderDevice* must include one pre-configured CommandChannel, but the number of NotificationChannels and regarding *Triggers* may vary. Detailed description of the EPCglobal Reader Protocol object model can be found from the protocol specifications (EPCglobal, 2006).

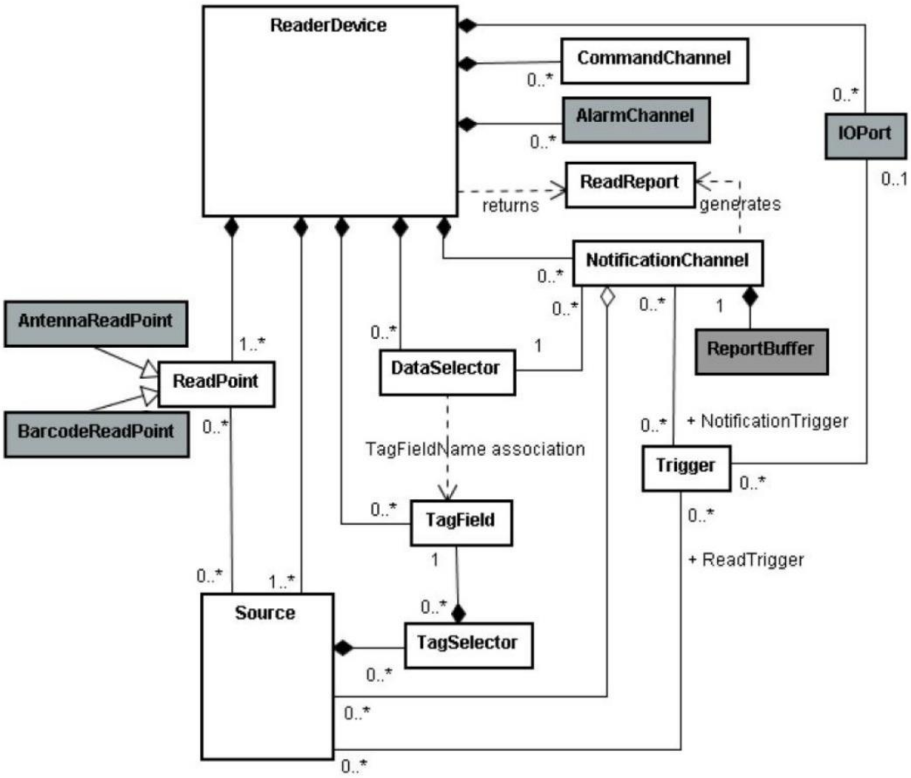


**Figure 2.5 :** Object model of the EPCglobal reader protocol (EPCglobal, 2006).

### 2.3.3 Protocol conformance

Software or devices that claim conformance to the EPCglobal Reader Protocol standard have to implement all mandatory commands and comply with all mandatory clauses presented in the Reader Protocol standard. Also, requirements presented in the Reader Protocol Conformance Requirements document that is available to EPC subscribers only at the EPCglobal website (EPCglobal Inc.) have to be complied with.

### 2.3.4 LLRP

The LLRP (Low-Level Reader Protocol) standard (EPCglobal, 2010) is a specification for the interface between RFiD readers and clients, usually in the form of PCs. Many RFiD vendors adopted this standard for their reader-client interface (Vries & Dietrich, 2007). LLRP supports the EPC Gen 2 standard, as well as allowing the addition of other standards. The protocol allows setting the reader configuration as well as air-protocol configurations, such as: modulation, encoding, frequency range, Q-value, output power level, and sensitivity. These settings can be modified to boost performance or to mitigate interference of RFiD systems.

In the LLRP, the data units are called messages and all communication between the reader and the client is performed using these messages. Client-to-Reader messages include getting and setting configuration of the reader, capability discovery, managing inventory, and access operations. Messages from Reader-to-Client include status reports, RF survey reports, inventory results, and access results. LLRP parameters are used to communicate specific settings of LLRP operation in the messages. A parameter contains one or more fields, and in some cases may nest one or more other parameters.

## 3. HARDWARE DESIGN

In this chapter of study, the hardware designs of the UHF RFiD reader and RF multiplexer are described. The designed hardware is a low-cost, compact and long-range Gen2 compliant UHF RFiD reader with dense reader mode capability (feature of reader IC). The reader has up to 30 dBm (1 Watt) output RF power at two selectable antenna ports. The reader has an antenna tuning circuit, a novel feature, to reduce reflected RF power from antennas. This is achieved by tuning output impedance of the reader to the impedance of antenna. The reader can also tune the antenna impedance during operation in case the environment of the antenna changes. A power detector is used to control and limit the output power to regulatory requirements. The default operating voltage of the reader is 6 Volt. The MCU used in circuit is a widely used 8051 controller for host communication via USB or UART. The designed UHF RFiD reader is shown in Figure 3.1. There is another circuit designed for the antenna outputs of UHF RFiD reader for multiplication. Actually, this is an independent device that could be used for any RF switching application. The main purpose of this product is to increase the number of antenna output ports of UHF RFiD reader for dense antenna applications. In the following sections, design of mentioned hardware will be investigated in detail.

### 3.1 UHF RFiD Reader Design

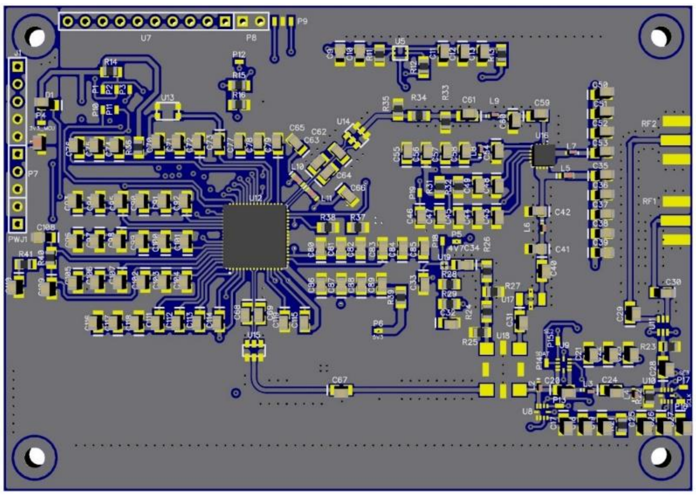

**Figure 3.1 :** UHF RFiD Reader.

### 3.1.1 Block diagram of circuit

In the following figure (Figure 3.2), the block diagram of the whole system is shown.

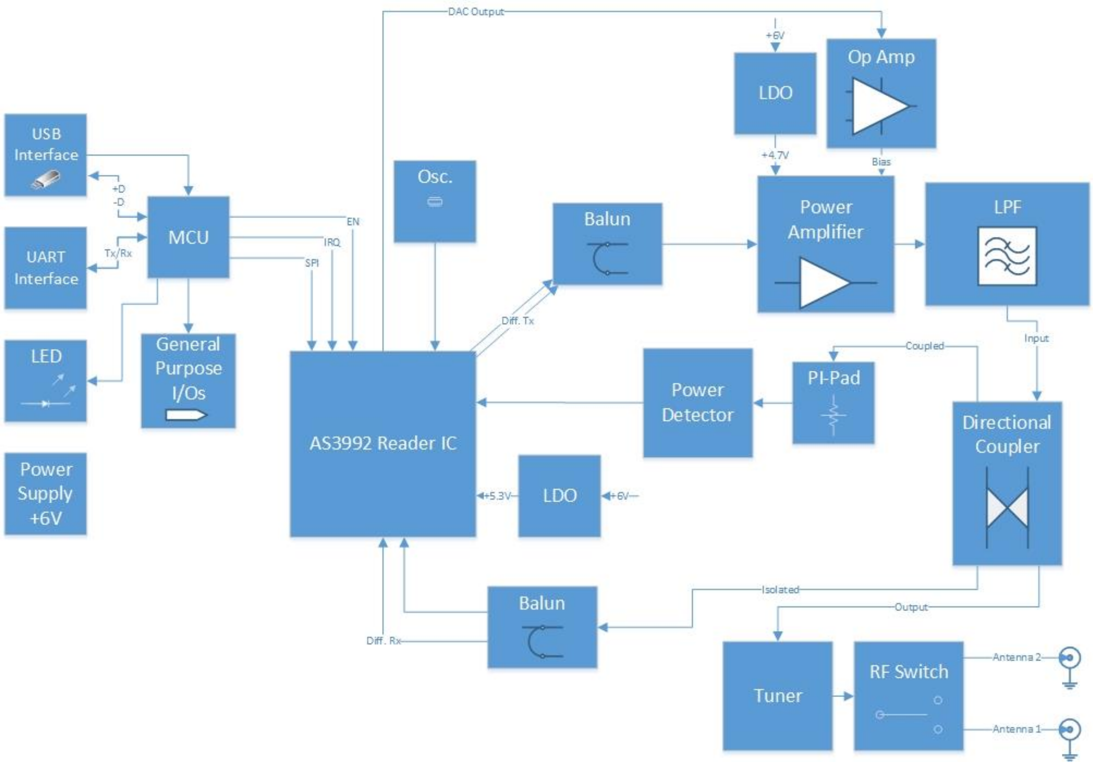


**Figure 3.2 :** Block diagram of the hardware section.

### 3.1.2 Building blocks of reader core module

In this section, all the building blocks (components) on the PCB are described in detail. For more information that is technical please refer to the links of dedicated datasheets of the components given in Appendix A.

#### 3.1.2.1 AMS 3992 – reader IC

The Gen2 compliant UHF RFiD reader IC is the main device on the reader that handles all the Gen2 protocol related tasks, furthermore it acts as RF front end for transmission and reception covering modulation and decoding. The location of the AS3992 reader IC is shown in Figure 3.3.

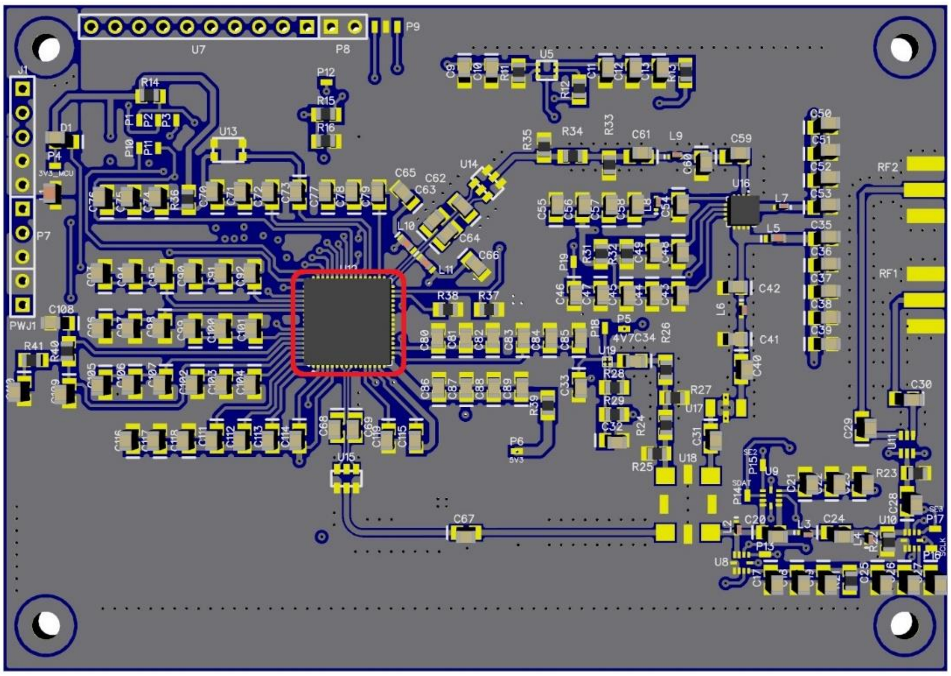


**Figure 3.3 :** AS3992 location.

The supply voltage of the AS3992 reader IC is 5.3V regulated from the external power supply (6V) via the LDO IC AS1364.

AS3992 reader IC is configured to communicate with the microcontroller via the SPI interface (SPI mode 1), which is selected by setting pin IO0 to “low” and pin IO1 to “high” before AS3992 is enabled. When hardware coders and decoders are used for transmission, data is transferred via 24 bytes FIFO register (AMS, 2010).

For RF transmission the 0-dBm differential ports are used, which amplified by a PA SKY65111 up to 30-dBm. On the other hand, for RF reception the differential mixer inputs are used.

In order to provide frequency stability and accuracy needed to comply with Gen2 operation, a 20 MHz TCXO clock source is used.

The AS3992 offers improved receive sensitivity to -86 dB, programmable Rx Dense Reader Mode (DRM) filters on chip and pre-distortion. Fully scalable, the AS3992 is ideal for long range and higher power applications (AMS, 2010).

The receiver system allows AM and PM demodulation. The receiver also comprises automatic gain control option (patent pending), selectable gain and signal bandwidth to cover a range of input link frequency and bit rate options. The signal strength of AM and PM modulation is measured and can be accessed in RSSI register. The receiver output is selectable between digitized sub-carrier signal and any of integrated sub-carrier decoders. Selected decoders deliver bit stream and data clock as outputs (AMS, 2010).

The receiver system also comprises framing system. This system performs the CRC check and organizes the data in bytes. Framed data is accessible to the host system through a 24-byte FIFO register (AMS, 2010).

To support external MCU and other circuitry a 3.3V regulated supply and clock outputs are available. The regulated supply has 20 mA current capability (AMS, 2010).

The AS3992 is available in a 64-pin QFN (9mm x 9mm), ensuring the smallest possible footprint (AMS, 2010).

The RF block diagram of AS3992 is shown in Figure 3.4. The elements included in the chip are a complete UHF Gen2 standard transmit, receive, demodulation and baseband functions.

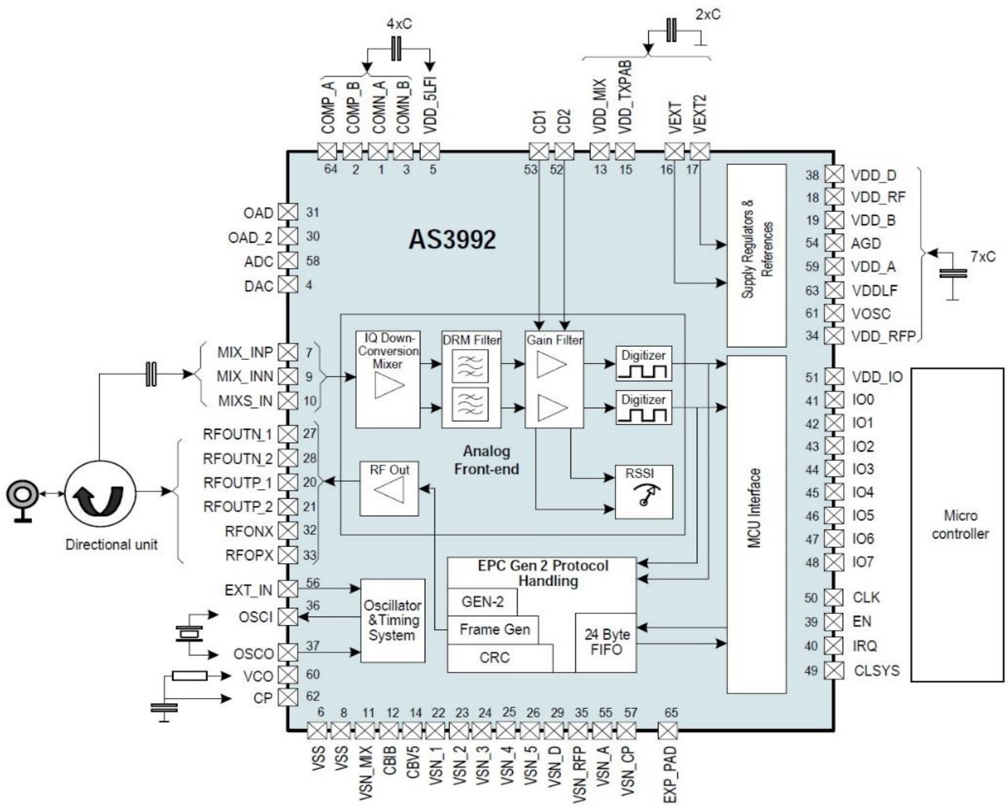


**Figure 3.4 :** RF block diagram of AS3992 (AMS, 2010).

The RFID reader IC AS3992 comprises complete analog and digital functionality for reader operation including transmitter and receiver section with complete EPC Gen2 or ISO18000-6C digital protocol support. Transmitting and receiving is possible in the Normal Mode and Direct Mode. The integrated modulator uses ASK and PR-ASK modulation with adjustable ASK modulation index. To integrate as many components as possible, the device also comprises an on-board PLL section with integrated VCO, supply section, A/D converter section, and host interface section (AMS, 2010). The reader configuration is achieved through setting the 48 control registers allowing fine-tuning of different reader parameters.

As shown in Figure 3.4, the RF signal received via antenna into the directional coupler is divided into two balanced signals by the balun, then transmitted into AS3992. Two signals are divided into I and Q branches by the mixers then delivered into the protocol processing unit after amplification, filtering, RSSI sampling and analog-digital conversion. In the protocol processing unit, the chip could select the protocol flexibility according to the control signals.

In Normal Mode, the baseband data is transferred to the 24 byte FIFO and all signal processing (protocol encoding, adding preamble or frame-sync, CRC, signal shaping, and modulation) is done internally. The data is then coded to the modulation pulse level and sent to the modulator and power amplifier, finally exported to RFOPX and RFONX pin to transmit. Direct Mode is used in case one wants to use only analog functions, bypassing all the protocol handling support of the reader device.

This reader IC was selected as it integrates 90% of the needed components for the hardware design of an RFiD reader. In other words, it allows simple design, low cost and compact size. It has great support for software development kit and a great datasheet that helps while system design.

#### 3.1.2.2 MCU – controller unit

For the UHF RFiD Reader an 8-bit microcontroller is used, which interacts with the AS3992 reader IC via the SPI interface and with the host computer via the USB interface. The location of the MCU is shown in Figure 3.5.

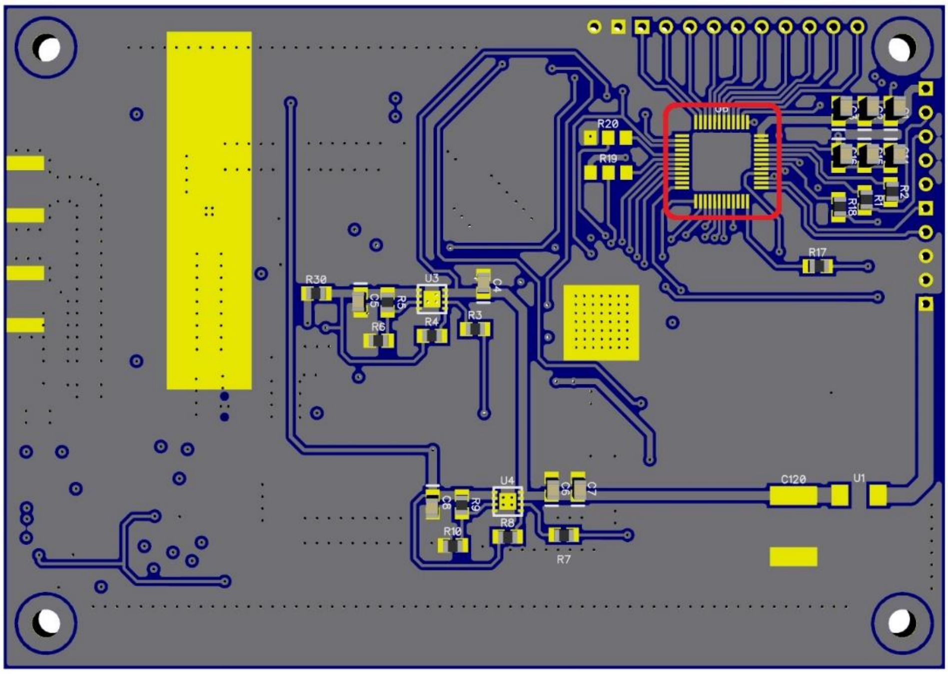

**Figure 3.5 :** MCU location.

The MCU is supplied with 5V via the USB interface. By doing this, as the power supply of MCU is independent of the AS3992 reader IC, it is possible to update firmware and program the boot-loader without connecting the external power supply to the reader.

The MCU provides 3.3V, generated with the internal voltage regulator, to the pin VDD_IO of AS3992 to have a common interface voltage.

### 3.1.2.3 Balun – impedance conversion

To convert the 100 ohm differential signal of the AS3992 reader IC to a single ended signal with 50 ohm for transmitting the power, a 2:1 balun is used. On the receiving side there is another balun used for converting 50 ohm to 100 ohm impedance (single ended to differential). While the RF signals propagate through the baluns (not only eligible for baluns but also for all RF components), a power loss occurs called insertion loss. Maximum insertion loss of these baluns is 1 dB for UHF band. The locations of the baluns are shown in Figure 3.6.

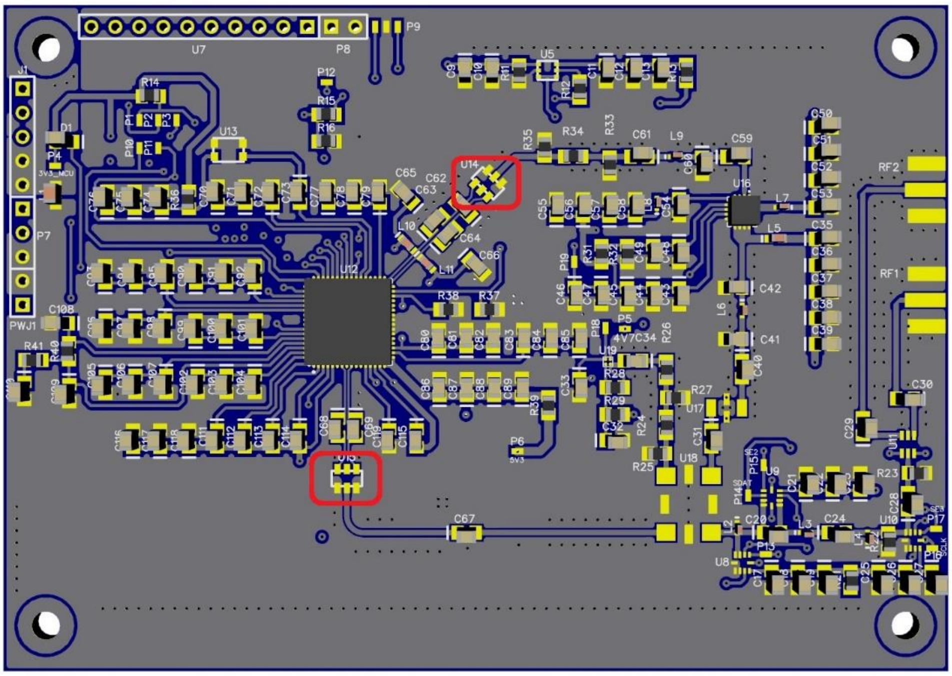

**Figure 3.6 :** Balun locations.

#### 3.1.2.4 PA – external amplification

An external 3-stage power amplifier is used to increase the transmission signal output from AS3992 up to 30 dBm.

The PA is supplied with 4.7V via a voltage regulator AS1364. The power amplifier has two bias voltage inputs. The bias for the first two stages ($V_{APC1}$) is held at a fixed voltage of 2.6V via a voltage divider circuit. The second bias voltage ($V_{APC2}$) is controlled from the DAC output of AS3992 that is buffered with an OP-Amp AS1710. The location of the PA is shown in Figure 3.7.

A simulation circuit was designed in AWR Microwave Office and based on the power amplifier parameters, provided by the manufacturer, output power of the PA was measured as a simulation result. At a given frequency and input power, 866 MHz and zero-dBm respectively, it is indicated in Figure 3.8 that the output power is nearly 36 dBm without adjusting the control voltage for the third stage. Another view of that chart is also presented in Figure 3.9. The values are nearly the same with the values that are in the datasheet of the product.

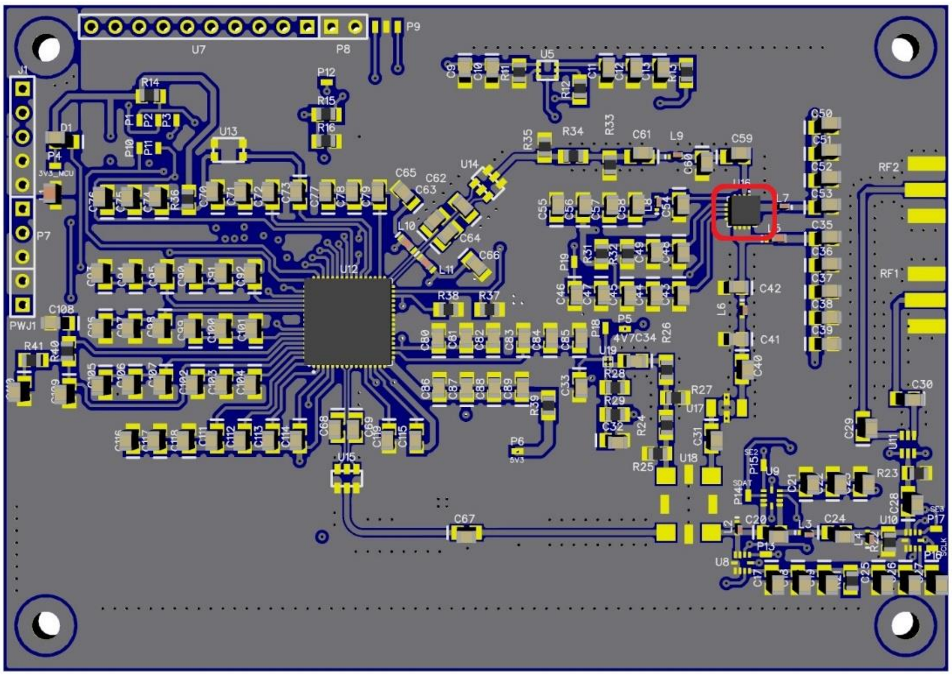

**Figure 3.7 :** Power Amplifier location.

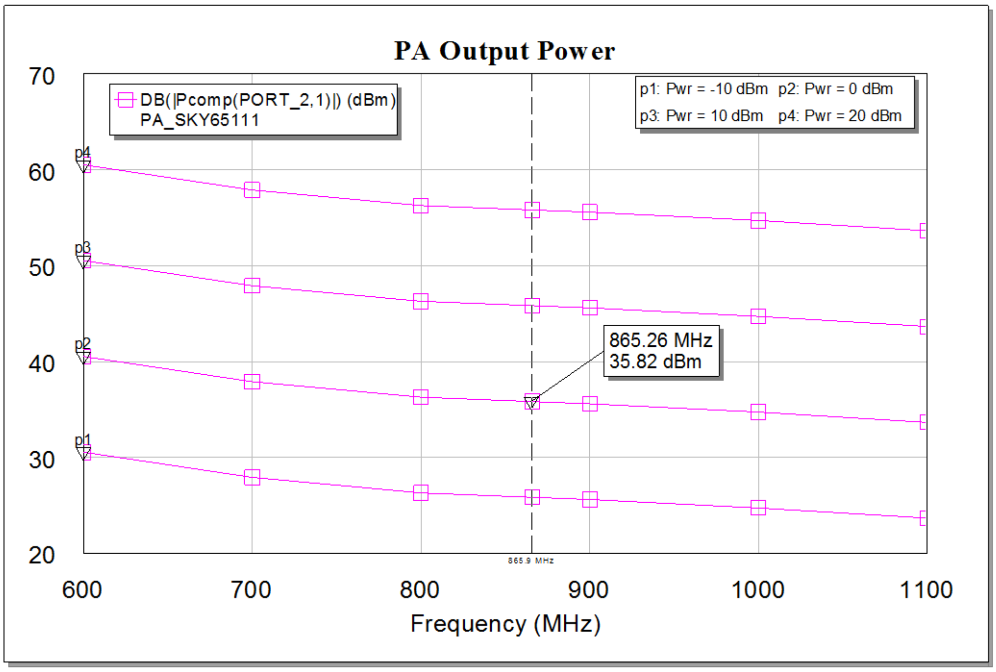


**Figure 3.8 :** Simulated output power of PA.

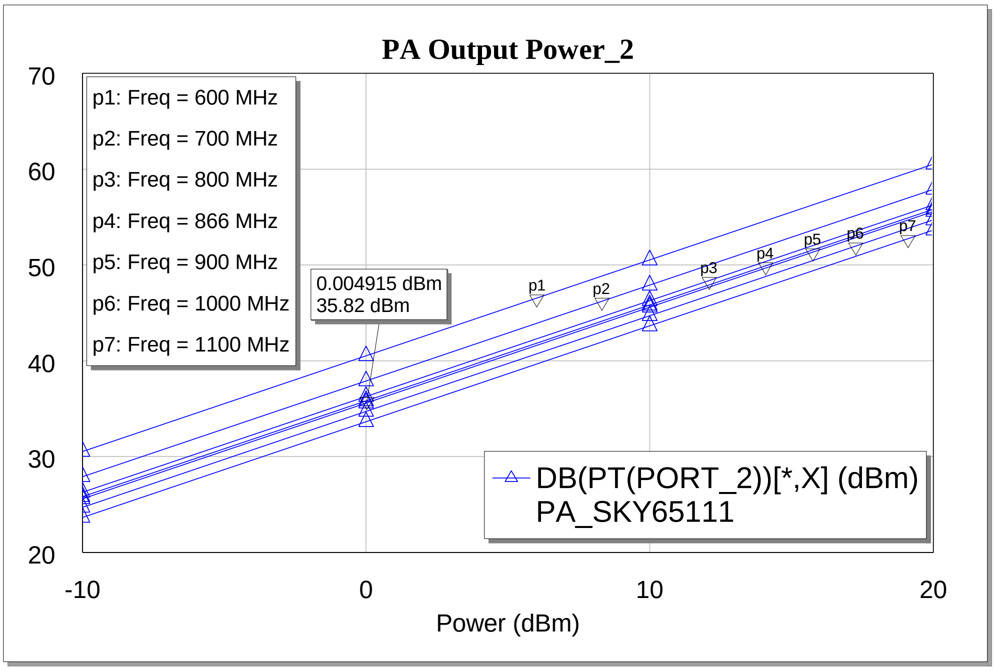


**Figure 3.9 :** Simulated output power of PA-2

### 3.1.2.5 LPF – filtering

A low pass filter is used for attenuating the higher order harmonics of amplified transmit signal. The device has a typical insertion loss of 0.7 dB at UHF band and provide typically 30 dB of attenuation. The location of the LPF is shown in Figure 3.10.

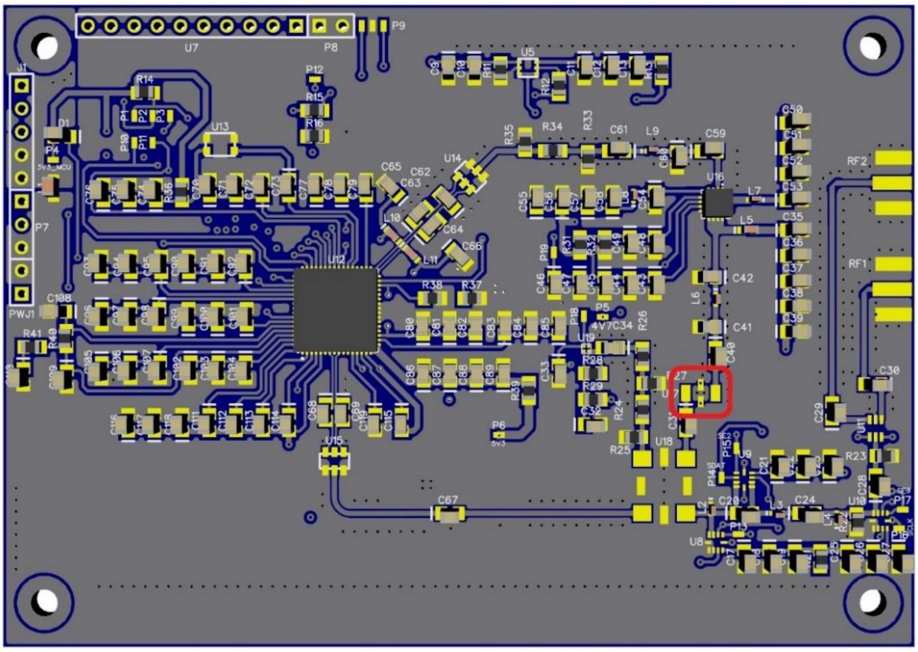

**Figure 3.10 :** Low pass filter location.

To show the characteristics and measure the losses (insertion and return) a PCB board was designed. Based on the measurements results the low pass filter has a insertion loss of 0.93 dB. On the other hand, simulation results show that it has less loss than the measured result, which is 0.55 dB. All the given values are presented in the following figures, Figure 3.11 and 3.12 respectively. Return loss is also presented in simulation result chart. The characteristics of the LPF is shown in both Figure 3.13 and 3.12. Its cut off frequency is nearly 1250 MHz at 3 dB insertion loss point as indicated 1.3 GHz in the datasheet of the component.

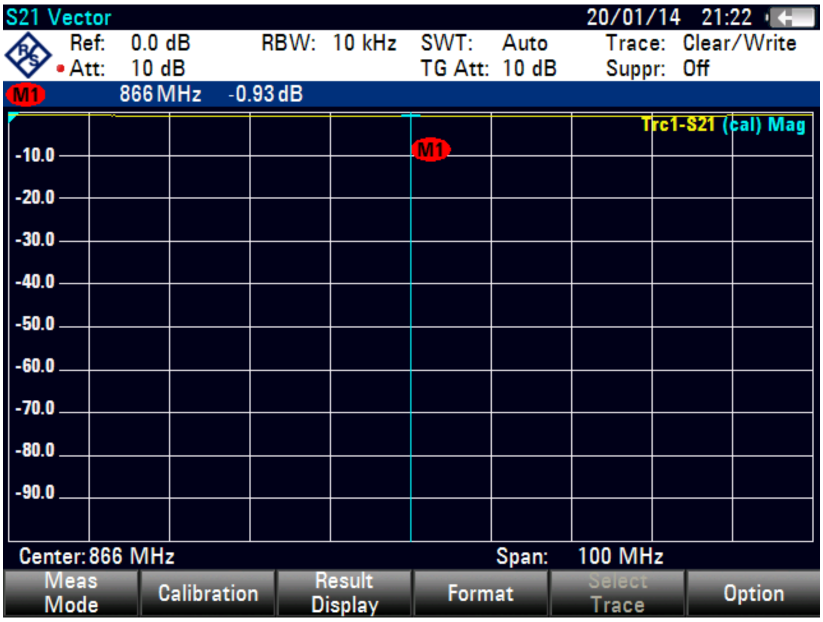


**Figure 3.11 :** Measured insertion loss of LPF.

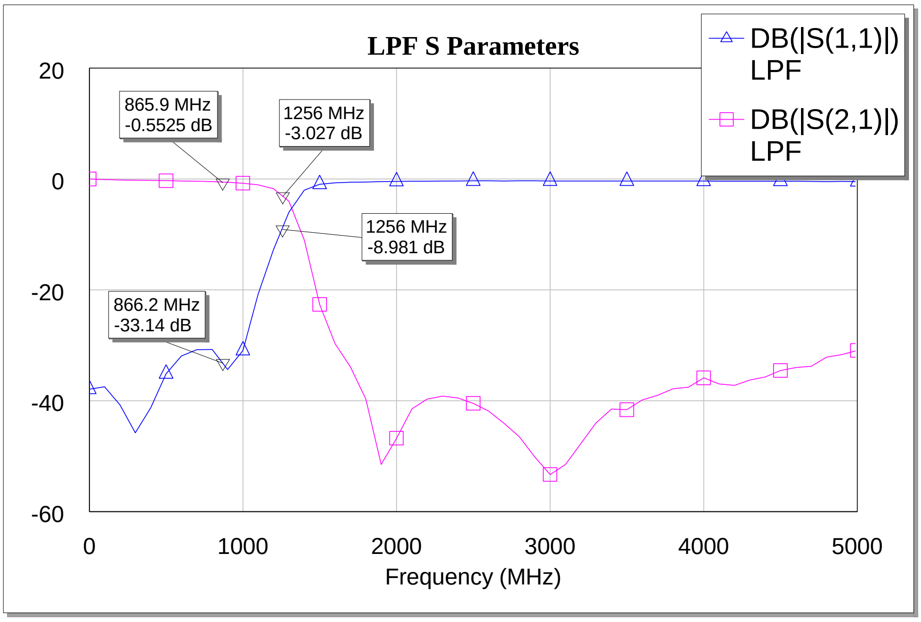


**Figure 3.12 :** Simulated insertion loss of LPF.


**Figure 3.13 :** Measured characteristics of LPF.

### 3.1.2.6 Directional coupler – isolation

Since the transmit RF signal is on even during reception, isolation between Tx and Rx is required. The sensitivity of the reader is related to the level of isolation. If isolation is poor, system performance is severely degraded. With this directional coupler the reader has a coupling of 10 dB and provides excellent isolation and hence directivity. The device has a typical insertion loss of 0.3 dB. The location of the coupler is shown in Figure 3.14.

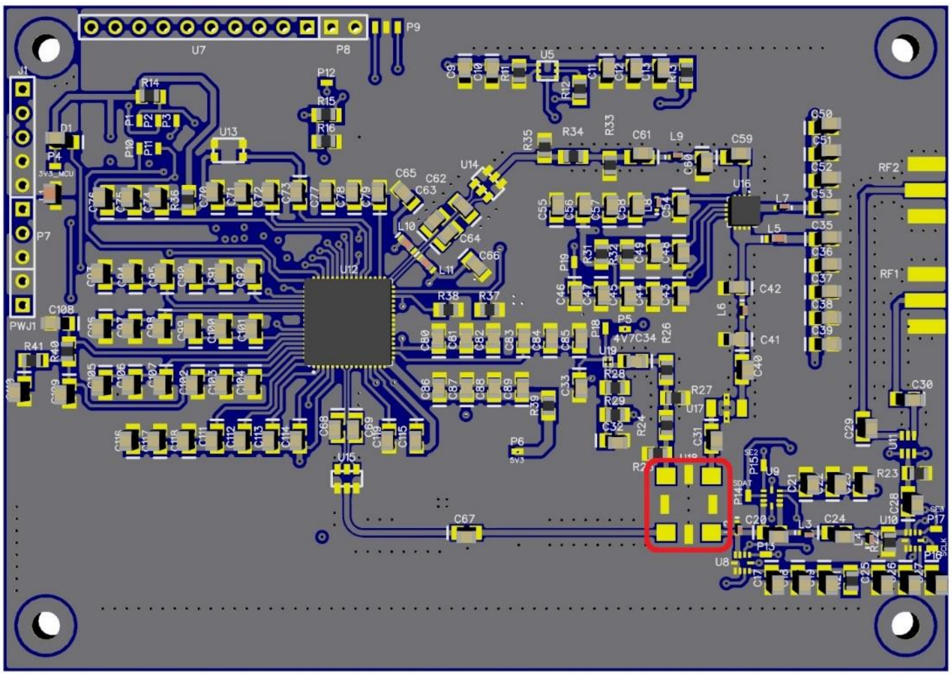

**Figure 3.14 :** Directional coupler location.

To check whether the loss parameters are satisfied, simulation and measurement operations were performed. Simulation results ensure the parameters are accurate compared with the values in datasheet. At the given frequency, 866 MHz, the directional coupler has an insertion loss of nearly 0.3 dB. But, in reality, in the designed board it has a really poor performance. Measured results show that insertion loss is 3.42 dB at 866 MHz. All the values indicated in the chart are shown in Figure 3.15 and 3.16 respectively. Return loss value is also presented in the simulation result chart. There is another graph, Figure 3.17, shows that at which frequencies the behavior of coupler is efficient. It has a wideband view and after 780 MHz and before 955 MHz, the characteristics of the coupler changes in a poor way.

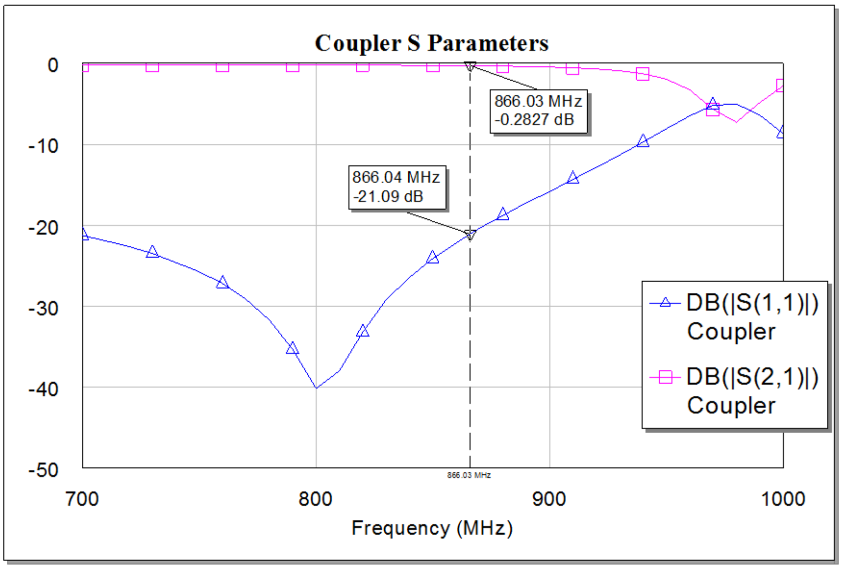


**Figure 3.15 :** Simulated insertion loss of coupler.

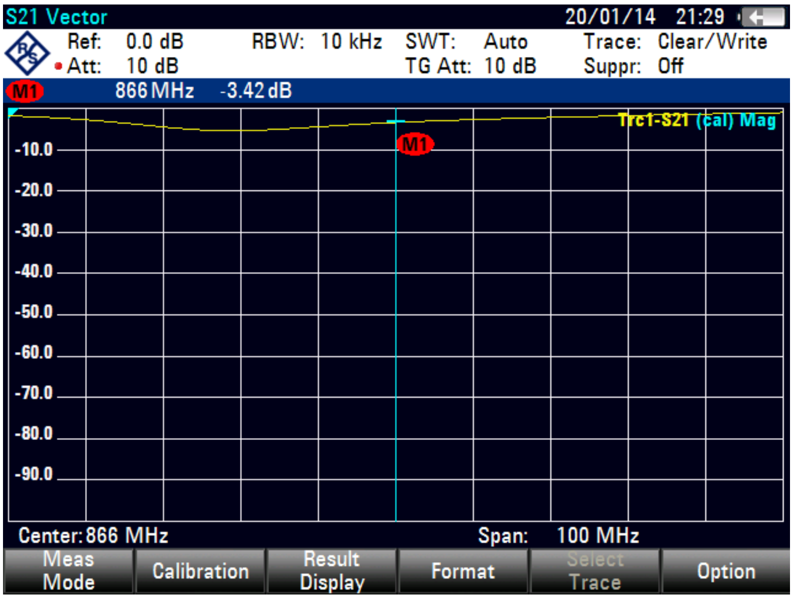


**Figure 3.16 :** Measured insertion loss of coupler.

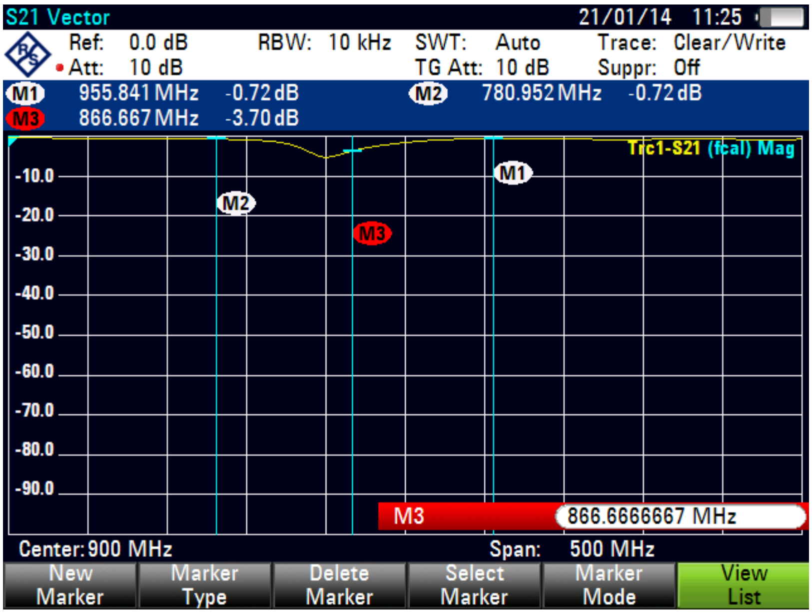


**Figure 3.17 :** Measured characteristics of coupler.

### 3.1.2.7 Power detection circuit

A power detector is used for the reader outputs at the antenna ports to control and limit the output RF power. It is placed at the coupled port of the directional coupler. Its location is shown in Figure 3.18.

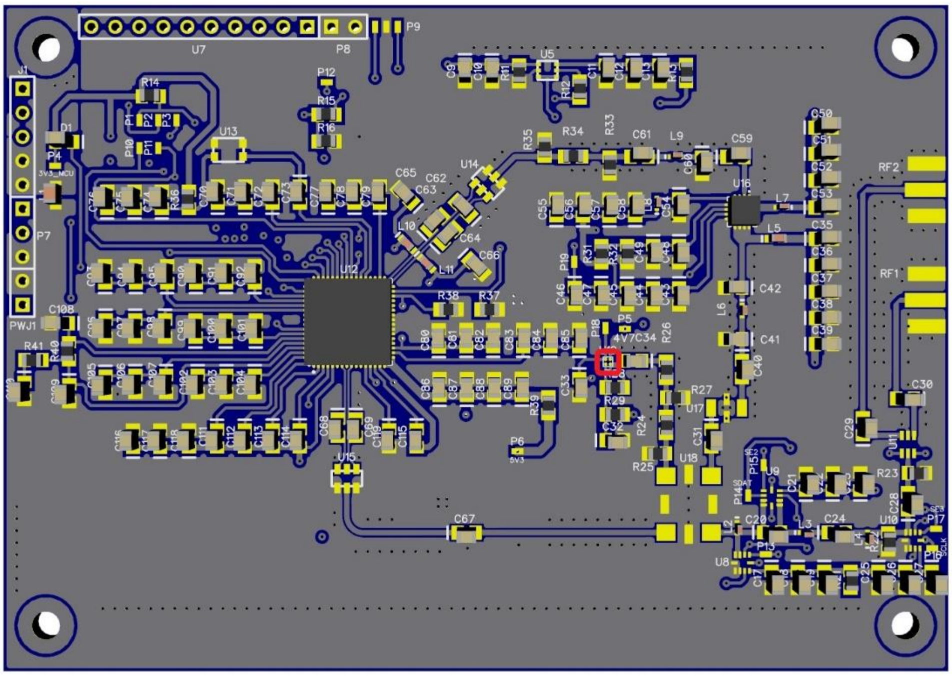

**Figure 3.18 :** Power detector location.

At the input of the power detector, a PI-Pad attenuator is placed in order to limit the input power seen by the power detector. A DC voltage is generated depending on the RF power at the detector input. This DC voltage is routed to the ADC input of the

AS3992 reader IC. Based on the DC voltage from the power detector, the bias voltage for the third amplifier stage of the PA is controlled via the DAC output of AS3992.

### 3.1.2.8 Tuner – antenna tuning circuit

Tuner circuit is one of the most important and innovative building blocks in the reader design. This part of the reader is used to compensate reflections of transmit power at the reader antenna. In an ideal case, transmit power which is fed to the antenna would not be reflected. However, in real cases every antenna reflects some amount of power back into the system because of changes in the vicinity of the antenna causing impedance mismatch. For instance, by placing objects near the antenna, the impedance of the antenna is changed. The effect of impedance change depends on the material properties of the object. In a 50 ohm system, an impedance which is different from 50 ohm increases the reflection coefficient (S11). Often antenna design constraints (size, material, etc…) also result in a considerable high reflection coefficient (S11). In RFiD, this reflected power is called self-jammer and couples into the receiving part of the reader, limiting its sensitivity. The tuning circuit can compensate this mismatch at the antenna by the unique feature of AS3992 reader IC. In figure 3.19, the location of the tuning circuit is shown.

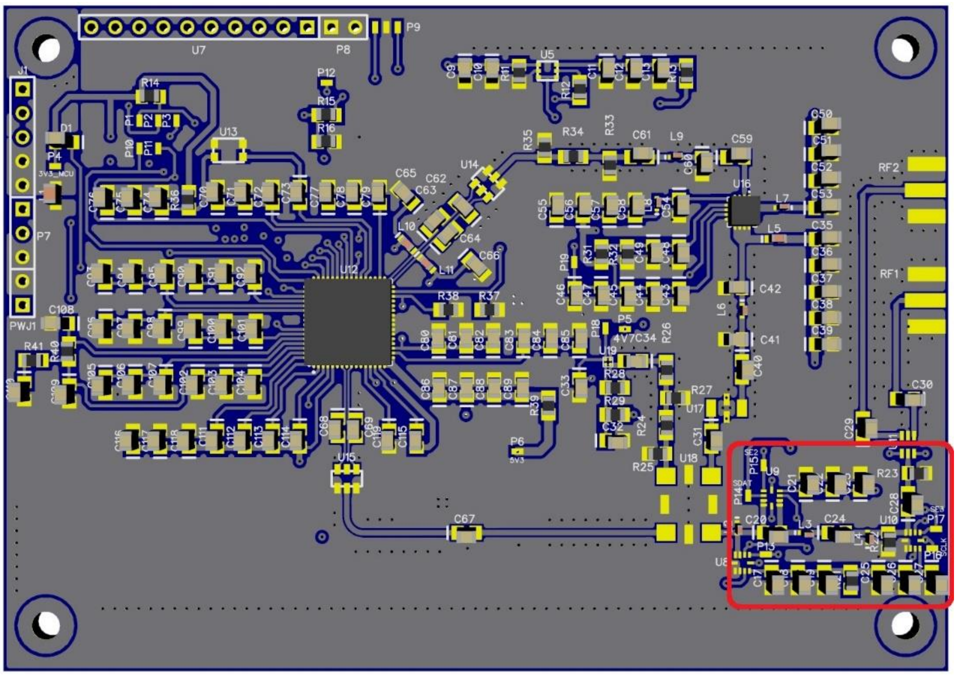

**Figure 3.19 :** Tuner location.

This tuning circuit comprises three digital tunable capacitors (DTC) of which capacitance values can range from 1.05 pF up to 5.1 pF with a step value of 131 fF. The DTCs are controlled via SPI interface. Since the AS3992 reader IC also has a SPI interface, the whole reader can operate with one microcontroller. Additional lumped components are used to set the center impedance of the tuning circuit around 50 ohm and to set the tuning range.

To perform simulations for measuring the losses, equivalent circuit model of a DTC was designed using AWR Microwave Office and three of them combined in a circuit for a tuner application based on the recommended structure at 866 MHz. Designed schematics are presented in Figure 3.20 and 3.21 respectively. The tuned value of DTC is 4.61 pF for 50 ohm at 866 MHz. It can be tuned for other frequencies for related applications.

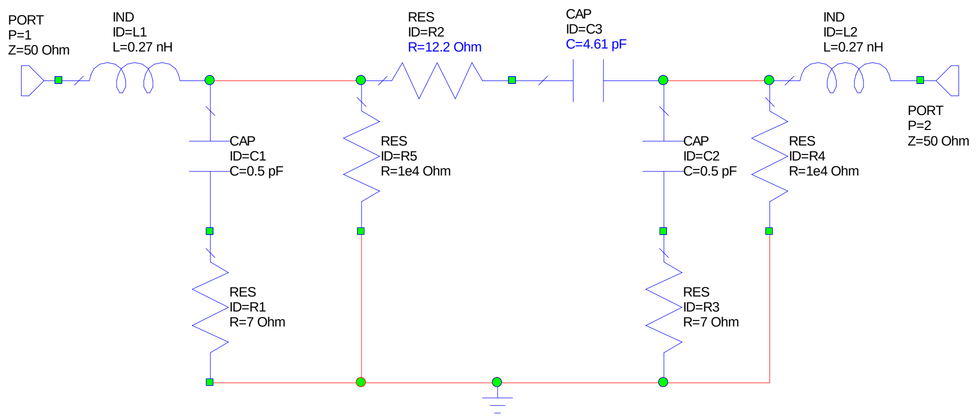


**Figure 3.20 :** Equivalent circuit of DTC.

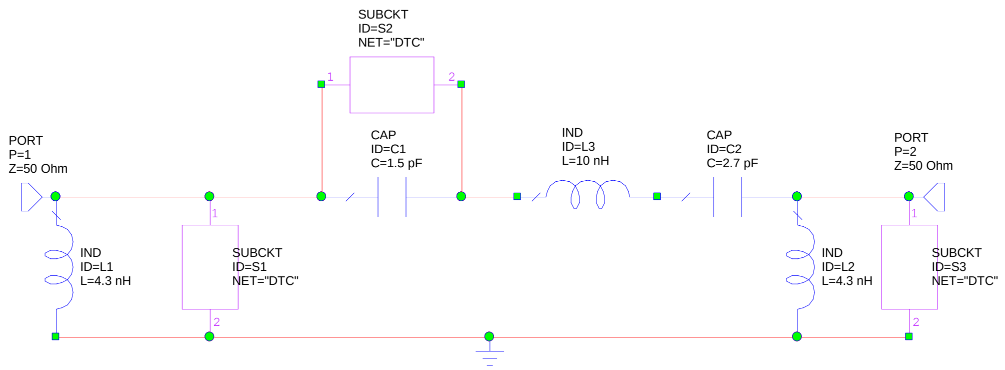


**Figure 3.21 :** Tuner circuit.

After designing the circuits in AWR, simulations were performed and losses were measured. In Figure 3.22, insertion loss of a DTC is shown and indicated as nearly 1.9 dB and in Figure 3.23 the loss of the combination of DTCs, tuner structure, is presented. It is clear from the graph that tuner circuit has an insertion loss of 0.73 dB at 866 MHz. Since this circuit is an impedance matching network, there is also a chart (Smith Chart), Figure 3.24, which represents the return loss of the system. It shows that, impedance matching is nearly achieved with a little loss at 866 MHz.

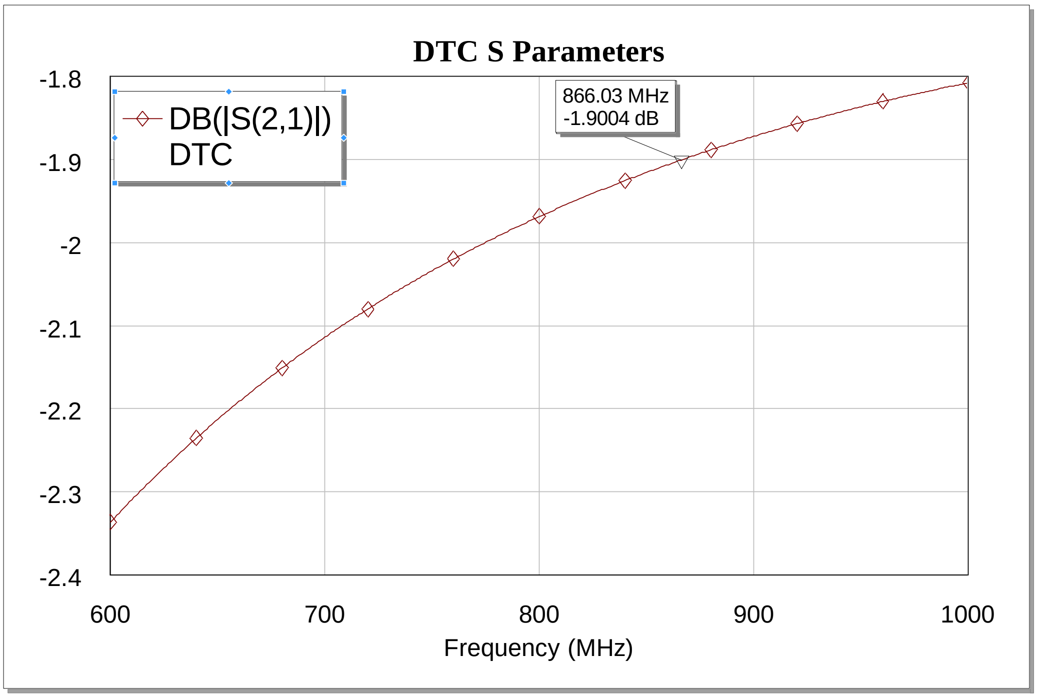


**Figure 3.22 :** Insertion loss of DTC.

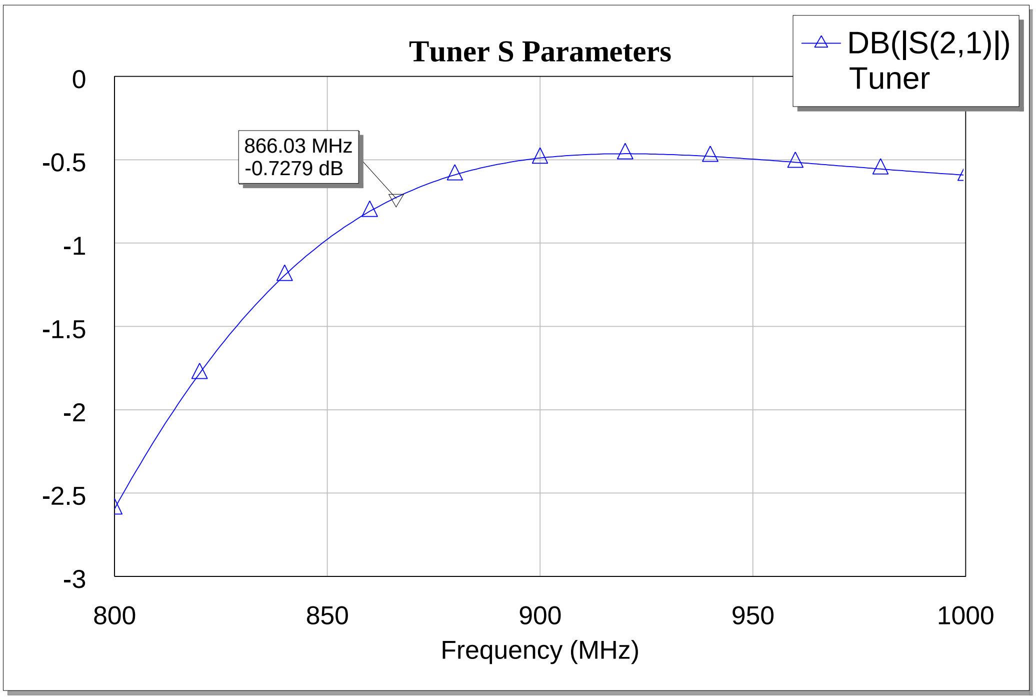


**Figure 3.23 :** Insertion loss of tuner.

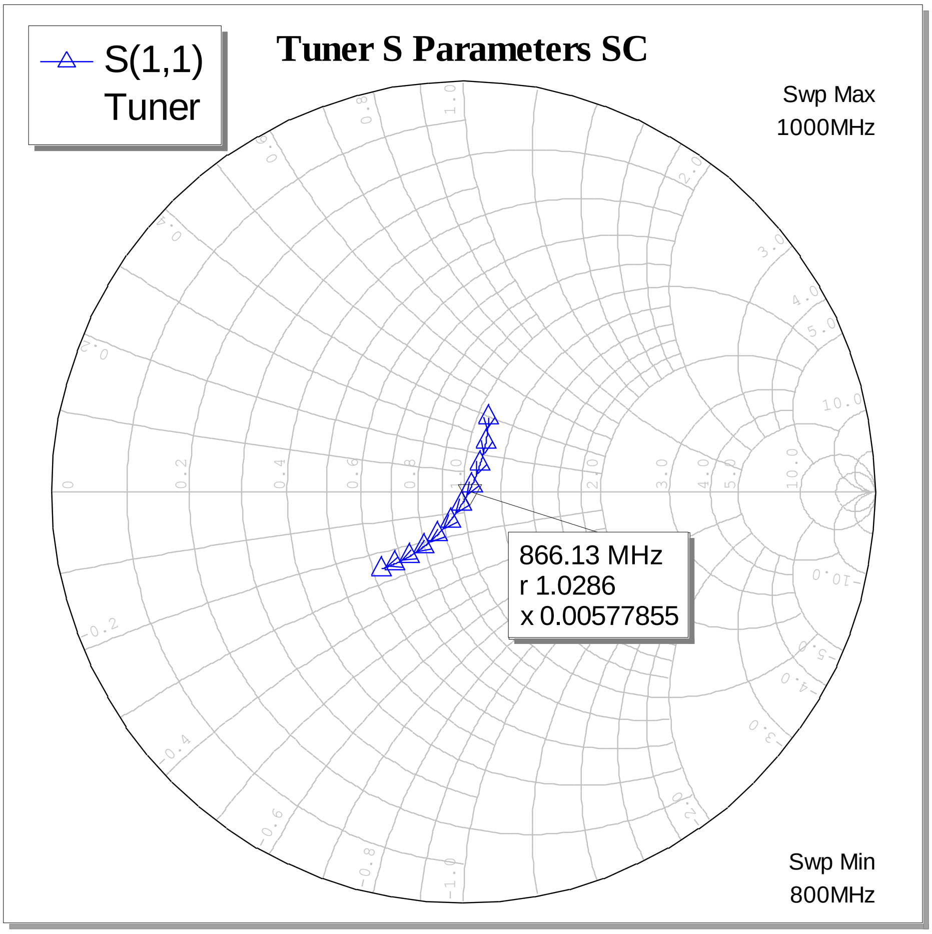


**Figure 3.24 :** Return loss of tuner.

### 3.1.2.9 RF Switch – antenna multiplexing

It is possible to connect two antennas to the UHF RFiD reader. It is provided by an SPDT RF switch, which has two control lines driven by the MCU complementary. It integrates on-board CMOS control logic with a low voltage CMOS-compatible control interface (Peregrine Semiconductor Corp., 2012). The truth table for the operation can be found in Table 3.1. The switch has a typical insertion loss of 0.35 dB at UHF band. The location of the switch is shown in Figure 3.25.

**Table 3.1 :** Truth table of RF switch for multiplexing.

| Control Voltages | Signal Path |
|---|---|
| Pin VDD = Low<br>Pin CTRL = High | RFC to RF1 |
| Pin VDD = High<br>Pin CTRL = Low | RFC to RF2 |

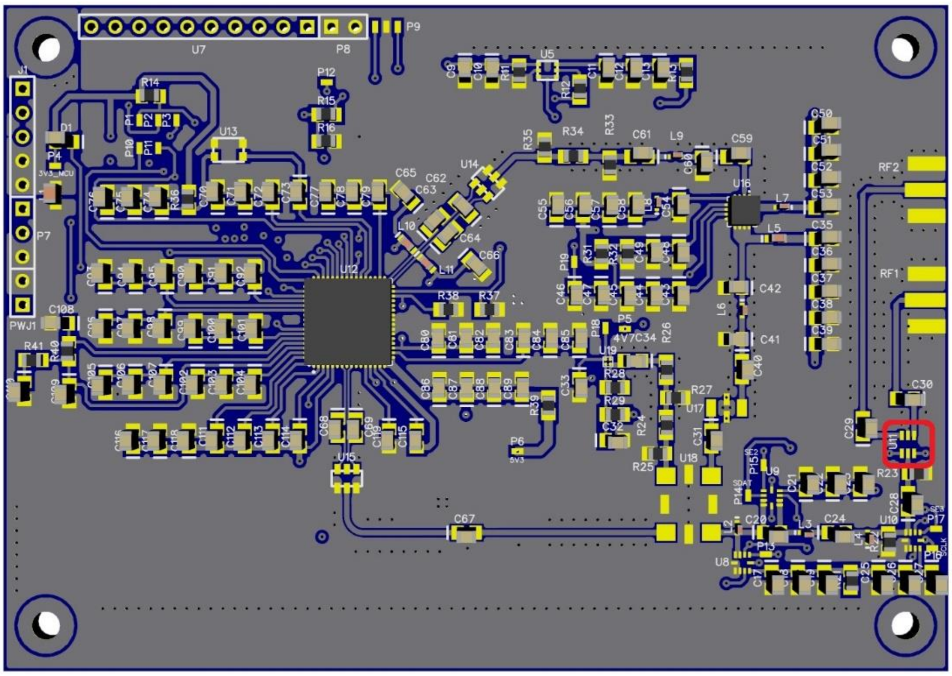

**Figure 3.25 :** Antenna switch location

Simulations and measurements were performed in order to check the efficiency of the components. Figure 3.26 indicates that RF switch IC has an insertion loss of 0.48 dB at 866 MHz. In measurement result, the value is nearly the same as 0.55 dB shown in Figure 3.27. Return loss value is also presented in simulation results chart.

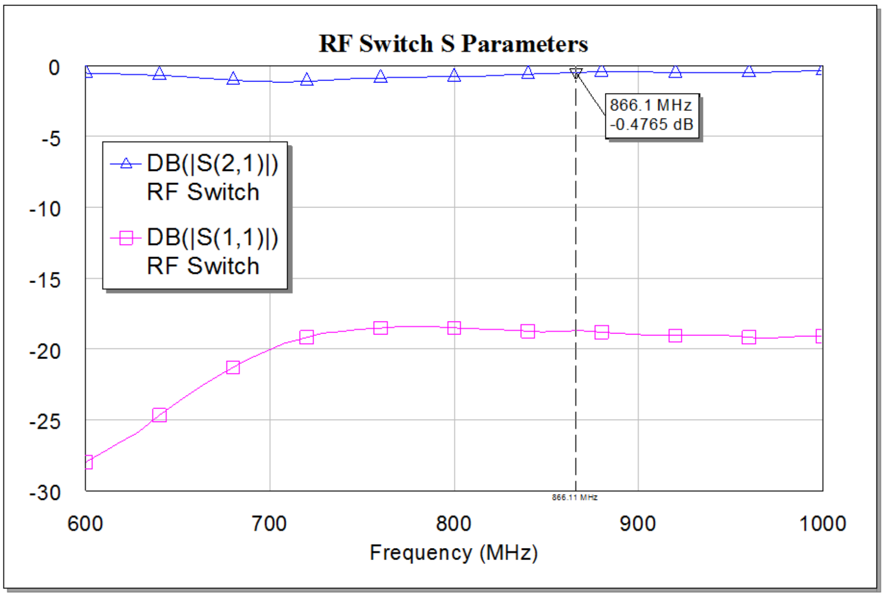


**Figure 3.26 :** Simulated insertion loss of RF switch.

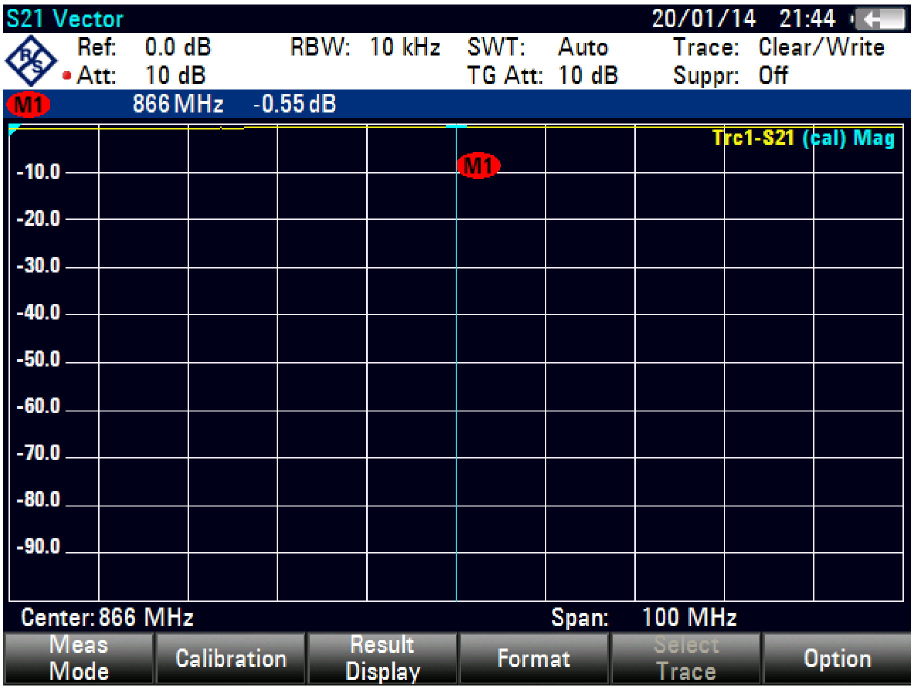


**Figure 3.27 :** Measured insertion loss of RF switch.

### 3.1.2.10 LDOs – Power supplies for whole system

There are two voltage regulators in the reader system. One is used for AS3992 reader IC and OP-Amp. The output voltage is adjusted to 5.3V by an external voltage divider.

<u>Voltage Divider Calculation for the First Regulator:</u>

$$V_{SETBYP} \;=\; 1.2V \tag{4.1}$$

$$R_X \;=\; 90.9\;k\Omega \tag{4.2}$$

$$R_Y \;=\; R_X\left(\frac{V_{OUT}}{V_{SETBYP}} - 1\right) = 310.5\;k\Omega \tag{4.3}$$

$$V_{OUT} = V_{SETBYP}\left(1 + \frac{R_Y}{R_X}\right) = 5.37V \tag{4.4}$$

The other regulator is used to supply the power amplifier and provides the bias reference voltage for the PA. The output voltage is adjusted to 4.7V by an external voltage divider.

Voltage Divider Calculation for the Second Regulator:

$$V_{SETBYP} = 1.2V \tag{4.5}$$

$$R_A = 82\ k\Omega \tag{4.6}$$

$$R_B = R_A\left(\frac{V_{OUT}}{V_{SETBYP}} - 1\right) = 239.17\ k\Omega \tag{4.7}$$

$$V_{OUT} = V_{SETBYP}\left(1 + \frac{R_B}{R_A}\right) = 4.7V \tag{4.8}$$

The locations of the regulators are shown in Figure 3.28.

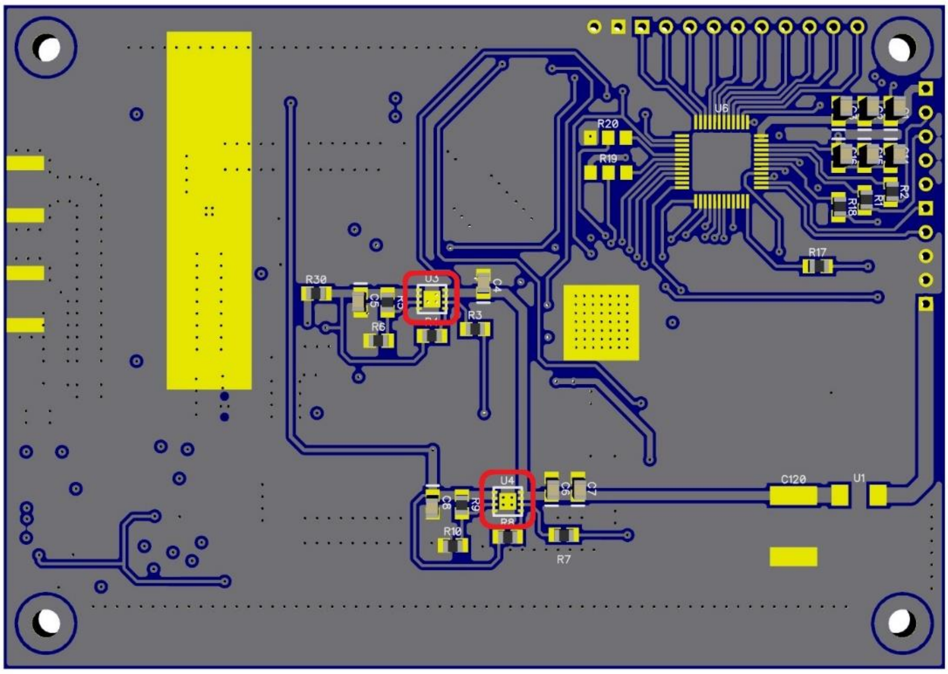


**Figure 3.28 :** Regulator locations.

### 3.1.3 Schematics of Blocks

In this section of the thesis, the schematics of the building blocks are investigated. The UHF RFiD reader circuit has been designed with a professional schematic & PCB design sotware DipTrace.

### 3.1.3.1 AS3992 section

In this section, the circuit has been designed depending on the instructions in the datasheet of the reader IC. The schematic of the circuit is shown in Figure 3.29.

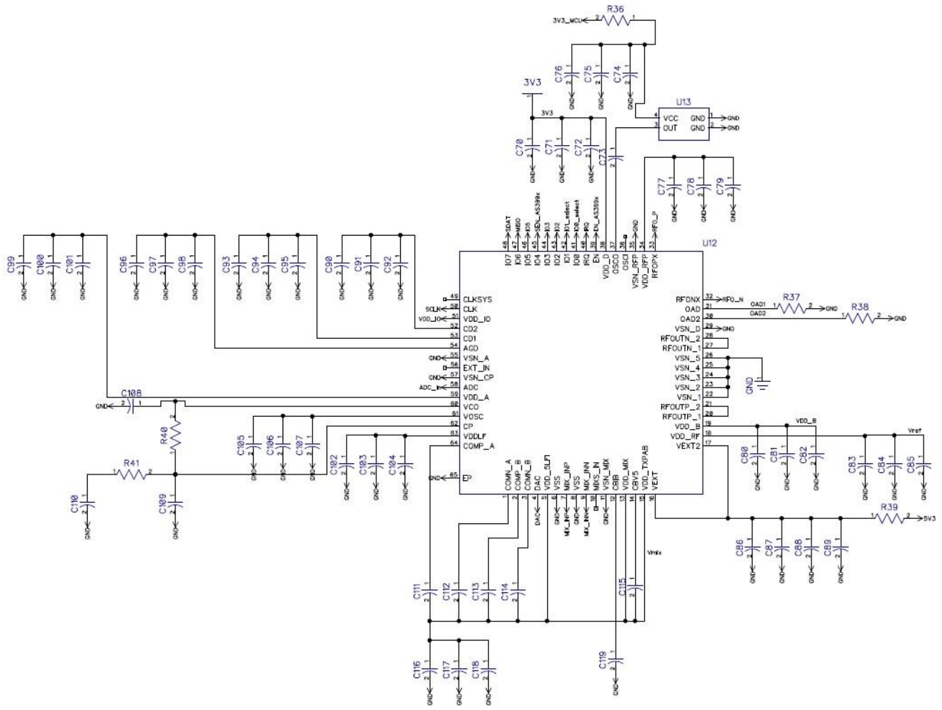

**Figure 3.29 :** Schematic of AS3992 section.

### 3.1.3.2 Power amplifier / coupler section

The designed power amplifier and coupler section is shown in Figure 3.30. The lumped components are chosen via the instructions in the datasheet.

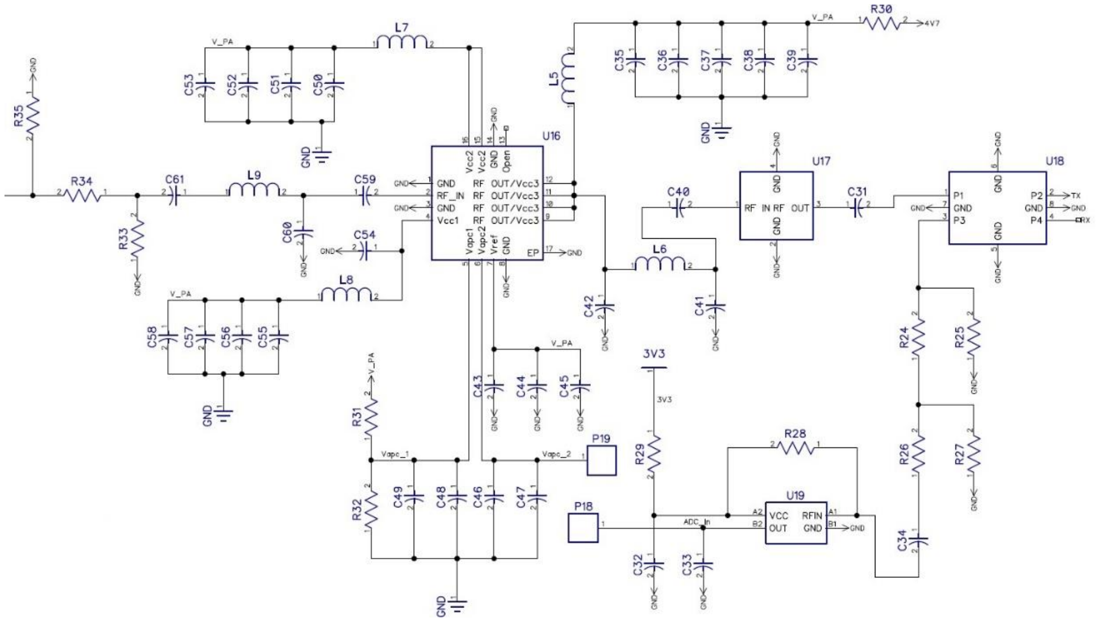

**Figure 3.30 :** Schematic of power amplifier/coupler section.

### 3.1.3.3 Tuning / antenna switch section

To design this circuit three tunable capacitors and an RF switch were used. The designed schematic is shown in Figure 3.31.

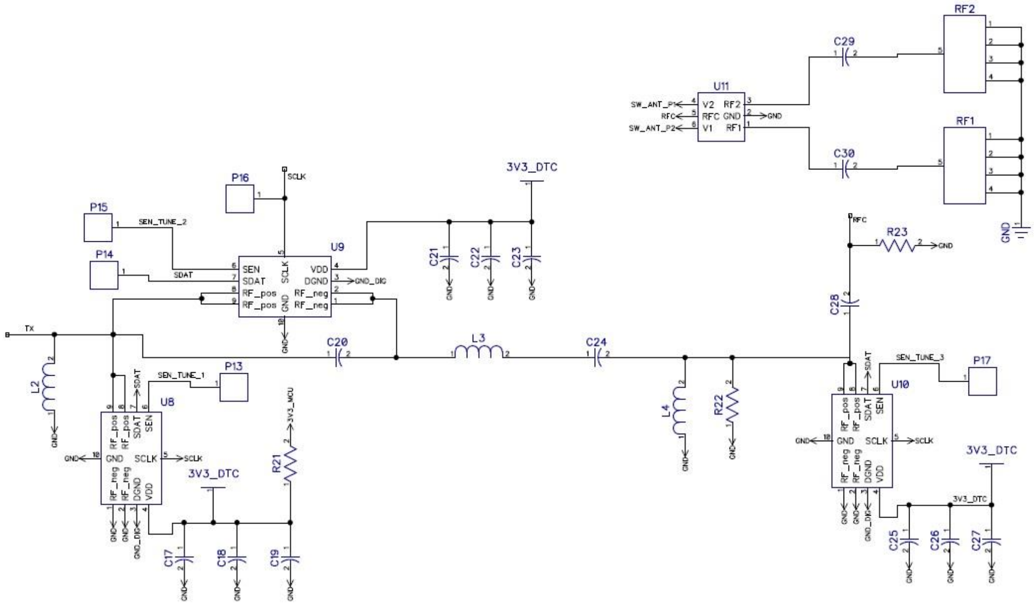


**Figure 3.31 :** Schematic of tuner/antenna switch section.

### 3.1.3.4 MCU section

This section is designed to interact with the AS3992 devices via the SPI interface and with the host computer via the USB interface. The following Figure 3.32 shows the designed schematic of the MCU part.

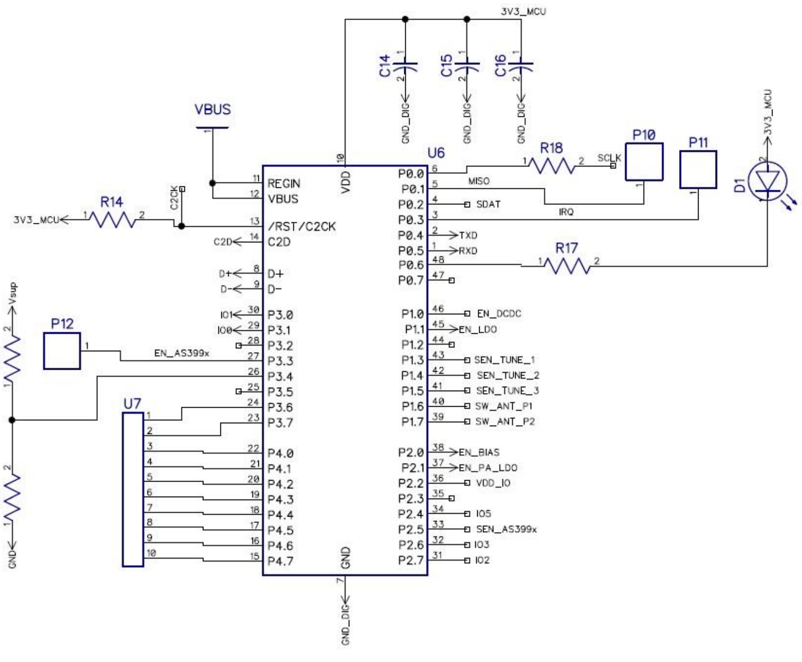


**Figure 3.32 :** Schematic of MCU section.

#### 3.1.3.5 LDO / buffer section

The regulator and Op-Amp section is shown in Figure 3.33.

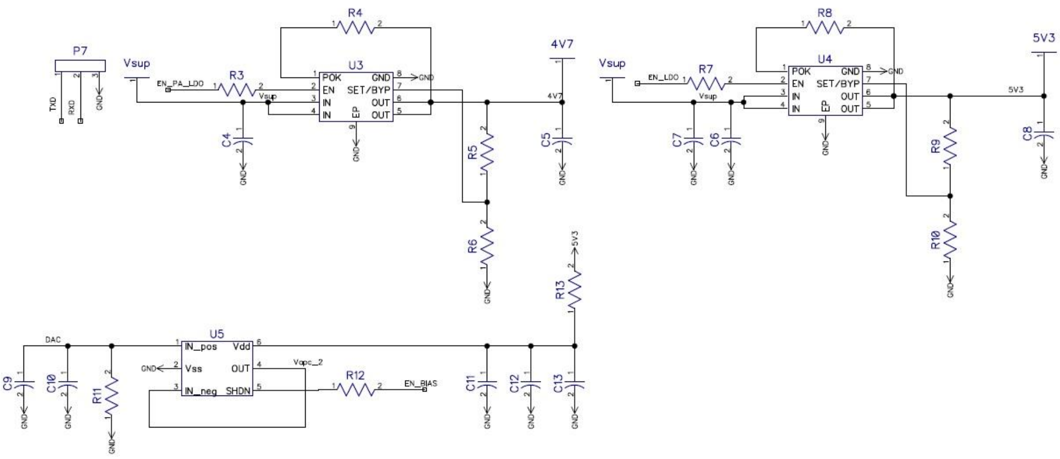

**Figure 3.33 :** Schematic of op-amp section.

#### 3.1.3.6 Connector / interface section

The connectors and interfaces section have been designed for communication with the outside of the device. The following Figure 3.34 shows the schematic of the designed section.

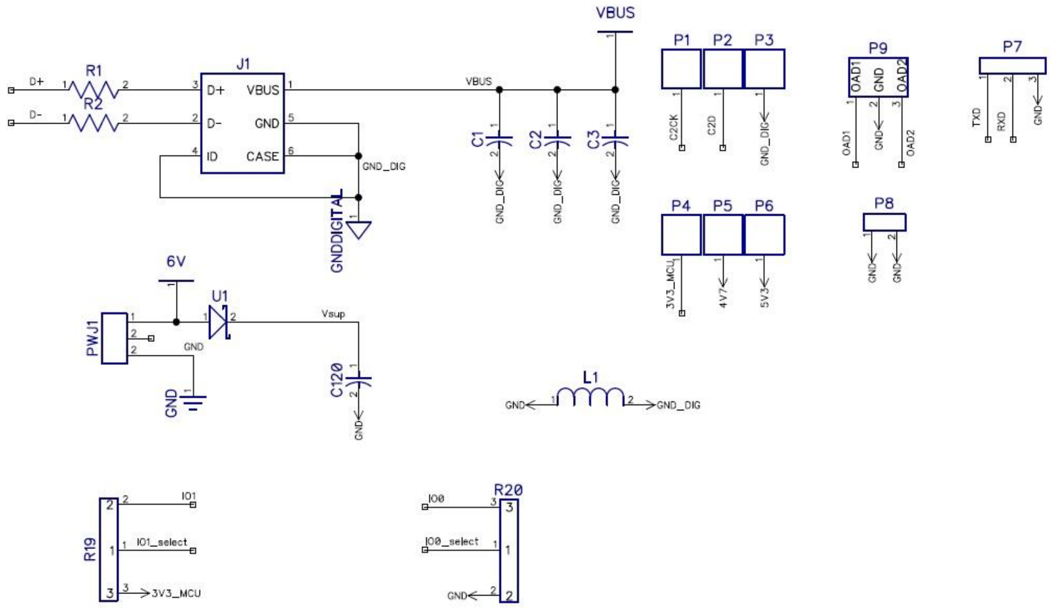

**Figure 3.34 :** Schematic of connector/interface section.

### 3.1.4 PCB Design

This section focuses on the selected PCB material, layer structure of it and layouts of designed UHF RFiD reader.

#### 3.1.4.1 PCB board selection

The used PCB material is a general purpose standard material called FR4. This material can be easily found at most of the PCB design houses. The designed PCB dimension is 100 mm x 70.5 mm and thickness is 1.88 mm. Detailed information about PCB material specification can be found in Appendix A.

#### 3.1.4.2 PCB board layer structure

The UHF RFiD reader has six layers. In the following Figure 3.35 all the layers are shown. The first layer (top) was used for RF transmission lines. It is important to keep the thickness of this layer constant as it influences the impedance of the coplanar waveguides. The second and fourth layers are used to separate layers to have a good isolation. The third layer is used for analog (RF) ground, the fifth layer is used for digital signals and digital ground and the sixth layer (bottom) is used for power signals. All the places other than the traces were poured with the copper ground to carry the RF signals with the guidance of analog ground.

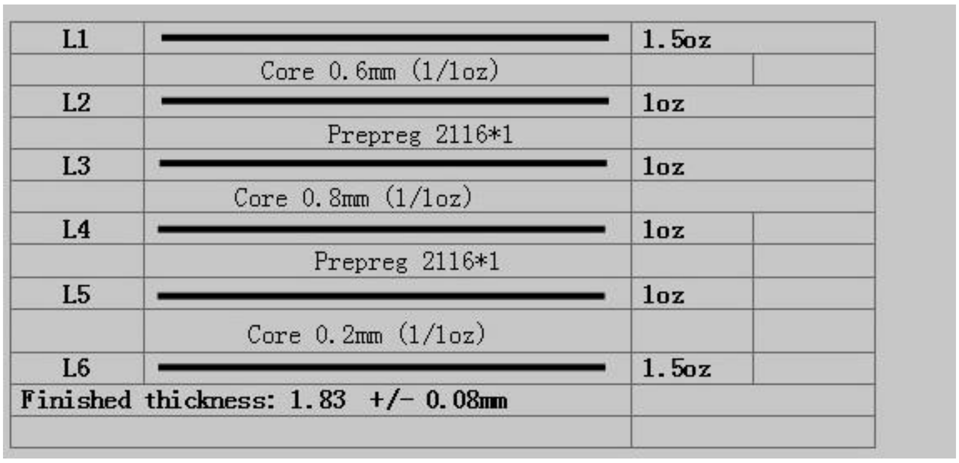


**Figure 3.35 :** Layer stack of the PCB.

#### 3.1.4.3 PCB Layouts

Following sub-sections shows the PCB layouts of all the layers of UHF RFiD reader in Figure 3.36, Figure 3.37, Figure 3.38, Figure 3.39, Figure 3.40 and Figure 3.41 respectively.

- **Top layer**

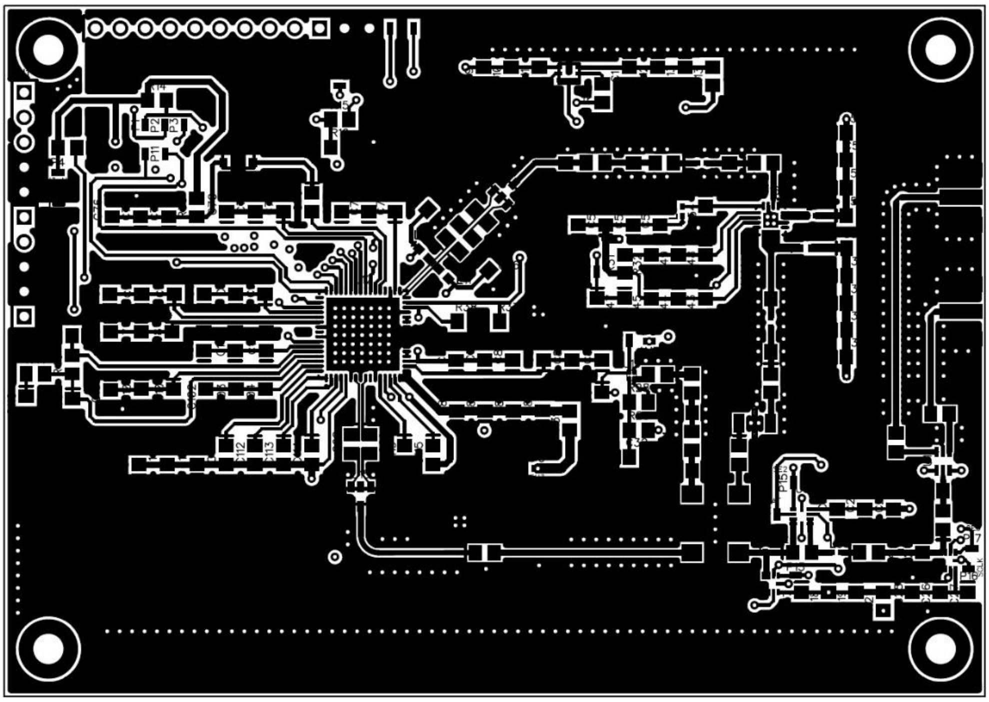

**Figure 3.36 :** Top layer (first layer) of the PCB.

- **2nd layer**

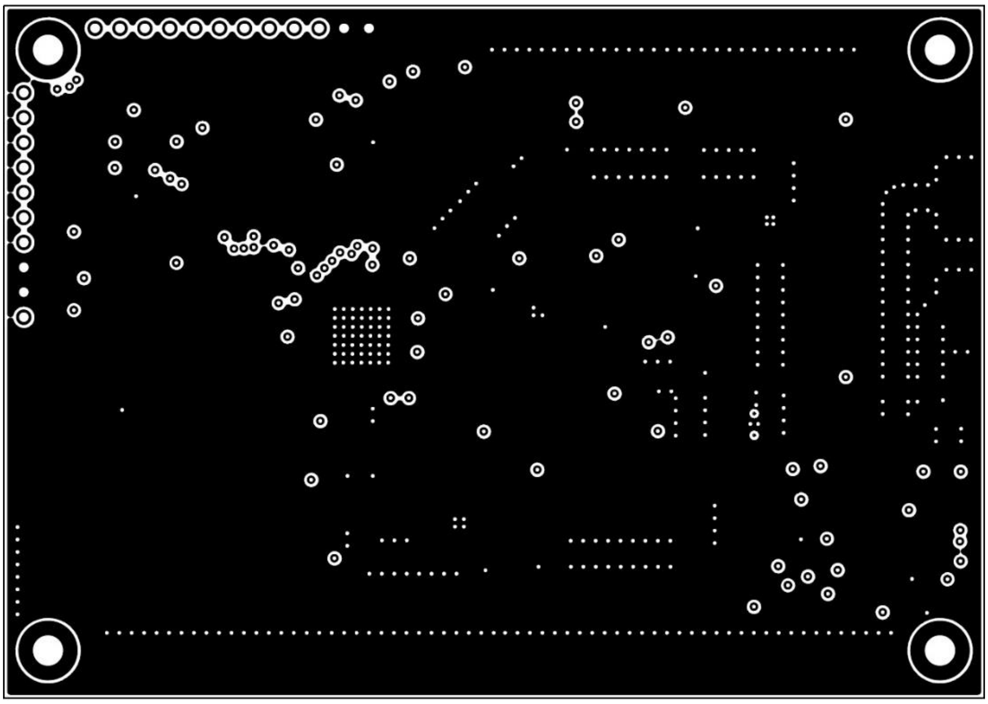

**Figure 3.37 :** Second layer of the PCB.

- **3$^{rd}$ layer**

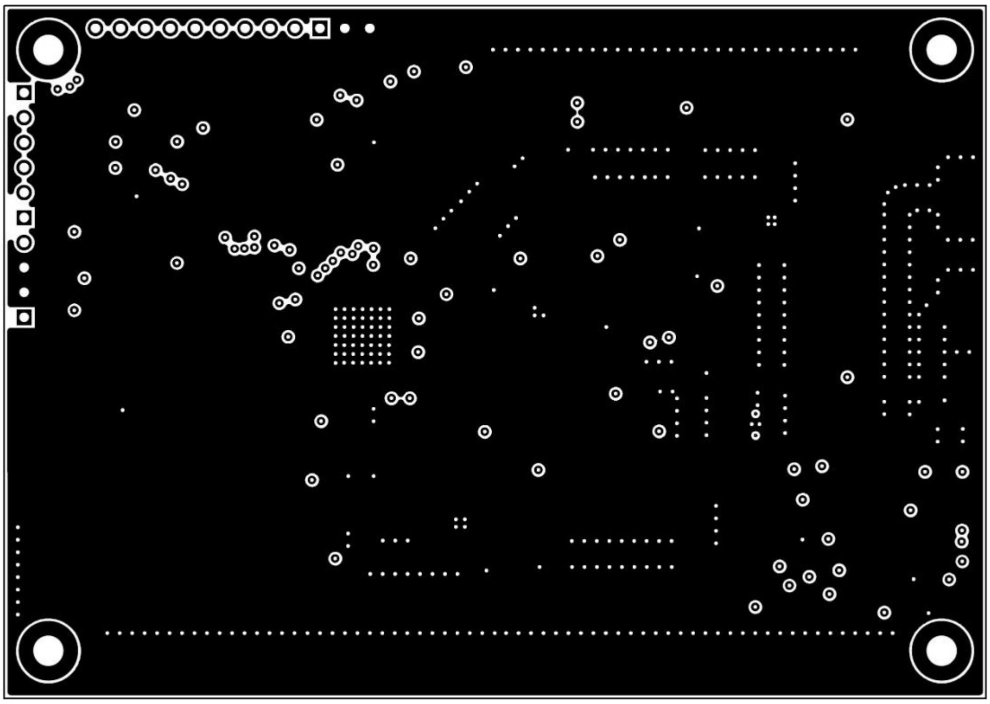

**Figure 3.38 :** Third layer of the PCB.

- **4$^{th}$ layer**

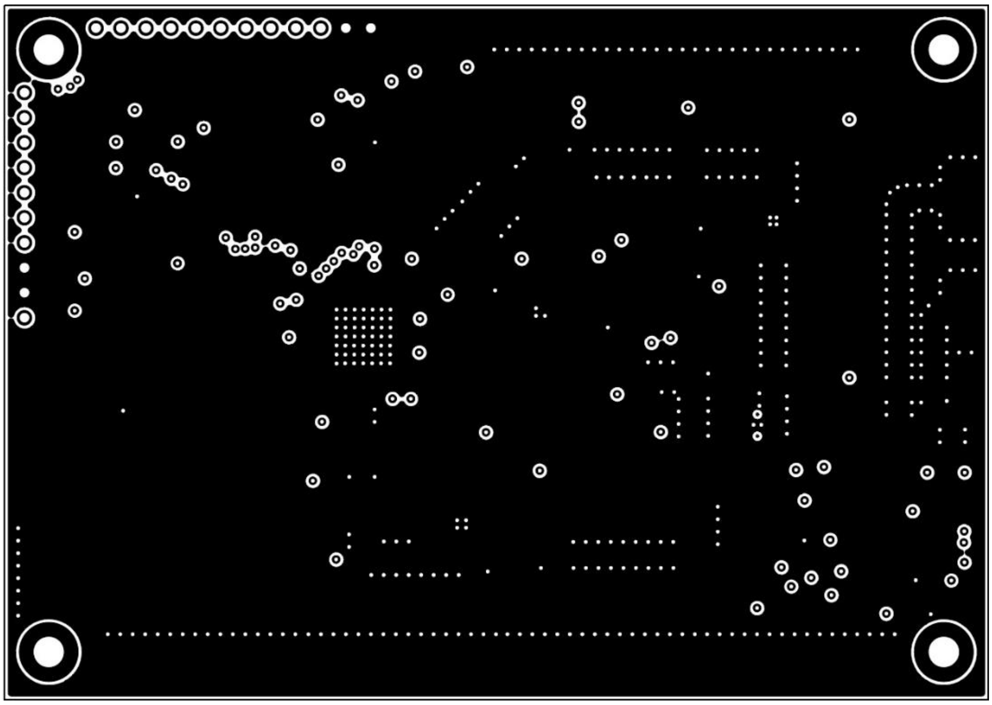

**Figure 3.39 :** Fourth layer of the PCB.

- **5$^{th}$ layer**

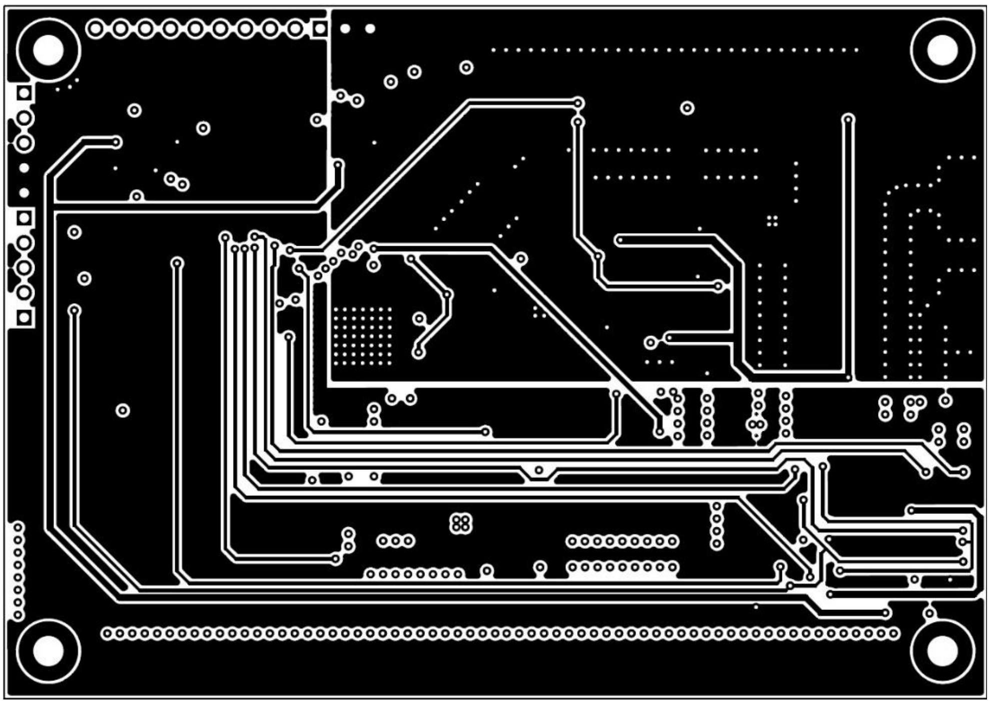

**Figure 3.40 :** Fifth layer of the PCB.

- **Bottom layer**

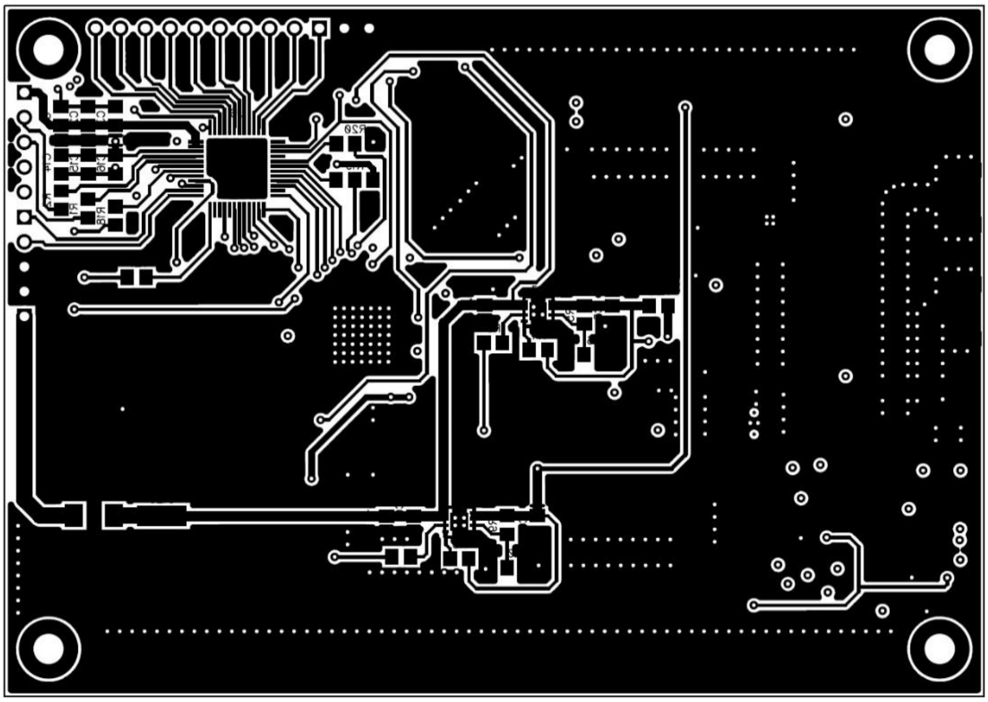

**Figure 3.41 :** Bottom layer (sixth layer) of the PCB.

#### 3.1.4.4 Impedance controlled traces

To minimize reflections and hence losses, the impedance of the single ended coplanar waveguides are matched to 50 ohms. Since transmitting and receiving operations at the AS3992 reader IC are done differential, differential coplanar waveguides are also used, which are matched to 100 ohms.

In today's world of high-speed digital systems with clock edge rates commonly approaching 10 Gbps and analog frequencies above the 5-10 GHz range, copper trace interconnects on printed circuit boards (PCBs) must be considered as transmission lines. Transmission lines are electronic interconnects that distribute high-speed digital signals over copper media, and these lines must be controlled by the PCB designer. The critical parameter is the characteristic impedance of the PCB trace, which is the ratio of a voltage to the current of a waveform moving along the trace. This voltage to current ratio is a function of frequency and a function of the physical geometries of the transmission line and its relationship to surrounding dielectric properties.

Electrical components possess certain characteristic impedance values, which will vary depending on the logic family. The designer's responsibility is to match the impedance of the component's load and source requirements with that of the interconnecting PCB traces. To achieve maximum signal transfer from a source (sending unit) to a load (receiving unit), the PCB trace impedance must match the output impedance of the source to the input or load. If the impedance of the PCB trace connecting two components does not match the components' characteristic impedance, multiple waveform reflections will occur on the signal line before the load device can settle into a new logic state. This will result in increased switching times within the device or the circuit and produce random errors. The circuit design engineer and PCB designer must carefully select a nominal value and tolerance of trace impedance. Tolerances of 10% or less are not uncommon for high-speed applications.

The characteristic impedance of a PCB trace is typically determined by its inductive and capacitive reactance, resistance, and conductance. These parameters will be a function of the physical dimensions of the trace, the dielectric constant of the PCB substrate material, and dielectric thickness. PCB trace impedance can range from 25 to 120 ohms. PCB transmission lines consist of a copper trace conductor, reference copper ground or power plane layers, and dielectric substrate. The relationship between the copper trace conductor layers and the reference plane layers (where the signal return path flows) form the controlled impedance structure and because of this structure, most controlled impedance PCBs will be multilayer structures. The impedance value generated from the PCB structure will be determined by the following parameters:

- width and thickness of the copper signal trace
- thickness of the core or prepreg material on either side of the copper trace
- dielectric constant of the core and prepreg material

Types of Transmission Lines:

**Single-ended** transmission lines are the most common way to connect two devices. This case is where a single conductor or PCB trace connects the source of one component to the load of another. There must be a reference or ground plane on the adjacent layer in order to provide a signal return path. Controlled impedance designs are usually produced with microstrip, embedded microstrip, stripline, or dual asymmetrical stripline configurations.

**Differential** configurations of transmission lines are used when better noise immunity and improved timing are required in critical applications. Typical configurations will have a balanced line where the signal and return paths have similar geometry. There are two modes of differential configuration: even and odd mode. Even mode is where the same signal is sent through both lines and there is no return path. For this configuration, the electrical field lines are directed toward ground with no coupling to each other. Odd mode is where the signals are sent in a complementary form and the signals are actually mirrored so that the voltage and current flows are opposite. The electrical fields are coupled together along the surface between the two adjacent signals. With the voltage reversed, the electric fields will originate with one line and terminate with the other. This is the differential form of signal transmission and results in good coupling (Viasystems Group, Inc., 2011).

✓ **50 ohm traces used in PCB design – single ended**

In the following Figure 3.42, the 50 ohm single ended impedance controlled traces are shown. The widths of the traces were calculated via "TXLINE" tool provided by AWR shown in Figure 3.43. The used parameters are as follows:

- Dielectric of PCB material (FR4): 4.5
- PCB layer thickness of RF section: 0.51 mm
- Copper thickness: 43 um
- Ground strip separation: 0.19 mm

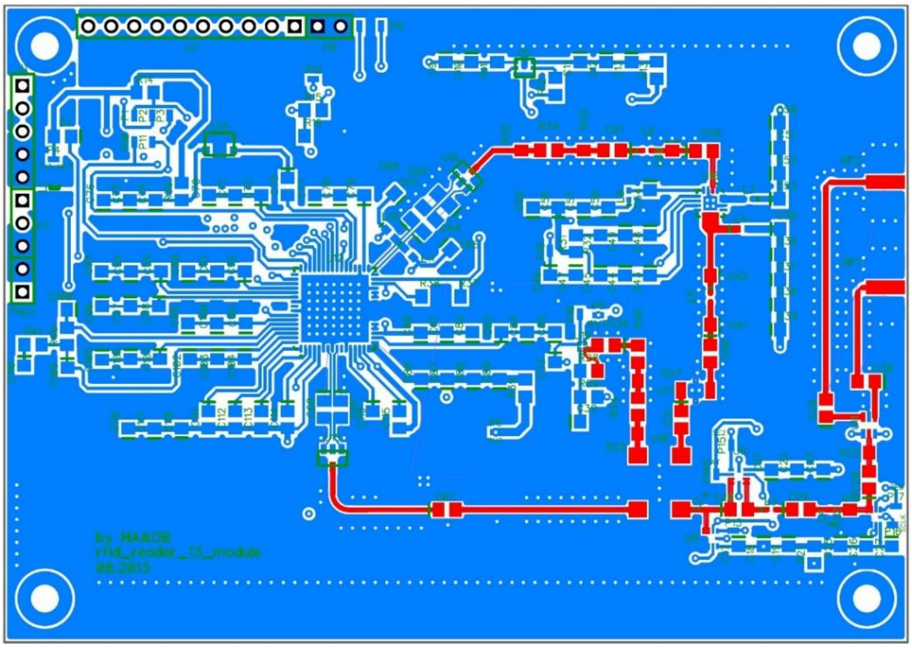

**Figure 3.42 :** 50 ohm single ended impedance controlled traces.

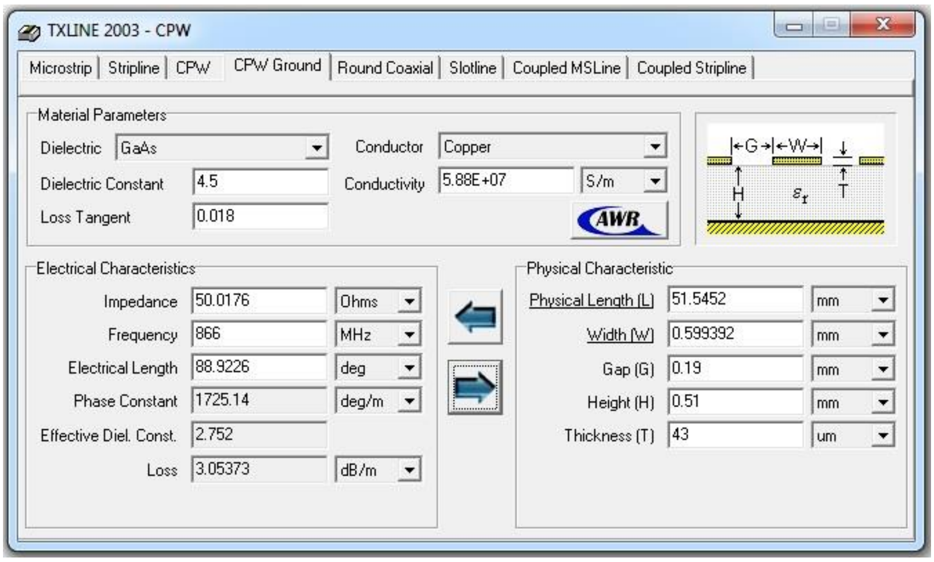


**Figure 3.43 :** TXLINE tool for impedance calculation.

✓ **100 ohm traces used in PCB design – differential**

Differential coplanar waveguides are shown in Figure 3.44. These impedance calculated traces are 100 ohms and the calculations were made via “PCB Toolkit” tool provided by Saturn PCB Design, Inc. shown in Figure 3.45. The used parameters are the same as 50 ohm traces.

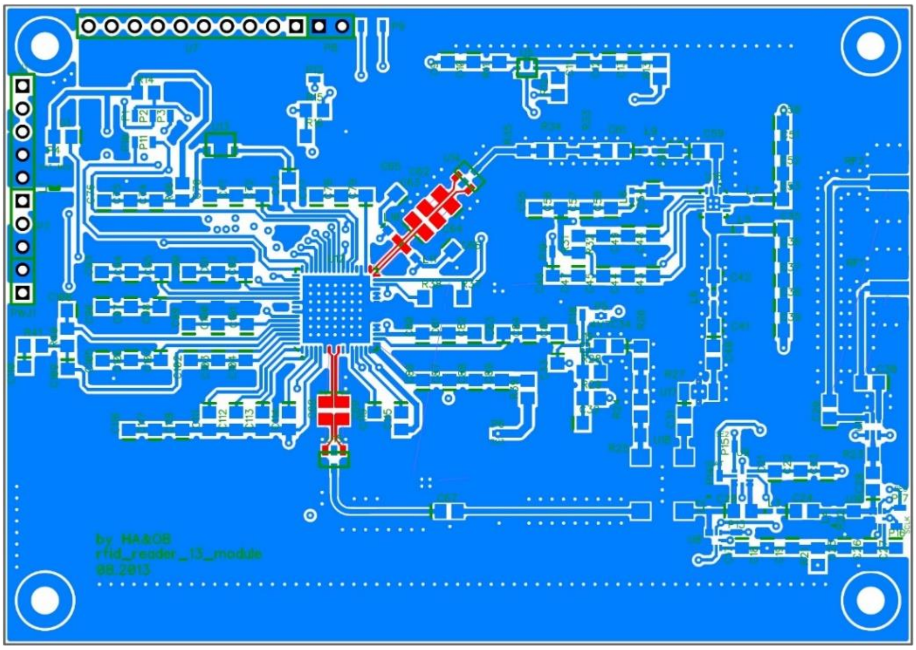

**Figure 3.44 :** 100 ohm differential impedance controlled traces.

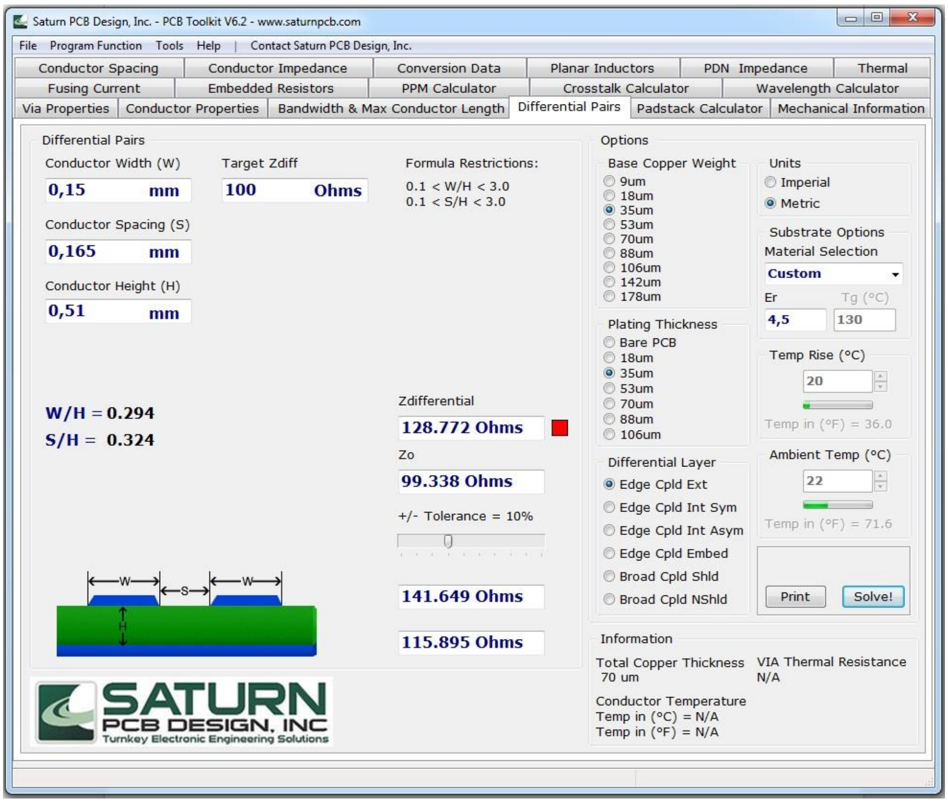


**Figure 3.45 :** PCB Toolkit tool for impedance calculation.

### 3.1.4.5 Connectors and interfaces

The UHF RFiD reader has a UDB interface and UART for communication with the host system. USB interface uses a USB mini A/B connector. UART interface connection is possible via pin headers.

For the power supply of the reader a DC socket is used. Outer diameter of the plug is 6 mm and the inner contact diameter is 1.95 mm.

For RF radiation 50 ohm SMA antenna connectors are used.

### 3.1.4.6 Test points

A number of test pads are available on the PCB pf the reader to get access to the various voltages and important lines for measurement.

Voltage control lines:

- 5V3, 4V7, 3V3_MCU, GND, GND_DIG, $V_{APC2}$, ADC_In.

Signals Tx/Rx:

- OAD, OAD2.

SPI Signals:

- MISO, SDAT, SCLK, SEN_TUNE1, SEN_TUNE2, SEN_TUNE3.

AS3992 Signals:

- IRQ, EN_AS3992.

MCU Programming Interface:

- C2CK, C2D.

## 3.2 Control Unit Design

A control unit has been designed to add new features like Ethernet and RS-232 interfaces and I/O ports to the UHF RFiD reader device. PIC18F97J60 is used as a microcontroller unit from Microchip Technology Inc. for embedded applications. It has IEEE 802.3 compatible Ethernet controller, low-power and high-speed CMOS flash technology. PIC18F97J60 was selected since the requirements of the project are satisfied by this MCU. The following Figure 3.46 shows the whole control unit device.  The main objective of the control unit is to bridge serial data comes from the RFiD reader to the Ethernet interface.

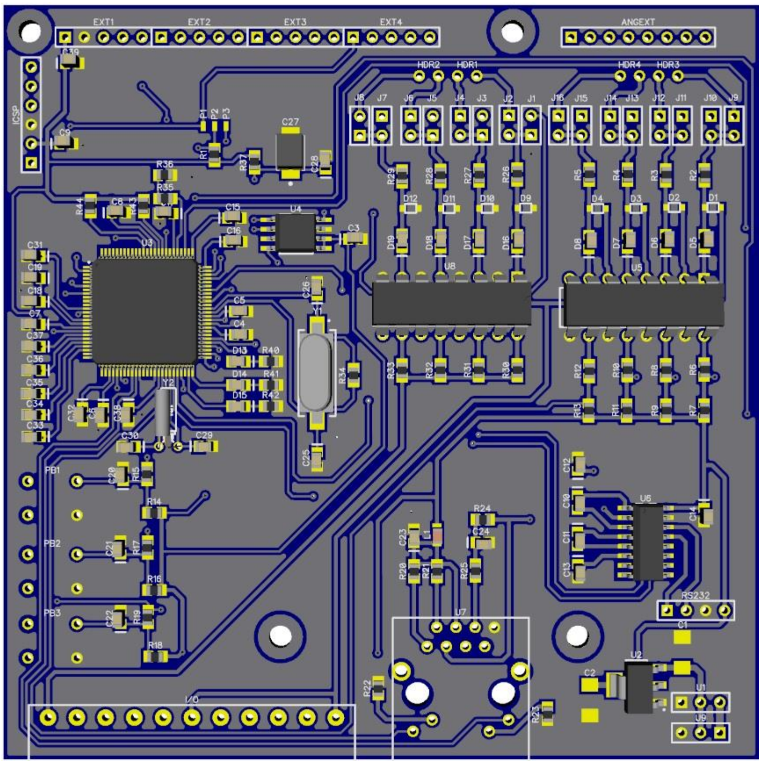

**Figure 3.46 :** Control unit.

### 3.2.1 Ethernet interface section

The control unit has the ability to provide Ethernet and RS-232 interface. It is possible to connect the control unit to the various platforms via these interfaces. It is really easy to communicate with the host computers via Ethernet interface by using just an Ethernet cable. There is a graphical user interface embedded in to the flash memory of the device that enables the users to interact with the control unit more easily and conveniently. It is possible to change device parameters such as IP, MAC and DNS addresses. All the data communication is provided by Ethernet connection. Ethernet interface section is presented in Figure 3.47.

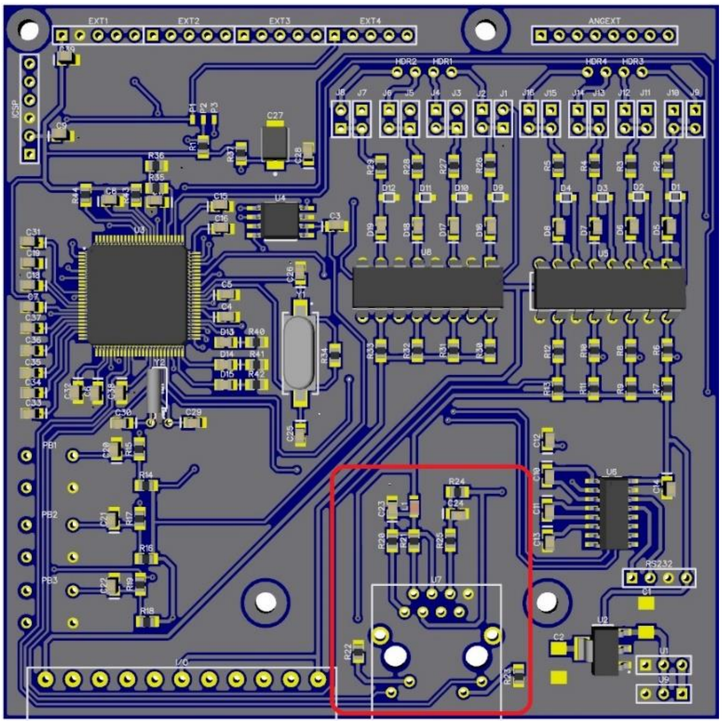

**Figure 3.47 :** Ethernet interface section of control unit.

### 3.2.2 RS-232 interface section

RS-232 interface enables serial communication with the host computer. It is possible to change and monitor fundamental options of the device like IP and MAC addresses via serial interface. RS-232 interface section is presented in Figure 3.48.

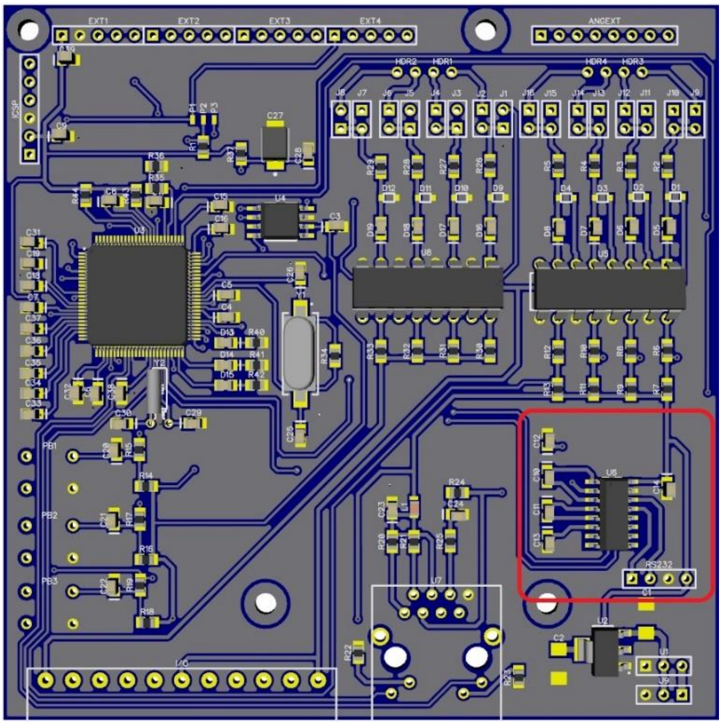

**Figure 3.48 :** RS-232 interface section of control unit.

### 3.2.3 I/O section

There are four opto-isolated digital inputs and four digital outputs for the communication between the control device and the outside world. Inputs are the signals or data received by the system, outputs are the signals and data sent from it. The operation status of the I/Os are indicated by LEDs placed next to the I/O unit. I/O unit section is presented in Figure 3.49.

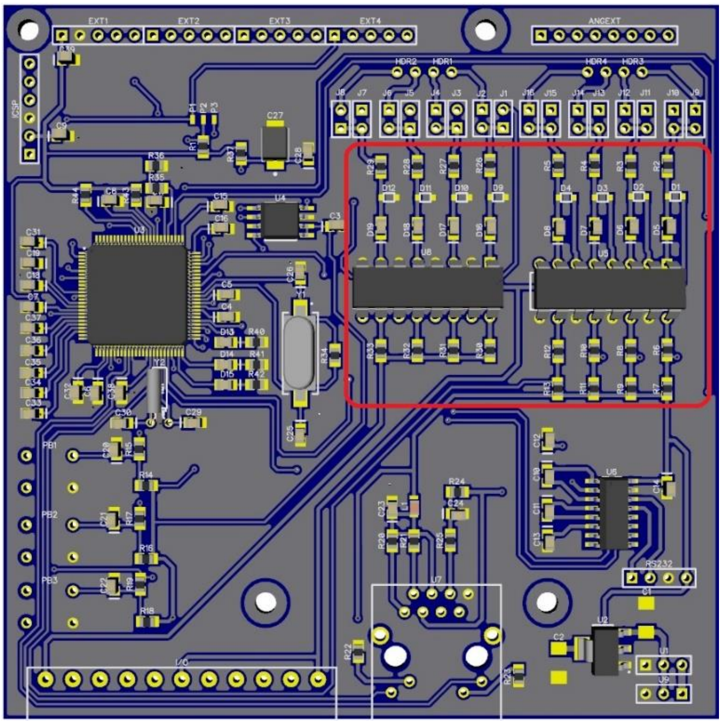

**Figure 3.49 :** I/O section of control unit.

## 3.3 RF Multiplexer Design

This multiplexer circuit was designed in order to increase the number of antenna output ports of UHF RFiD reader for dense antenna applications like smart shelves, library management systems etc. It has single pole double throw RF switch ICs for the operation of multiplication. It has the capability of working in wideband applications from 10 MHz to 4 GHz. However, in this project, the device is used at UHF band as the related applications of RFiD operate in this band (860 – 960 MHz). The device has its own microcontroller unit for performing the operations automatically and processing the inputs to control the antenna channel selection. As indicated, two selectable options are ready for switching operation. It is possible to control the switching frequency and antenna channel selection both via microcontroller and inputs from outside the world. The second option is available for the digital output ports of other devices such as RFiD readers, PLCs, I/O modules, servers etc. The device has also another feature of connecting each other as a cascaded structure. It is possible to connect the RF multiplexer devices with extension cables for the operation of multiple structure.

### 3.3.1 Schematic of RF multiplexer

The designed circuit comprises three RF switch ICs in a cascaded structure shown in Figure 3.50. Antenna switching operation is performed via control inputs of the ICs. Required control voltages are supplied by microcontroller or digital inputs from other devices as shown in Figure 3.51. The truth table for the switching operation is shown in Table 3.2. There are also a regulator part for voltage supply and a line extension part for cascaded system connection. In the digital part of the system, opto-isolated inputs and outputs were used to isolate the internal circuitry from the outside world input voltages. There are also indicators (LEDs) to show the active operation channel. The complete system PCB layout is shown in Figure 3.52.

**Table 3.2 :** Truth table of RF multiplexer.

| V1 | V2 | Signal Path |
|---|---|---|
| 0 | 0 | RFC to RF1 |
| 0 | 1 | RFC to RF2 |
| 1 | 0 | RFC to RF3 |
| 1 | 1 | RFC to RF4 |

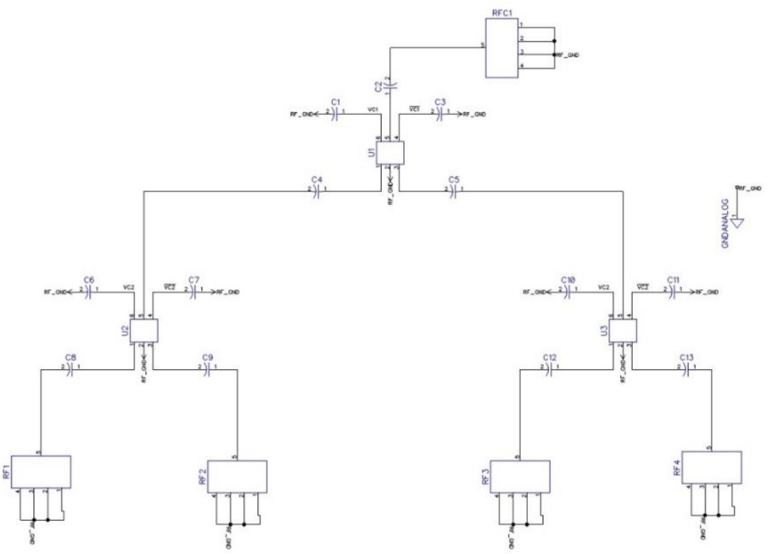

**Figure 3.50 :** Schematic of RF multiplexer RF part.

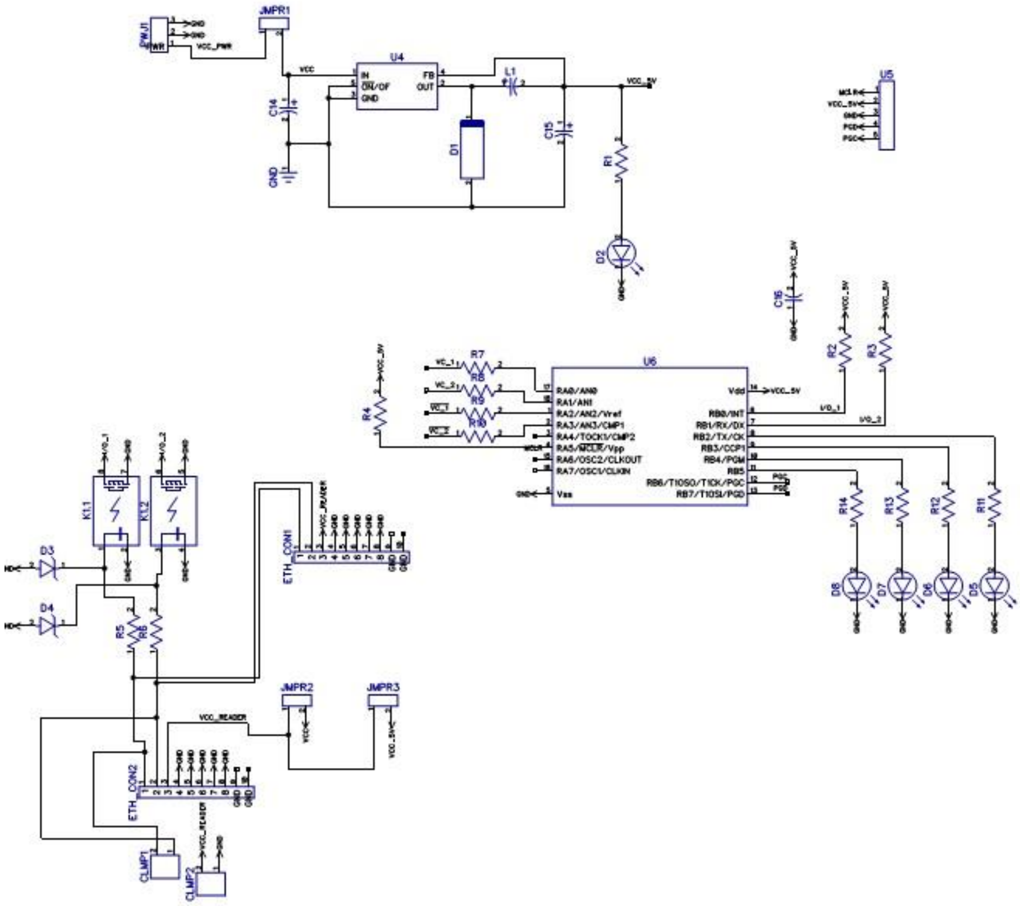

**Figure 3.51 :** Schematic of RF multiplexer digital part.

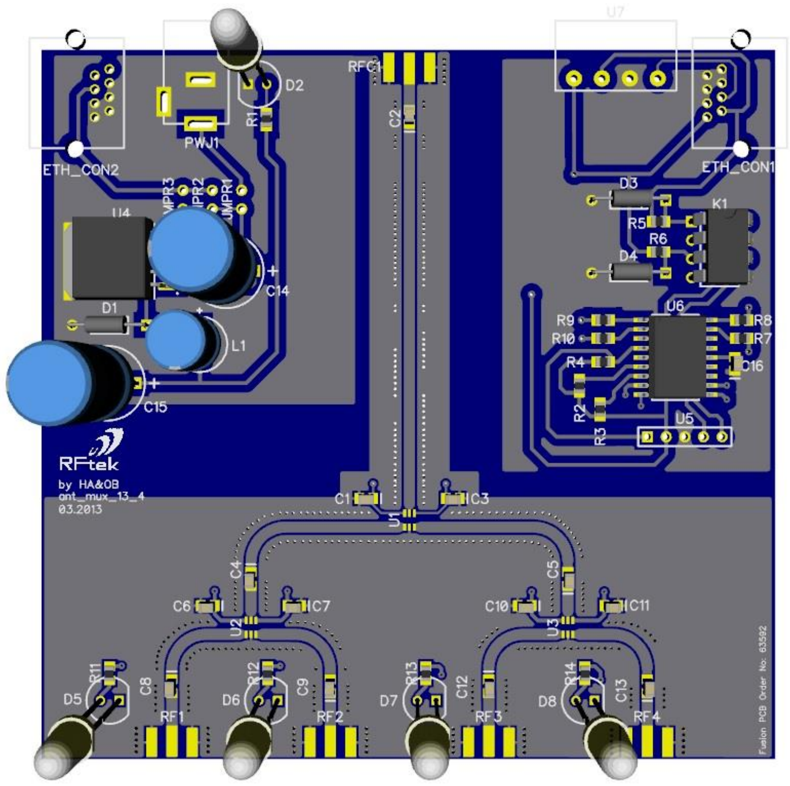

**Figure 3.52 :** RF multiplexer.

This multiplexer device is compatible with the all industrial UHF RFiD readers and antennas. It has been designed as a universal product, which has the capability of operating with all the readers from any brand.

It could be used for multiple antenna applications to reduce the cost of system implementation. Since the device increases the number of antenna outputs, it eliminates the need of using extra readers. Instead of purchasing a new reader, it is enough to use this RF multiplexer device for antennas more than the number of outputs of the reader.

### 3.3.2 Simulation and measurement results

For the implementation of system, measurements and simulations were performed to check the stability and losses. As a single unit, firstly, one of the RF switch ICs is simulated and its insertion loss was measured as 0.48 dB shown in Figure 3.53. In real conditions, it was measured as nearly the same 0.55 dB shown in Figure 3.54. Return loss value is also presented in simulated result chart.

As a second objective, the RF switching system designed in AWR Microwave Office to get the insertion loss of the whole system. The simulated measurement result and the real conditions' result are 1.05 dB and 1.3 dB respectively. The results are presented in Figure 3.55 and 3.56 respectively. Return loss of the whole system is also presented in simulated result chart.

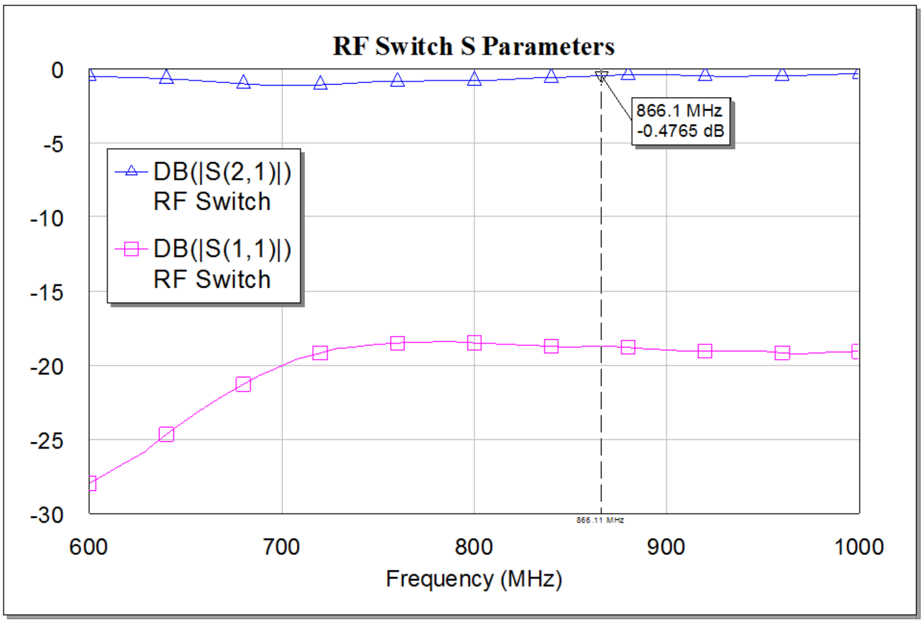


**Figure 3.53 :** Simulated insertion loss of RF switch IC.

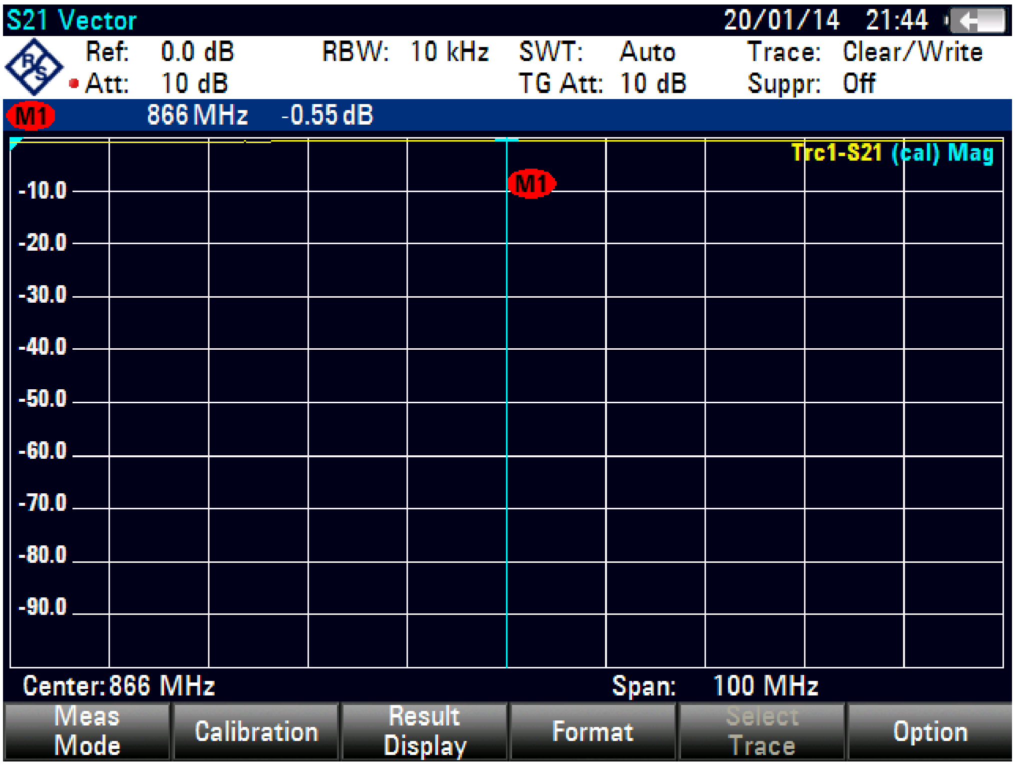


**Figure 3.54 :** Measured insertion loss of RF switch IC.

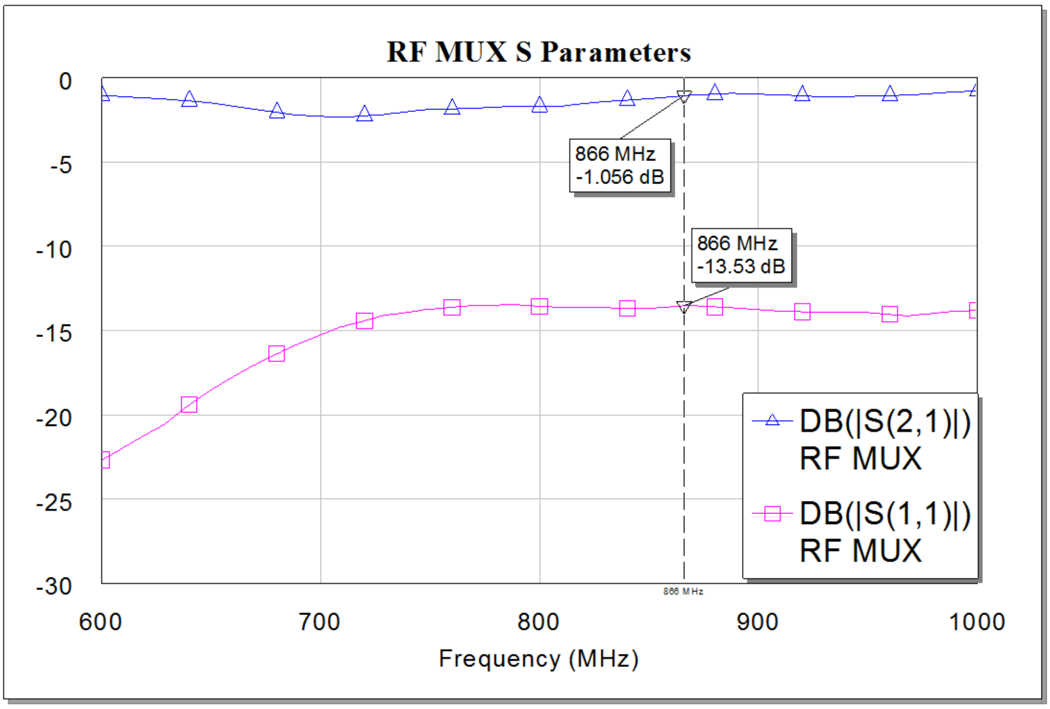


**Figure 3.55 :** Simulated insertion loss of RF multiplexer.

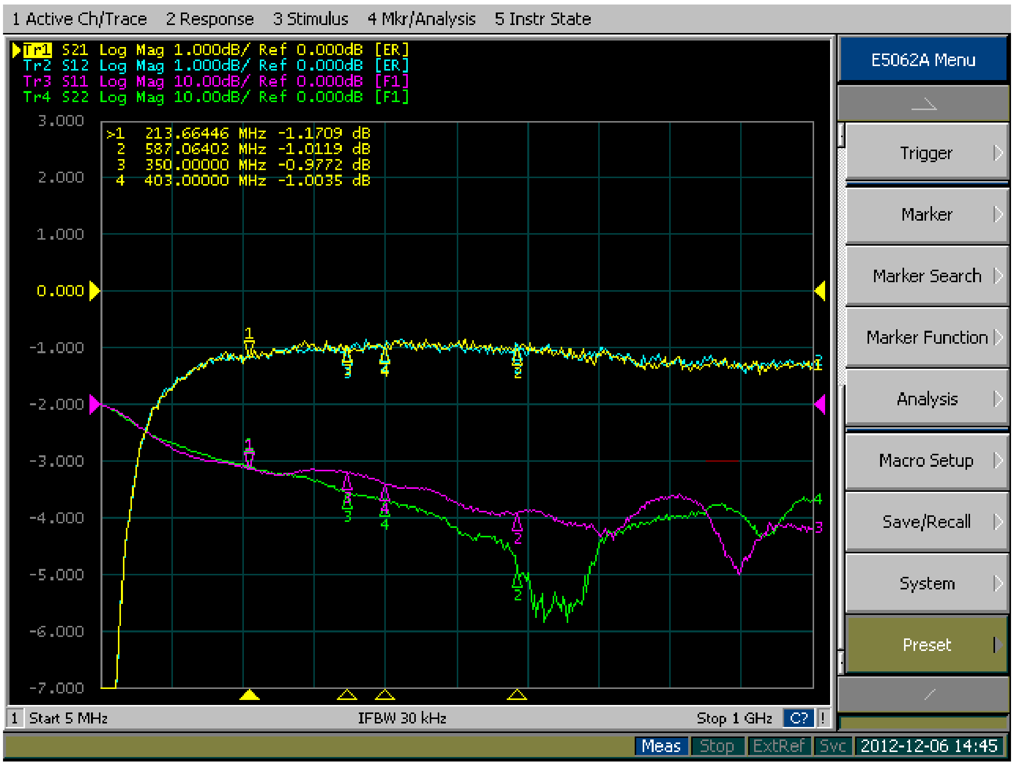


**Figure 3.56 :** Measured insertion loss of RF multiplexer.

# 5. CONCLUSIONS AND RECOMMENDATIONS

## 5.1 Conclusions

Within the scope of this thesis, a UHF RFiD reader and an RF multiplexer have been designed and manufactured. Reader device has various attractive features -low-cost, compact, long range and monostatic with extended read point capability- required by some industrial RFiD applications. RF multiplexer circuit adds the feature of multiple antenna operation for extended read point to the UHF RFiD reader. It increases the number of antenna output ports of the reader to lower the system implementation cost. Another hardware device has also been designed as a control unit to command the reader for fundamental operations and provide communication with the host computer via ethernet and RS-232 interface. The whole RFiD system, including UHF RFiD reader and control unit, and screen capture of tag read operation are shown in Figure 4.1 and Figure 4.2 respectively. To present the read point extension, UHF RFiD reader and RF multiplexer system with antennas is shown in Figure 4.3.

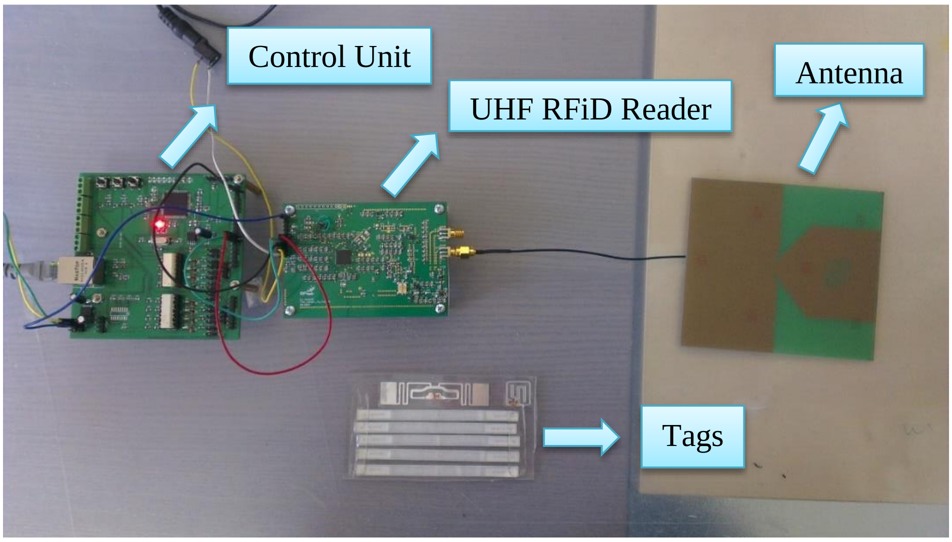


**Figure 4.1 :** A prototype RFiD system.

In this figure, a basic RFiD system is presented. The reader is connected to the control unit for communication with the host computer via ethernet interface. Antenna is the device used while tag read operation by means of electromagnetic waves. The tag read operation is also shown in the following figure captured from graphical user interface of the reader.

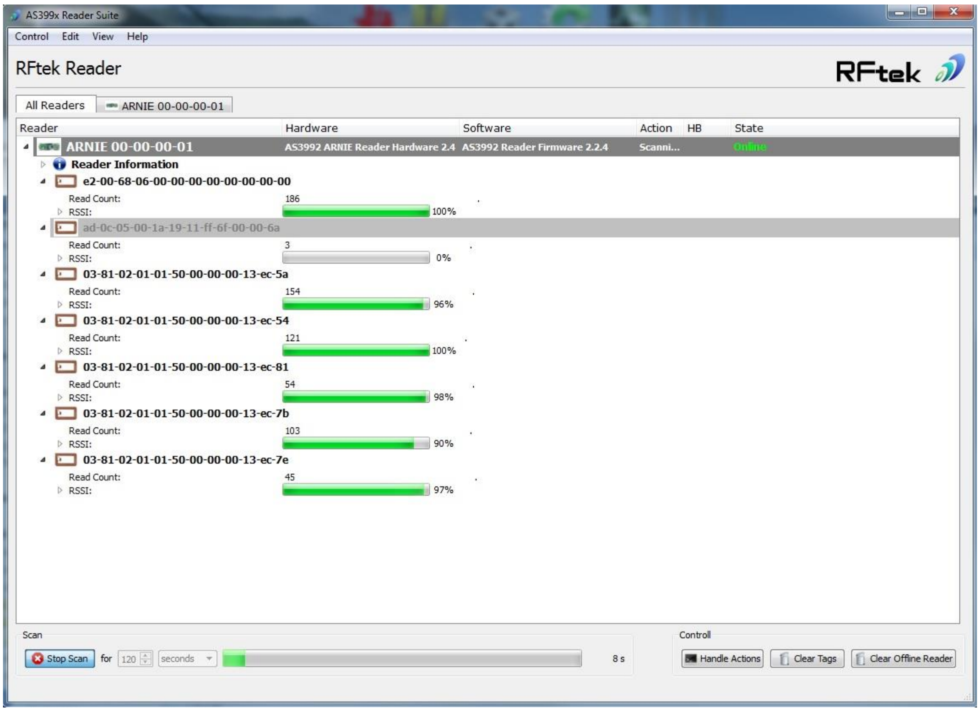


**Figure 4.2 :** Tag read operation.

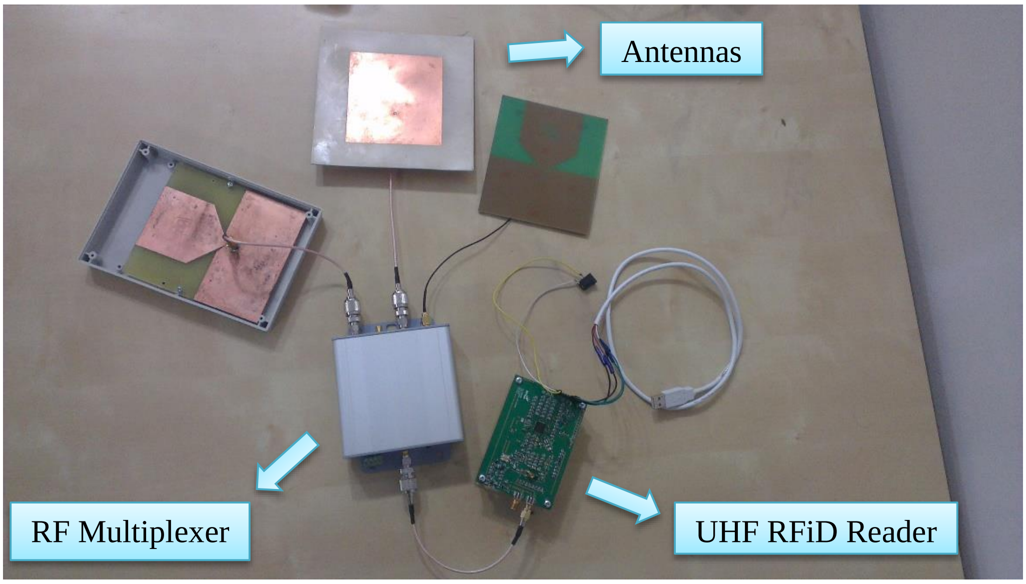


**Figure 4.3 :** UHF RFiD reaeder with RF multiplexer

In previous sections, first, the background of RFiD and key standards of it have been introduced, and then, some basic principles of electromagnetics of RFiD have been investigated for hardware development. Finally, last section before conclusion is the hardware design part of the study.

As a result of hardware design, some experimental graphs are presented in the following figures that show the output power of the reader. It is clear from Figure 4.4 that the maximum output power of the reader is nearly 22.3 dBm.

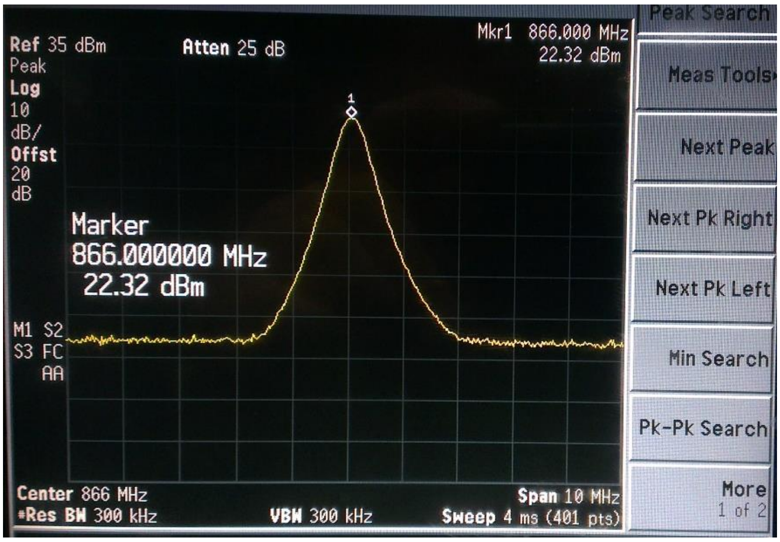


**Figure 4.4 :** Measured output power.

The expected value is 30 dBm, but because of the RF measurement instruments including RF extension cable, attenuator and RF SMA connectors there is almost 1 – 1.5 dB loss. Another reason for the loss is the components used after the output of the power amplifier. Low pass filter has an insertion loss of 1 dB, directional coupler has 0.3 dB, RF switch has 0.35 dB based on values in datasheet. The measurement results are already shown in Section 3. Based on the measurements, total insertion loss after power amplifier is 4.9 dB, including LPF (0.93 dB), coupler (3.42 dB) and RF switch (0.55 dB). On the other hand, in simulation results, the total insertion loss is nearly 1.8 dB shown in Figure 4.6. To perform the simulations, a circuit is designed in AWR Microwave Office covering the components of the reader after power amplifier section as shown in Figure 4.5. Moreover, rest part of the loss is caused because of the RF transmission lines.

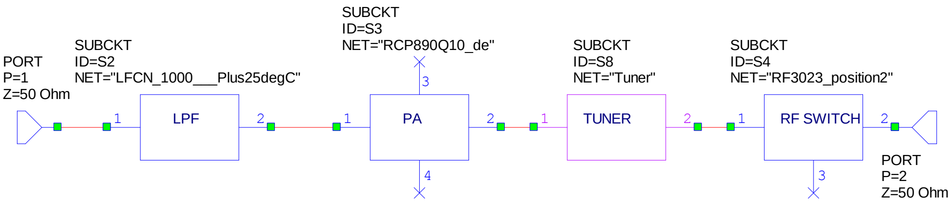


**Figure 4.5 :** Components after PA section.

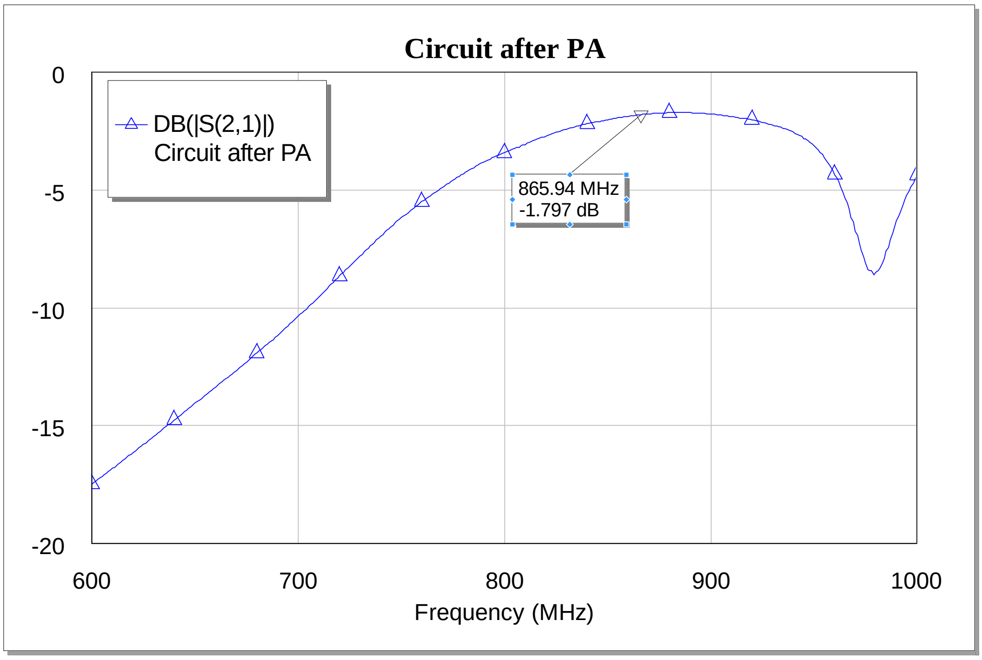


**Figure 4.6 :** Simulated insertion loss of Components after PA section.

For the measurement of the output power of UHF RFID reader, a spectrum analyzer from Agilent with a 20 dB attenuator is used. On the other hand, for insertion loss measurements a network analyzer from R&S is used. The test setups are shown in Figure 4.7 and Figure 4.8 respectively.

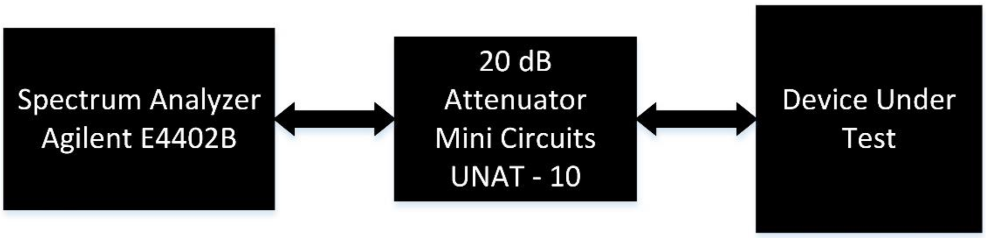


**Figure 4.7 :** Test setup with spectrum analyzer.

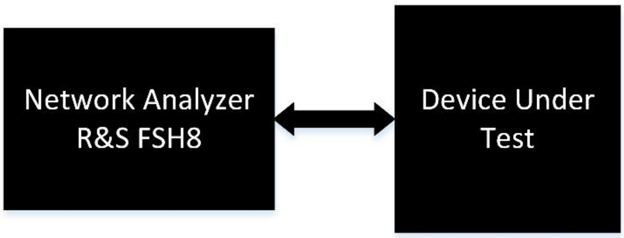


**Figure 4.8 :** Test setup with network analyzer.

Table 4.1 shows the difference between the expected and measured output power values. The losses are caused because of the RF measurement instruments, components used after PA and transmission lines as mentioned before.

**Table 4.1 :** Comparison between expected and measured output power values.

| Expected Output Power (dBm) | Measured Output Power (dBm) |
|---|---|
| 23 | 15.35 |
| 25 | 18 |
| 26 | 19 |
| 27 | 21 |
| 28 | 22.6 |
| 29 | 21.83 |
| 30 | 22.32 |

The designed and fabricated UHF RFID reader could be successfully used in any long range applications that the developers want.

## 5.2 Future Work

As a recommendation for future works, some new features could have the potentials to be added to the designed UHF RFiD reader and RF multiplexer.

- The number of antenna outputs could be increased for multiple antenna read zones.
- Some new wireless communication interfaces could be added for commanding the operations without wires.
- After the new architectural developments of reader ICs, system design costs could be reduced further.
- Instead of using microcontroller, microprocessors could be used for more effective operations.
- On the embedded software side, Low Level Reader Protocol (LLRP) could be used for universal usage regardless of reader brand.
- To increase the stability and security of the cascaded RF multiplexer circuit system, CAN based network could be used instead of traditional extension cables.

## REFERENCES


**Ahson, S. A., & Ilyas, M.** (2012). In *RFID Handbook: Applications, Technology, Security, and Privacy* (p. 478). CRC Press.

**AMS.** (2010). *AS3992_Datasheet_1V1.*

**Borisenko, A.** (2012). *Design and Implementation of an Augmented RFiD System.* Ottowa, Canada: School of Electrical Engineering and Computer Science, Faculty of Engineering, University of Ottowa.

**Dobkin, D. M.** (2008). *The RF in RFiD: Passive UHF RFiD in Practice.* Massachusetts, USA: Newnes.

**Feng, X., Wang, X., Zhang, X., Ge, B., Liu, S., Shen, J., . . . Liu, Y.** (2009). A Mobile UHF RFiD Reader with High Linearity Receiver. *International Conference on ASIC* (pp. 537-540). Changsha, Hunan: IEEE.

**Finkenzeller, K.** (2003). *RFID Handbook - Fundamentals and Applications in Contactless Smart Cards and Identification (2nd Edition).* West Sussex, England: John Wiley & Sons.

**Glover, B., & Bhatt, H.** (2006). In *RFiD Essentials* (p. 43). O'Reilly Media, Inc.

**Guo, Z.-j., & Ting-lei, H.** (2009). Design of UFH RFiD Reader Based on ARM. *Chinese Control and Decision Conference* (pp. 1394-1397). Guilin: IEEE.

**Hancke, G. P.** (2011). Practical eavesdropping and skimming attacks on high-frequency RFID tokens. *Journal of Computer Security, 19*(2), 259-288.

**Hansen, M., & Meissner, S.** (2007). *Identification and Tracking of Individuals and Social Networks using the Electronic Product Code on RFiD Tags.* Karistad: IFIP Summer School.

**Huusko, M.** (2009). *Embedded System for Networked Real-Time RFiD Reader.* Helsinki: Helsinki University of Technology.

**Juels, A., & Pappu, R.** (2003). Squealing Euros: Privacy Protection in RFiD-Enabled Banknotes. *Financial Cryptography. Lecture Notes in Computer Science*, 103-121.

**King, P. F.** (2010). *Patent No. 20100127876.* USA.

**Landt, J.** (2005). The History of RFiD. *IEEE Potentials*.

**Lee, S., Kwon, H., Ryu, C., Kim, S., Kang, K., Chun, S., . . . Nguyen, C.** (2012). A Complete Single-Chip Multi-Standard Dual-Mode CMOS RFiD Reader with Low Power Consumption. *Asia-Pacific Microwave Conference Proceedings* (pp. 268-270). Kaohsiung: IEEE.

**Lei, Q., Wang, G., & Wang, D.** (2011). Design of a handheld UHF RFiD reader for The Internet of Things. *International Conference on Computer and Management* (pp. 1-4). Wuhan: IEEE.

**Li, H., Mou, X., & Ji, Z.** (2009). A New Implementation of UHF RFiD Reader. *TENCON* (pp. 1-4). Singapore: IEEE.

**Li, H., Wang, H.-j., Shang, Z., Li, Q.-h., & Xiao, W.** (2010). Low-power UHF Handheld RFiD Reader Design and Optimization. *8th World Congress on Intelligent Control and Automation* (pp. 3068-3072). Jinan: IEEE.

**Li, M., & Wu, Y.-s.** (2011). Design of Radio Frequency Circuit of Reader Based on AS3990. *3rd International Conference on Communication Software and Networks* (pp. 274-277). Xi'an: IEEE.

**Mayordomo, I., Berenguer, R., Garcia-Alonso, A., Fernandez, I., & Gutierrez, I.** (2009). Design and Implementation of a Long-Range RFiD Reader for Passive Transponders. *Microwave Theory and Techniques, 57*(5), 1283-1290.

**McFarlane, D.** (2006). *Networked RFiD in Industrial Control: Current and Future.* University of Cambridge, Cambridge, UK: Auto-ID Labs Whitepaper.

**Nakao, S., Norimatsu, T., Yamazoe, T., Oshima, T., Watanabe, K., Minatozaki, K., & Kobayashi, Y.** (2011). UHF RFiD Mobile Reader for Passive and Active Tag Communication. *Radio and Wireless Symposium* (pp. 311-314). Phoenix, AZ: IEEE.

**Narayanaswamy, G.** (2009). *Blocking Reader: Design and Implementation of a Passive UHF RFiD Blocking Reader.* Texas: The University of Texas at Arlington.

**Narayanaswamy, G., Jagannatha, S. K., & Engels, D. W.** (2010). Blocking Reader:Design and Implementation of a Low-Cost Passive UHF RFiD Blocking Reader. *International Conference on RFiD* (pp. 274-281). Orlando, FL: IEEE.

**Natarajan, B.** (2009). *Impact of RFiD Physics on Airport Baggage Handling System: A Simulation Study.* San Antonio: The University of Texas at San Antonio.

**Pang, X., Yao, X., Liang, C. P., & Hong, W.** (2008). Design and Realization of a Highly Integrated UHF RFiD Reader Module. *Microwave and Millimeter Wave Technology* (pp. 1503-1505). Nanjing: IEEE.

**Park, C.-w., Choi, G.-y., Chae, J.-s., & Kim, B.-g.** (2009). A Design for Passive RFiD System on a Chip. *International Conference on Advanced Communication Technology* (pp. 836-839). Phoenix Park: IEEE.

**Peregrine Semiconductor Corp.** (2012). *pe4259ds.*

**Pursula, P., Kiviranta, M., & Seppa, H.** (2009). UHF RFiD Reader With Reflected Power Canceller. *Microwave and Wireless Components Letters, 19*(1), 48-50.

**Robledo, J. C.** (2010). *How to Design a Low Cost UHF RFiD Reader.* Helsinki, Finland: Helsinki Metropolia University of Applied Sciences.

**Song, J.-M., Wang, G.-B., & Xiao, B.-C.** (2012). Design of UHF RFiD Reader Based on Embedded Linux. *4th International Conference on Computational and Information Sciences* (pp. 1001-1004). Chongqing: IEEE.

**Sorrells, P.** (1998). *Passive RFiD Basics.* Microchip Technology Inc.

**Sweeney II, P. J.** (2005). *RFiD for Dummies.* Hoboken, NJ: Wiley Publishing Inc.

**Tang, C.-p., Tang, Z.-y., Yang, Y.-h., & Zhan, Y.-j.** (2010). Design of UHF RFiD Reader Based on AS3991. *International Conference on RFID-Technology and Applications* (pp. 222-226). Guangzhou, China: IEEE.

**Thornton, F., & Haines, B.** (2006). *RFID Security: Protect the Supply Chain.* Massachusetss, USA: Syngress.

**Viasystems Group, Inc.** (2011). *Controlled Impedance Designs.*

**Wang, W., Lou, S., Chui, K. W., Rong, S., Lok, C. F., Zheng, H., . . . Tsui, C. Y.** (2008). A Single-Chip UHF RFiD Reader in 0.18 um CMOS Process. *IEEE Journal of Solid-State Circuits, 43*(8), 1741-1754.

**Weis, S. A.** (n.d.). *RFiD: Principles and Applications.* Bostan, MA: MIT CSAIL.

**Wnag, J., Zhang, C., & Wang, Z.** (2010). A Low Power Low Cost Fully Integrated UHF RFiD Reader with 17.6dBm Output P1dB in 0.18 μm CMOS Process. *Radio Frequency Integrated Circuits Symposium* (pp. 109-112). Anaheim, CA: IEEE.

**Xia, H., Wu, J., Xiao, B., Zan, X., & Wang, G.** (2012). Design of UHF RFiD Reader and the Solution of Crosstalk Problems. *Internatioanl Conference on Computational Problem-Solving* (pp. 212-217). Leshan: IEEE.

**Ye, L., Liao, H., Song, F., Chen, J., Xiao, H., Liu, R., . . . Wang, Y.** (2008). A 900MHz UHF RFiD Reader Transceiver in O.18um CMOS Technology. *Solid-State and Integrated-Circuit Technology* (pp. 1569-1572). Beijing: IEEE.

**Yi, K., Kim, H., Kim, J., Kim, J., Cho, J., An, K., & Kim, S.** (2008). Implementation of HF/UHF Multiband RFiD Reader SiP with Package-on-Package Technology. *Electrical Design of Advanced Packaging and Systems Symposium* (pp. 65-68). Seoul: IEEE.

**Ying, C., & Fu-hong, Z.** (2008). A System Design for UHF RFiD Reader. *Communication Technology* (pp. 301-304). Hangzhou: IEEE.

**Zhang, P.-c., & Ma, G.-f.** (2010). Design of Passive RFiD Reader Based on Mobile Phone. *2nd International Conference on Networks Security Wireless Communications and Trusted Computing* (pp. 446-449). Wuhan, Hubei: IEEE.

**Zimu, T.** (2010). *RFiD Systems and Applications in Positioning.* Mikkeli, Finland: Mikkeli University of Applied Sciences.

**Anderson, N.** (2006, March 15). *RFiD chips can carry viruses.* Retrieved October 16, 2013, from Ars Technica : http://arstechnica.com/uncategorized/2006/03/6386-2/

**Collins , J.** (2004, July 19). *RFiD for Meat Eaters.* Retrieved October 16, 2013, from RFiD Journal: http://www.rfidjournal.com/articles/view?1036

**EPCglobal.** (2006, June 21). *Reader Protocol Standard, Version 1.1.* Retrieved October 13, 2013, from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.186.2436&rep=rep1&type=pdf

**EPCglobal.** (2010, October 13). *Low Level Reader Protocol.* Retrieved October 14, 2013, from The Global Language of Businesss: http://www.gs1.org/gsmp/kc/epcglobal/llrp/llrp_1_1-standard-20101013.pdf

**EPCglobal Inc.** (2008, October 23). *Class 1 Generation 2 UHF Air Interface Protocol Standard "Gen 2".* Retrieved October 13, 2013, from The Global Language of Business: http://www.gs1.org/gsmp/kc/epcglobal/uhfc1g2/uhfc1g2_1_2_0-standard-20080511.pdf

**EPCglobal Inc.** (n.d.). *EPCglobal*. Retrieved October 13, 2013, from The Global Language of Business: http://www.gs1.org/epcglobal

***How to clone a biometric passport while it's still in the bag. Mail exposes the postal vulnerability.*** (2007, March 6). Retrieved October 16, 2013, from The Register: http://www.theregister.co.uk/2007/03/06/daily_mail_passport_clone/

**McCullagh, D., & Broache, A.** (2005, October 25). *Passports to get RFiD chip implants.* Retrieved October 16, 2013, from CNET: http://news.cnet.com/Passports-to-get-RFID-chip-implants/2100-7348_3-5913644.html

**O'Connar, M. C.** (2009, March 18). *Dash7 Alliance Seeks to Promote RFiD Hardware Based on ISO 18000-7 Standard.* Retrieved October 13, 2013, from RFiD Journal: http://www.rfidjournal.com/articles/view?4696

***Radio Silence.*** (2007, June 7). Retrieved October 16, 2013, from The Economist: http://www.economist.com/node/9249278

***RFiD Network Launches TV Series.*** (2012, July 11). Retrieved October 16, 2013, from The RFiD Network: http://rfid.net/news/362-the-rfid-network-tv-series

***RFiD Privacy and Security*.** (n.d.). Retrieved October 16, 2013, from RSA Laboratories: http://www.emc.com/domains/rsa/index.htm?id=2115

***RFiD Security & Privacy Lounge*.** (n.d.). Retrieved October 16, 2013, from GSI Information Security Gruoup: http://avoine.net/rfid/

***RFiD Technology Transforming Food Retailers Like Wal-Mart.*** (2010, March 18). Retrieved October 16, 2013, from Seeking Alpha: http://seekingalpha.com/article/194466-rfid-technology-transforming-food-retailers-like-wal-mart

***Speedpass*.** (n.d.). Retrieved October 16, 2013, from Speedpass: https://www.speedpass.com/spMyAccount/xhtml/frmSpHome.xhtml

**Sterling, B.** (2006, November 17). *RFID Passports cracked. Easily, cheaply, and quickly.* Retrieved October 16, 2013, from Wired: http://www.wired.com/beyond_the_beyond/2006/11/arphid_watch_fi/

**Tedjasaptura, A.** (2007, February 26). *Putting RFID Network Security in Perspective.* Retrieved October 16, 2013, from RFiD Asia: http://www.rfid-asia.info/2007/02/putting-rfid-network-security-in.htm

**Thomson, I.** (2009, February 3). *Hacker clones passports in drive-by RFID heist.* Retrieved October 16, 2013, from V3.co.uk: http://www.v3.co.uk/v3-uk/news/1953428/hacker-clones-passports-drive-rfid-heist

**Vries, A. D., & Dietrich, P.** (2007, September). *Standards Facilitate RFID Adoption.* Retrieved October 14, 2013, from rfdesign.com: http://defenseelectronicsmag.com/site-files/defenseelectronicsmag.com/files/archive/rfdesign.com/mag/709RFDEf1.pdf

## APPENDICES

**APPENDIX A:** Datasheets of used components and PCB material

**APPENDIX A:** Datasheets of used components and PCB material

AS3992 (Reader IC):
http://www.ams.com/eng/acceptpolicy/information/46223/525896/18677 **(A 1.1)**

AS1364 (LDO):
http://www.ams.com/eng/content/download/1961/15107/1937 **(A 1.2)**

PE4259 (RF Switch):
http://www.psemi.com/pdf/datasheets/pe4259ds.pdf **(A 1.3)**

SKY6511(Power Amplifier):
http://www.skyworksinc.com/uploads/documents/200428E.pdf **(A 1.4)**

PCB Material:
http://www.piu-printex.at/printex/multilayer%20de-104ml-1105d.pdf **(A 1.5)**

**CURRICULUM VITAE**

**Name Surname:** Özgür BOSTAN

**Place and Date of Birth:** Istanbul, 29.02.1988

**Address:** Emanet Sok. No:29/16 Bostanci-Kadıkoy/ISTANBUL

**E-Mail:** ozgbostan@gmail.com

**B.Sc.:** Maltepe University, Faculty of Engineering, Department of Electronics Engineering **(2006 - 2010)** (Full scholarship)

**Professional Experience and Rewards:**

RFtek Electronics **(05.2012 - present)**
-Co-Founder, Electronics R&D Engineer
-R&D activities in RF (Radio Frequency) circuits and hardware design of electronic devices.

Bits Computer Ltd. **(03.2011 - 02.2012)**
-Electronics R&D Engineer, responsible for R&D activities on electronic devices (especially RFiD applications)
-RFiD system design and implementation

T.C. Maltepe University **(03.2010 - 06.2010)**
-Student Assistant, responsible for assisting electronics lab courses with research assistants

Bits Computer Ltd. **(10.2009 - 03.2010)**
-R&D Engineer, responsible for RFiD system components and electronic devices design

**List of Publications and Patents:**

Smart Shelf Capable of Inventory Management (Patent pending)
-This patent is about a smart shelf, which is capable of performing promotion activities of RFiD tag attached goods and inventory management by using RFiD technology.