UNIVERSITY OF NAIROBI

Department of Electrical and Information Engineering

Interference Cancellation in Radio Frequency Identification (RFID) Systems

Project Number: 022

By: Njoroge Joseph Ngoiyo- F17/0757/2010

Supervisor: Prof. Vitalice K. Oduol

Examiner: Prof. H. A. Ouma

A Project submitted as a partial fulfillment for the requirement for the award of the degree of
BACHELOR OF SCIENCE IN ELECTRICAL AND ELECTRONIC ENGINEERING
of the University of Nairobi

Project Re-submitted On: 28th April 2015
Declaration of Originality

College: Architecture and Engineering
Faculty/School/Institute: Engineering
Department: Electrical and Information Engineering
Course: Bachelor of Science in Electrical and Electronic Engineering
Registration Number: F17/0757/2010
Name of Student: Njoroge Joseph Ngoiyo
Title of Work: Interference Cancellation in Radio Frequency Identification (RFID) Systems

1. I understand what plagiarism is and I am aware of the University policy in this regard.
2. I declare that this final year project report is my original work and has not been submitted elsewhere for examination, award of a degree or publication. Where other people’s work or my own work has been used, this has properly been acknowledged and referenced in accordance with the University of Nairobi’s requirements.
3. I have not sought or used the services of any professional agencies to produce this work.
4. I have not allowed, and shall not allow anyone to copy my work with the intention of passing it off as his/her own work.
5. I understand that any false claim in respect of this work shall result in disciplinary action, in accordance with University anti-plagiarism policy.

.................................................. ..................................................
Signature Date
Abstract
Maximizing the efficiency of Radio Frequency Identification (RFID) systems is one of the main challenges in application domains, such as logistics and supply chain management, where the undesired effect of interference can significantly degrade the speed of the inventory process.

In RFID systems, a problem arises when one or several noise signals that are external to the system are present within the frequency band of the system during a read operation. Such interference will often cause misidentification of items and fault reporting in the RFID system. Increasingly, such interference is being caused by other RFID readers and/or transponders located near the system-of-interest that operate within the same or similar frequency band.

In this project, RFID systems and interference in RFID systems are studied. Interference is demonstrated using Gaussian noise and its cancellation also designed and demonstrated using Quadrature Amplitude Modulation, with the aim of improving performance in RFID readers.
Acknowledgement

Greatest appreciation to God Almighty for the grace He bestowed me during the treacherous five years in Engineering School. For my supervisor, Professor V. K. Oduol, I cannot thank you enough for all the guidance you have given me throughout the projects’ period, and for nurturing my interest in telecommunications as my professor for the unit in fourth year.

To all the staff and students of the department, I would not have made it through the five years without your input. You are invaluable.

Also importantly, my friends’ and family’s support and encouragement has been unparalleled, you are appreciated.
Dedication
To my future wife, sons and daughters. Were it not for your well-being, I would not have labored this much.
## Table of Contents

Declaration of Originality ........................................................................................................... 1
Abstract ........................................................................................................................................ 2
Acknowledgement ........................................................................................................................ 3
Dedication ...................................................................................................................................... 4
List of Figures ............................................................................................................................... 7
Chapter One ................................................................................................................................. 8

Introduction ................................................................................................................................... 8

1.1: Problem Statement ............................................................................................................... 8
1.2: Objectives ............................................................................................................................. 8
  1.2.1: Overall objective ............................................................................................................. 8
  1.2.2: Specific Objectives ......................................................................................................... 8
1.3: Project Justification ............................................................................................................. 8
1.4: Scope of work ....................................................................................................................... 8
1.5: Organisation of the Report ................................................................................................. 9

Chapter Two ............................................................................................................................... 10

Literature Review ........................................................................................................................ 10

2.1: Overview of Automatic Identification Systems ................................................................ 10
  2.1.1: Barcodes ......................................................................................................................... 11
  2.1.2: Optical Character Recognition (OCR) ......................................................................... 11
  2.1.3: Biometric Procedures ................................................................................................... 11
  2.1.4: Smart Cards .................................................................................................................. 12
  2.1.5: RFID Systems .............................................................................................................. 13
2.2: Components of an RFID system ....................................................................................... 13
  2.2.1: RFID Reader ................................................................................................................ 13
  2.2.2: RFID Tag ..................................................................................................................... 17
2.3: Working of an RFID system ............................................................................................... 23
  2.3.1: Forward Power transfer ................................................................................................ 25
  2.3.2: Data transfer between a tag and a reader .................................................................... 28
  2.3.3: UHF Reader Electronic Circuitry ................................................................................ 32
  2.3.4: RFID Power Sources ................................................................................................ 34
  2.3.5: 1-Bit Transponder ....................................................................................................... 36
2.3.6: Full and Half Duplex Procedure .................................................................36
2.4: Interference and Interference Cancellation in RFID Systems .........................38
  2.4.1: Adjacent Channel Interference .................................................................39
  2.4.2: Band Congestion Interference .................................................................39
  2.4.3: Environmental Interference .....................................................................39
  2.4.4: Jamming .................................................................................................39
  2.4.5: Spurious emissions interference ...............................................................39

Chapter Three ........................................................................................................40
Methodology ............................................................................................................40
Chapter Four ...........................................................................................................46
Results and Analysis ...............................................................................................46
Chapter Five ...........................................................................................................50
Conclusion and Recommendations for Further Work ........................................50
References ..............................................................................................................51
List of Acronyms .....................................................................................................52
List of Figures
Figure 1: Overview of the most important auto-ID procedures ..................................................10
Figure 2: Block diagram of a reader constituting of a control system and RF interface ..........14
Figure 3: Block diagram of an RF interface for an inductively coupled RFID system ..........15
Figure 4: Block diagram of the control unit of a reader ............................................................16
Figure 5: Comparison of passive, semi-passive and active transponders .................................19
Figure 6: Forward Power Transfer ..............................................................................................25
Figure 7: Received power against distance for tag ......................................................................27
Figure 8: Functional blocks of an RFID reader ...........................................................................32
Figure 9: Power supply to an inductively coupled transponder from the energy of the magnetic
alternating field generated by the reader ..................................................................................35
Figure 10: Representation of full-duplex, half-duplex and sequential systems over time ........37
Figure 11: Block diagram for the whole circuit .........................................................................40
Figure 12: Simulation environment of the transmitter in Simulink ...........................................41
Figure 13: Simulation environment of the wireless channel in Simulink ..................................42
Figure 14: Simulation environment for passive RFID tag and Return Link .............................43
Figure 15: Simulation environment for the receiver block .........................................................44
Figure 16: Simulation of AWGN and its cancellation ..................................................................45
Figure 17: Output of the transmitter ............................................................................................46
Figure 18: Receiver Output ..........................................................................................................47
Figure 19: Signal with interference ..............................................................................................47
Figure 20: Signal after QAM .........................................................................................................48
Chapter One

Introduction

1.1: Problem Statement
With continuous increase in uptake of RFID systems in identification of various objects, there is increasing need to make efficient systems. Use of multiple RFID readers and tags in one establishment will often result in interference that this project aims to cancel out.

1.2: Objectives

1.2.1: Overall objective
To design and demonstrate interference cancellation for performance improvement in RFID systems

1.2.2: Specific Objectives
- Study RFID systems and their functionality
- Study Sources and Nature of interference in RFID systems
- Design and demonstrate interference in RFID systems using Simulink
- Design and demonstrate cancellation of this interference using Simulink
- Determine extent of performance improvement in RFID readers as a result of the interference cancellation designed above

1.3: Project Justification
Many multinational retail stores, defense departments, transport industries among others, are increasingly taking up RFID as the optimal identification technology due to its multiple advantages over other forms of automatic identification systems in existent. There is need for efficient systems that are free of interference that may result in false alarm or false dismissal of the objects to be identified.

1.4: Scope of work
The focus of the project will be:
- Illustrating the functionality of an RFID system
- Demonstrating interference for an RFID system by introducing AWGN using a Random Number Generator
- Designing and demonstrating cancellation of this interference using Quadrature Amplitude Modulation
1.5: Organisation of the Report
A literature review of a RFID reader, RFID tag, their functionality and the wireless link between them is presented in chapter 2.

In chapter 3, the methodology of the project has been explained. The chapter begins with the simulation of RFID reader transmitter section, passive tag and return link of the system and the RFID reader receiver. Interference has also been simulated in this section by introducing AWGN from a Random Number Generator. Finally, for this chapter, DSB QAM has been incorporated to cancel out this interference.

Chapter 4 incorporates the results obtained using Simulink. The results are analysed and discussed in this chapter.

Lastly, conclusion and recommendations for future works are given in chapter 5
Literature Review

2.1: Overview of Automatic Identification Systems
In recent years, automatic identification (Auto-ID) procedures have become very popular in many service industries, purchasing and distribution logistics industry, manufacturing companies and material flow systems. The best solution to the problems of common auto-ID procedures is storage of data in a silicon chip, with the most common form of electronic data-carrying devices in use being the smart card based upon a contact field (telephone smart card, bank cards etc.) [1] However, the mechanical contact used in the smart card is the often impractical. A contactless transfer of data between the data-carrying device and its reader is far from flexible.

The overview of the auto-ID procedures is shown in figure 1 below:

![Figure 1: Overview of the Most Important Auto-ID Procedures](image)
The RFID market belongs to the fastest growing sector of the radio technology industry including:

- Security/Access control
- Asset management
- Transportation
- Supply chain management
- Point of sale
- Rental item tracking
- Toll collection
- Automobile immobilizers
- Baggage handling
- Animal tracking
- Real time location system

2.1.1: Barcodes
Consists of binary code comprising a field of bars and gaps arranged in a parallel configuration. The sequence, made up of wide and narrow bars and gaps, can be interpreted numerically and alphanumerically. It is read by optical laser scanning, i.e. by the different reflection of a laser beam from the black bars and white gaps. [1]

2.1.2: Optical Character Recognition (OCR)
Special fonts developed for this application that use stylized characters so that they could be read both in the normal way by the people and automatically by machines. They have an advantage of high density of information and the possibility of reading data usually in an emergency, or simply for checking.

Today, OCR is used in production, service and administrative fields, and also in banks for the registration of cheques. However, OCR systems have failed to become universally applicable because of their high price and the complicated readers that they require in comparison with other identification procedures. [1]

2.1.3: Biometric Procedures
Biometric identification is the science of counting and body measurement procedures involving living things. The system identifies people by comparing unmistakable and individual physical characteristics. They include finger printing and hand-printing procedures, voice identification and retina or iris identification.

2.1.3.1: Voice identification
The technology identifies individuals using speaker recognition. The user talks into a microphone linked to a computer. The equipment converts the spoken word into digital signals, which are evaluated by the identification software. The identification is achieved by checking the speech characteristics of the speaker against an existing reference pattern. If they correspond, then a reaction, such as opening a door, can be initiated.
2.1.3.2: Finger Printing
This type of identification is based on the comparison of papillae and dermal ridges of the finger tips, which can be obtained not only from the finger itself, but also from objects that the individual in question has touched. When fingerprinting procedures are used for personal identification, usually for entrance procedures, the figure tip is placed upon a special reader. The system calculates a data record from the pattern it has read and compares this with a stored reference pattern. In order to prevent violent frauds, fingerprint ID systems have even been developed that can detect whether the finger placed on the reader is that of a living person. [1]

2.1.4: Smart Cards
It’s an electronic data storage system, possibly with an additional computing capacity (microprocessor card), which- for convenience- is incorporated into a plastic card the size of a credit card. Smart cards are placed in a reader, which makes a galvanic connection to the contact surfaces of the smart card using contact springs. The smart card is supplied with energy and a clock pulse from the reader via the contact surfaces. Data transfer between the reader and the card takes place using bidirectional serial interface (I/O port).

A primary advantage of the smart card is the fact that the data stored in it can be protected against undesired access and manipulation. The smart cards make all services that relate to information or financial transactions per simpler, safer and cheaper.

One disadvantage of contact-based smart cards is the vulnerability of the contacts to wear, corrosion and dirt. Readers that are used frequently are expensive to maintain due to their tendency to malfunction. In addition, readers that are accessible to the public (e.g. telephone boxes) cannot be protected against vandalism.

2.1.4.1: Memory cards
In memory cards, the memory-usually an EEPROM- is accessed using a sequential logic (state machine). It is also possible to incorporate simple security algorithms, e.g. stream ciphering, using this system. [1] Flexibility of application is highly limited, but on the positive side, memory cards are very cost-effective.

2.1.4.2: Microprocessor cards
They contain a microprocessor which is connected to a segmented memory (ROM, RAM and EEPROM segment). The mask programmable ROM incorporates an operating system for the microprocessor and is inserted during chip manufacture. The contents of the ROM are determined during manufacturing, and are identical for all microchips from the same production batch, and cannot be overwritten.

The chip’s EEPROM contains application data and application-related programme code. Reading from or writing to this memory area is controlled by the operating system. The RAM is the microprocessor’s temporary working memory. Data stored in the RAM are lost when the supply voltage is disconnected.

Microprocessor cards are very flexible. In modern smart card systems, it is also possible to integrate different applications in a single card (multi-application) [1]. The application-specific parts of the programme are not loaded into the EEPROM until further manufacture and can be
initiated via the operating system. Microprocessor cards are primarily used in security-sensitive applications.

2.1.5: RFID Systems

They are closely related to smart cards. Data is stored on an electronic data-carrying device called the tag. However, unlike the smart cards, the power supply to the data-carrying device and the data exchange between the data-carrying device and the reader are achieved without use of galvanic contacts, using instead magnetic fields.

The comparison of different automatic identification systems is shown in the table below:

<table>
<thead>
<tr>
<th>System Parameter</th>
<th>Barcode</th>
<th>OCR</th>
<th>Voice Recognition</th>
<th>Biometry</th>
<th>Smart Card</th>
<th>RFID Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Typical data quantity (bytes)</td>
<td>1-100</td>
<td>1-100</td>
<td>-</td>
<td>-</td>
<td>16-64k</td>
<td>16-64k</td>
</tr>
<tr>
<td>Data density</td>
<td>Low</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>Very High</td>
<td>Very High</td>
</tr>
<tr>
<td>Readability by people</td>
<td>Limited</td>
<td>Simple</td>
<td>Simple</td>
<td>Difficult</td>
<td>Impossible</td>
<td>Impossible</td>
</tr>
<tr>
<td>Influence of dirt (damp)</td>
<td>Very High</td>
<td>Very High</td>
<td>-</td>
<td>-</td>
<td>Possible</td>
<td>No influence</td>
</tr>
<tr>
<td>Influence of (optical) covering</td>
<td>Total Failure</td>
<td>Total Failure</td>
<td>-</td>
<td>Possible</td>
<td>-</td>
<td>No influence</td>
</tr>
<tr>
<td>Influence of direction and position</td>
<td>Low</td>
<td>Low</td>
<td>-</td>
<td>-</td>
<td>Unidirectional</td>
<td>No influence</td>
</tr>
<tr>
<td>Degradation/wear</td>
<td>Limited</td>
<td>Limited</td>
<td>-</td>
<td>-</td>
<td>Contacts</td>
<td>No influence</td>
</tr>
<tr>
<td>Unauthorized copying/modification</td>
<td>Slight</td>
<td>Slight</td>
<td>Possible (audio tape)</td>
<td>Impossible</td>
<td>Impossible</td>
<td>Impossible</td>
</tr>
<tr>
<td>Reading speed</td>
<td>Low ~4s</td>
<td>Low ~3s</td>
<td>Very low &gt;5s</td>
<td>Very low &gt;5-10s</td>
<td>Low ~4s</td>
<td>Very fast ~0.5s</td>
</tr>
<tr>
<td>Maximum distance between data carrier and reader</td>
<td>0-50 cm</td>
<td>&lt;1 cm scanner</td>
<td>0-50cm</td>
<td>Direct contact (Only for fingerprint)</td>
<td>Direct contact</td>
<td>0-5m</td>
</tr>
</tbody>
</table>

Table 1: Comparison of different auto-ID systems showing advantages and disadvantages [1]

2.2: Components of an RFID system

RFID is an automatic identification method relying on storing and remotely retrieving data using devices called RFID tags or transponders. An RFID tag is a small chip that can be attached to or incorporated into an object. The tags contain antennas to enable them receive and respond to radio frequencies from and RFID reader or interrogator. [2-Pascal]

2.2.1: RIFD Reader

RFID tags are interrogated by readers, which in turn are connected to a host computer. Readers may be portable handheld terminals or fixed devices positioned at strategic points, such as a store
entrance, assembly line, or toll booth. The reader is equipped with antennas for sending and receiving signals, a transceiver, and a processor to decode data. [3]

RFID readers are used to activate passive tags with RF energy and to extract information from the tag. For this function, the reader includes an RF transmission for receiving and data decoding sections. In addition, the reader often includes a serial communication (RS-232, USB, and so on) capability to communicate with a host computer. Typically, the reader is a read-only device, whereas the reader for a read/write device is often called an interrogator. Unlike the reader for a read-only device, the interrogator uses command pulses to communicate with a tag for reading and writing data. The carrier is the transmitted radio signal of the reader (interrogator). This RF carrier provides energy to the tag device and is used to detect modulation data from the tag using a backscattering. In read/write devices, the carrier is also used to deliver the interrogator’s commands and data to the tag. [3]

Readers in all systems can be reduced to two fundamental functional blocks: the control system and the RF interface which consists of a transmitter and a receiver as illustrated in figure 2 below:

![Figure 2: Block diagram of a reader constituting of a control system and RF interface. The entire system is controlled by an external application via control command [1]](image)

### 2.2.1.1 RF interface

The reader’s interface performs the following functions:

- Generation of high-frequency transmission power to activate the tag and supply of with power
- Modulation of the transmission signal to send data to the transponder
- Reception and demodulation of RF signals transmitted by a tag
The RF interface contains two separate signal paths to correspond with two directions of data flow from and to the transponder/tag as shown in figure 3 below:

**Figure 3: Block diagram of an RF interface for an inductively coupled RFID system[1]**

Data transmitted to the transponder travels through the transmitter arm. Conversely, data received from the transponder is processed in the receiver arm.

2.2.1.2: Control Unit

The reader’s control unit is shown in figure 4 below and it performs the following functions:

- Communication with the application software and the execution of commands from the application software
- Control of the communication with a tag (master-slave principle)
- Signal coding and decoding
In more complex systems, the following additional functions are available:

- Execution of an anti-collision algorithm.
- Encryption and decryption of the data to be transferred between transponder and reader
- Performance of authentication between tag and reader.

Different types and designs of readers are available for different applications. They can be generally classified as OEM readers, readers for industrial or portable use and numerous special designs.

OEM readers are available for integration into customer’s own data capture systems, BDE terminals, access control systems, till systems, robots, etc. Industrial readers are available for use in assembly and manufacturing plant. These usually have a standardized field bus interface for simple integration into existing systems. Portable readers are used for the identification of animals, as a control device in public transport, as a terminal for payments, as an aid in servicing and testing, and in the commissioning of systems. [1]

The RF transmission section includes an RF carrier generator, an antenna and a tuning circuit. Data decoding for the received signal is accomplished using a microcontroller. The firmware algorithm in the microcontroller is written in such a way to transmit the RF signal, decode the incoming data, and communicate with the host computer.

The main criteria for readers include the following:

- Operating Frequency (LF, HF, UHF)
- Protocol agility, i.e the support for different tag protocols (ISO, EPC, proprietary)
- Different regional regulations- for example, for UHF readers[3]:
  - UHF frequency agility 902-930 MHz in the United States and 869 MHz in Europe
  - Power regulations of 4W in the United States and 500mW in some other countries;
  - Manage frequency hopping in the United States and duty cycle requirements.

- Networking to host capability [3]:
- TCP/IP;
- Wireless LAN (802.11);
- Ethernet LAN (10base T);
- RS 485.
  o Ability to network many readers together via connectors or via middleware.
  o Ability to upgrade the reader firmware in the field.
  o Management of multiple antennas:
    - Typically four antennas per reader
    - How antennas are polled or multiplexed
  o Adapting to antenna conditions (dynamic auto-tuning);
  o Interface to middleware products
  o Digital I/O for external sensors and control circuits.

2.2.1.3: Reader Antenna
The reader antenna establishes a connection between the reader electronics and the electromagnetic wave in the space. In the HF range, the reader antenna is a coil, designed to produce as strong a coupling as possible with the tag antenna. In the UHF range, reader antennas come in a variety of designs. Highly directional, high-gain antennas are used for large read distances. One advantage of highly directional antennas is that the reader power often has to be emitted only to the spaces in which the tags that are to read are located.

Generally speaking, physical interdependencies mean that the antenna gain is linked to the antenna size. The higher the gain (or the smaller the solid angle into which the antenna emits), the larger the mechanical design of the antenna will be. It follows, therefore, that highly directional antennas are not used for handheld readers. Antennas typically used for handheld readers include patch antennas, half-wave dipoles, and helix antennas. Larger antenna structures can be used for stationary readers; in the UHF range, they usually take the form of arrays. [3]

2.2.2: RFID Tag
A distinction criterion of different RFID systems is how the energy supply of the transponder works. In this case, we distinguish between passive and active transponders.

Passive transponders do not have any power supply. Through the transponder antenna, the magnetic or electromagnetic field of the reader provides all the energy required for operating the transponder. In order to transmit data from the transponder to the reader, the field of the reader can be modulated (e.g. by load modulation or modulated backscatter) or the transponder can immediately store, for a short time, energy from the field of the reader. That means that the energy emitted by the reader is used for data transmission both from the reader to the transponder and back to the reader. If the transponder is located outside the reader’s range, the transponder has no power supply at all and, therefore, will not be able to send signals.

Active transponders have their own energy supply from a battery or a solar cell. Here, the power supply is used to provide voltage to the chip. The magnetic or electromagnetic field received by the reader is therefore no longer necessary for the power supply of the chip. That means that the field may be much weaker than the field required for operating a passive transponder. This
condition can substantially increase the communication range if the transponder is capable of detecting weaker radio signal.

Both the passive and active transponders discussed above cannot generate a high-frequency signal of its own, but can only modulate the reader field in order to transmit data between the transponder and the reader. Thus, the energy from the active transponder’s own power supply does not contribute to data transmission from the transponder to the reader. In a matter of fact, this type of transponder is often called semi-passive transponder, which refers to the fact that this transponder is not able to generate a high frequency signal.

The circuit design for another class of active transponders corresponds to that of a classic radio device. These transponders have an active transmitter and often also a high-quality receiver. In order to transmit data to a reader, a transmitter is switched on and the antenna emits a high-frequency electromagnetic field. A local energy source like a battery supplies the transponder with high power.

Figure 5 below shows the comparison in block format between the passive, semi-passive and active transponders.

Criteria for selecting an RFID tag are as follows:

- Frequency band: desired frequency band of operation depends on the regulations of the country where the tag will be used
- Size and form: tag form and size must be such that it can be embedded or attached to the required objects (cardboard boxes, airline baggage strips, identification cards, and so on) or fitted inside a printed label.
- Read range: minimum required read range is usually specified
- EIRP: EIRP is determined by local country regulations (active versus passive tags)
- Objects: tag performance changes when it is placed in different objects or when other objects are present in the vicinity of the tagged object. A tag’s antenna can be designed or tuned for optimum performance on a particular object or designed to be less sensitive to the content on which the tag is placed.
- Orientation or polarization: the read range depends on antenna orientation. How tag are placed with respect to the polarization of the reader’s field can have significant effect on the communication distance for both HF and UHF tags, resulting in a reduced operating range of up to 50% and in the case of the tag being displaced by 90° and not being able to read the tag at all. The optimal orientation for HF tags is for the two antenna coils (reader and tag) to be parallel to each other as shown in figure 6 below. UHF tags are even more sensitive to polarization due to the directional nature of the dipole fields. Some applications require a tag to have a specific directivity pattern such as omnidirectional or hemispherical coverage.
Applications with mobility: RFID tags can be used in situations where tagged objects, such as pallets or boxes, travel on a conveyor belt at high speeds. The Doppler shift in this case is less than 30Hz at 915MHz and does not affect RFID operation. However, the tag spends less time in the rear field of the RFID reader, demanding a high-read-rate capability. In such cases, the RFID system must be carefully planned to ensure reliable tag identification.
Cost: the RFID tag must be a low-cost device, thus imposing restrictions both on antenna structure and on the choice of materials for its construction including the ASIC used. Typical conductors used in tags are copper, aluminium, and silver ink. The dielectrics include flexible polyester and rigid PCB substrates, such as FR4.

Reliability: the RFID tag must be a reliable device that can sustain variations in temperature, humidity, and stress and survive such processes as label insertion, printing and lamination.

Power for the tag: an active tag has its own battery and does not rely on the reader for any functions. Its range is greater than that of passive tags but has a lower life time. Passive tags rely on the reader for power to perform all functions, and semi-passive tags rely on the reader for power transmission but battery for powering their own circuitry.

2.2.2.1: Data Content of RFID tags

Read-Only Systems
Read-only systems can be considered low end; these tags usually only contain an individual serial number that is transmitted when queried by a reader. These systems can be used to replace the functionality of barcodes.

One-bit tags can be detected, but they do not contain any other information. This is very useful for protecting items in a shop against shoplifters. A system like this is called electronic article surveillance (EAS) and has been in use since the 1970s [3]. In practice, this system can be identified by the large gates of coils or antennas at the exits of shops.

Read-only tags that contain more than 1 bit of data are simple ones that only contain a unique serial number that it transmits on request. The contents of the read-only chips are usually written during manufacturing. Usually these simple chips also contain some logic for anticollision; that is, they allow multiple tags to be read simultaneously. [3]

Read/Write Systems.
Read/write systems specify what is possible in terms of read-only and read/write capability. Read-only devices are generally less costly and may be factory programmable as read only or one-time programmable (OTP). One-time programmability provides the opportunity to write once then read many times, thus supporting passport-type applications, in which data can be added at key points during the lifetime or usage of an item, and thus provide an incorruptible history or audit trail for the item data. Some chips allow writing only once, and they are often referred to as write once/read many (WORM). These tags are versatile because they can be written with a serial number when applied to an item, instead of linking a predefined serial number to an item. More advanced chips allow both reading and writing multiple times, and the contents of a tag can be altered remotely by a scanner. Read/write data carriers offer a facility for changing the content of the carrier as and when appropriate within a given application. [2]

2.2.2.2: Passive Tags
Because the tag has a limited supply of power, its transmission is much more limited than an active tag, typically no more than simply an ID number. Similarly, passive devices have a limited range of broadcast, requiring the reader to be significantly closer than an active one would. Uses
for passive devices tend to include things such as inventory, product shipping and tracking, use in hospitals and for other medical purposes, and antitheft, where it is practical to have a reader within a few meters or so of the RFID device.

Tags consist of a silicon device and antenna circuit. The purpose of the antenna circuit is to induce an energizing signal and to send a modulated RF signal. The read range of a tag largely depends on the antenna circuit and size. The antenna circuit is made of an LC resonant circuit or E-field dipole antenna, depending on the carrier frequency. The LC resonant circuit is typically used for frequencies of less than 100 MHz. In this frequency band, the communication between the reader and tag takes place with magnetic coupling between the two antennas through the magnetic field. An antenna utilizing inductive coupling is often called a magnetic dipole antenna. The antenna circuits must be designed in such a way as to maximize the magnetic coupling between them. This can be achieved with the following parameters:

- The LC circuit must be tuned to the carrier frequency of the reader.
- The Q of the tuned circuit must be maximized.
- The antenna size must be maximized within the physical limits of application requirements.

The passive RFID tags sometimes use backscattering of the carrier frequency for sending data from the tag to the reader. The amplitude of the back-scattering signal is modulated with modulation data from the tag device. The modulation data can be encoded in the form of ASK (NRZ or Manchester), FSK, or PSK. During backscatter modulation, the incoming RF carrier signal to the tag is loaded and unloaded, causing amplitude modulation of the carrier corresponding to the tag data bits. The RF voltage induced in the tag’s antenna is amplitude modulated by the modulation signal (data) of the tag device. This amplitude modulation can be achieved by using a modulation transistor across the LC resonant circuit or partially across the resonant circuit. Changes in the voltage amplitude of the tag’s antenna can affect the voltage of the reader antenna. By monitoring the changes in the reader antenna voltage (due to the tag’s modulation data), the data in the tag can be reconstructed.

The RF voltage link between the reader and tag antennas is often compared to weakly coupled transformer coils; as the secondary winding (tag coil) is momentarily shunted, the primary winding (reader coil) experiences a momentary voltage change. Opening and shunting the secondary winding (tag coil) in sequence with the tag data is seen as amplitude modulation at the primary winding (reader coil).

2.2.2.3: Active Tags

Active RFID tags, also called transponders because they contain a transmitter that is always on, are powered by a battery about the size of a coin and are designed for communications up to 100 feet from the RFID reader. They are larger and more expensive than passive RFID tags, but can hold more data about the product and are commonly used for high-value asset tracking. A feature that most active tags have and most passive tags do not is the ability to store data received from a transceiver. Active tags are ideal in environments with electromagnetic interference because they
can broadcast a stronger signal in situations that require a greater distance between the tag and the transmitter.

Although passive tags can only respond to an electromagnetic wave signal emitted from a reader, active tags can also spontaneously transmit an ID. There are various types of unscheduled transmission types, such as when there are changes in vibration or temperature or when a button is pushed. A semiaactive or semipassive (depending on the manufacturer) tag also has an on-board battery. The battery in this case is only used to operate the chip. Like the passive tag, it uses the energy in the electromagnetic field to wake up the chip and to transmit the data to the reader. These tags are sometimes called battery-assisted passive (BAP) tags.

Active tags are classified as below [3]:

- Wake-up tag systems are deactivated, or asleep, until activated by a coded message from a reader or interrogator. In the sleep mode, limiting the current drain to a low-level alert function conserves the battery energy. Where larger memories are accommodated, there is also generally a need to access data on an object or internal file basis to avoid having to transfer the entire amount of data so held. These are used in toll pay-ment collection, checkpoint control, and in tracking cargo.

- Awake tag or beacon systems are, as the term suggests, responsive to interrogation without a coded message being required to switch the tag from an energy conservation mode. However, they generally operate at lower data transfer rates and memory sizes than wake-up tags, so they con-serve battery energy in this way. (A greater switching rate is generally associated with higher energy usage.) This type of tag is the most widely used of the two, and because of lower component costs it is generally less expensive than a wake-up tag system. Beacons are used in most real-time locating systems (RTLS), where the precise location of an asset needs to be tracked. In an RTLS, a beacon emits a signal with its unique identifier at preset intervals, every 3 seconds or once a day, depending on how important it is to know the location of an asset at a particular moment in time.

### 2.2.2.4: RFID Chip Description

An RFID tag consists of an RFID chip, an antenna, and tag packaging. The RFID circuitry itself consists of an RF front end, some additional basic signal processing circuits, logic circuitry to implement the algorithms required, and EEPROM for storage. The RFID chip is an integrated circuit implemented in silicon. The major blocks and their functions of the RFID front end are as follows [1]:

- Rectifier: Generates the power supply voltage for front-end circuits and the whole chip, as well from the coupled EM field
- Power (voltage) regulator: maintains the power supply at a certain level and at the same time prevents the circuit from malfunctioning or breaking under large input RF power;
- Demodulator: Extracts the data symbols embedded in the carrier waveforms;
- Clock extraction or generation: Extracts the clock from the carrier (usually in HF systems) or generates the system clock by means of some kind of oscillator;
- Backscattering: Fulfills the return link by alternating the impedance of the chip;
- Power on reset: Generates the chip’s power on reset (POR) signal;
- Voltage (current) reference: Generates some voltage or current reference for the use of front-end and other circuit blocks, usually in terms of a bandgap reference;
- Other circuits: These include the persistent node or short-term memory (or ESD).

The RF front end is connected to the antenna, and typically, at UHF, an electric dipole antenna is used, while HF tags use a coil antenna. The front-end circuitry impacts the semiconductor process by requiring a process that allows for mixed-mode fabrication. Passive RF tags have no power source and rely on the signal from the reader to power up; thus, the RF front end implements modulators, voltage regulators, resets, and connections to an external antenna.

The IC in an RFID tag must be attached to an antenna to operate. The antenna captures and transmits signals to and from the reader. The coupling from the reader to the tag provides both the transmission data and the power to operate the passive RFID tag. Typically, antennas for passive RFID systems can be either simple dipole, 915-MHz RFID tags or more complex coiled shapes for 13.56-MHz systems.

### 2.3: Working of an RFID system

An RFID system is typically constituted of the forward link and the backscatter link entailing RFID tags and readers. In the forward link, the reader performs as the interrogation, transmitting a Radio Frequency (RF) wave to the tag. In the backscatter link communication, passive tag generates the reverse RF wave just by reflecting back a portion of interrogating RF wave in a process known as backscatter [4]

An RFID reader basically emits an RF signal and data is exchanged when the tag comes in proximity to the reader. RFID systems in the market today fall into two main categories: near-field systems that employ inductive (magnetic) coupling of the transponder tag to the reactive energy circulating around the reader antenna, and far field systems that couple to real power contained in free space propagating electromagnetic plane waves. Near field coupling techniques are generally applied to RFID systems operating in the LF and HF bands with relatively short reading distances, whereas far-field coupling is applicable to the potentially longer reading ranges of UHF and microwave RFID systems. Whether or not a tag is in the near or far field depends on how close it is to the field creation system and the operating frequency or wavelength. There is a distance, commonly known as the radian sphere, inside which one is said to be in the near field and outside of which one is said to be in the far field. Because changes is electromagnetic fields occur gradually, the boundary is not exactly defined; the primary magnetic field begins at the antenna and induces electric field lines in space (the near field).

The zone where the electromagnetic field separates from the antenna and propagates into free space as plane wave is called the far field. In the far field, the ratio of electric field $E$ to magnetic field $H$ has the constant value of $120\pi$ or $377\Omega$. The approximate distance where this transition zone happens is given as:
\[ r = \frac{\lambda}{2\pi} \] ................................. (2.1) [3]

It is important to notice that this expression is valid for small antennas where \( D \ll \lambda. \) The reactive near-field region is a region where the E- and H-fields are not orthogonal; anything within this region will couple with the antenna and distort the pattern, so the antenna gain is not a meaningful parameter here.

It has been estimated that the far-field distance for the case in which \( D > \lambda \) is given as follows:

\[ r = \frac{2D^2}{\lambda} \] ................................. (2.2) [3]

Where \( D \) is the maximum dimension of the radiating structure and \( r \) is the distance from the antenna. Note that this is only an estimate, and the transition from near field to far field is not abrupt. Typically, \( D \) for reader antennas is 0.3m. The far-field distance in the UHF ISM band in the USA (915MHz, \( \lambda=0.33m \)) is estimated to be 0.56m [2].

Generally speaking, the radiating near-field or transition region is defined as a region between the reactive near field and a far field. In this region, the antenna pattern is taking shape but is not fully formed, and the antenna gain measurements will vary with distance:

\[ \frac{\lambda}{2\pi} < r < \frac{2D^2}{\lambda} \] ................................. (2.3) [3]

The solution of Maxwell’s equations for the fields around the antenna consists of three different powers of the range \( \frac{1}{r}, \frac{1}{r^2} \) and \( \frac{1}{r^3} \). At very short ranges, the higher powers dominate the solution, while the first power dominates at longer ranges. This can be interpreted as the electromagnetic wave breaking free from the antenna. The near field may be thought of as the transition point where the laws of optics must be replaced by the Maxwell’s equations of electromagnetism.

RFID systems based on UHF and higher frequencies use far-field communication and the physical property of backscattering or “reflected” power. Far-field communication is based on electric radio waves where the reader sends a continuous base signal frequency that is reflected back by the tag’s antenna. During the process, the tag encodes the signal to be reflected with the information from the tag (the ID) using a modulation (i.e. shifting the amplitude or phase of the waves returned)

The concept of the radian sphere, which has a value for its radius of \( \lambda/2\pi \) helps in the visualization of whether the tag coupling is in the near or far field. If the tag is inside this sphere, the reactive energy storage fields (dipolar field terms) dominate and near-field coupling volume theory is used. If the tag falls outside the sphere, then propagating plane wave EM fields dominate and the familiar antenna engineering concepts of gain, effective area or aperture, and EIRP are used. These often more familiar EM concepts whereby real power is radiated into free space are relevant to the cases of UHF and microwave tagging technologies.

Most theoretical analyses, at least in the first approximation, assume the so-called free-space propagation. Free space simply means that there is no material or other physical phenomenon
present except the phenomenon under consideration. Free space is considered the baseline state of the electromagnetic field. Radiant energy propagates through free space in the form of electromagnetic waves, such as radio waves and visible light (among other electromagnetic spectrum frequencies).

A backscatter tag operates by modulating the electronics connected to the antenna in order to control the reflection of incident electromagnetic energy. For successful reading of a passive tag, two physical requirements must be met:

- **Forward power transfer**: Sufficient power must be transferred into the tag to energize the circuitry inside. The power transferred will be proportional to the second power of the distance.
- **The radar equation**: the reader must be able to detect and resolve the small fraction of energy returned to it. The power received will be reduced proportional to the fourth power of the distance.

### 2.3.1: Forward Power Transfer

A typical RFID tag consists of an antenna and an integrated circuit (chip), both with complex impedances. The chip contains power from the RF signal transmitted by the base station, called the RFID reader. The RFID tag antenna is loaded with the chip whose impedance switches between two impedance states, usually high and low. At each impedance state, the RFID tag presents a certain radar cross section (RCS). The tag sends the information back by varying its impedance and thus modulating the backscattered signal.

Consider figure 6 below that demonstrates forward power transfer.
From figure 6, $Z_A = R_a + jX_a$ is the complex antenna impedance and $Z_C = R_c + jX_c$ is the complex chip (load) impedance; chip impedance may vary with the loaded antenna can be divided into two parts. One part is called the structural mode and is due to currents induced on the antenna when it is terminated with complex conjugate impedance. The second part is called the antenna mode and results from the mismatch between antenna impedance and load impedance.

The separation between the antennas is $r$, which is assumed to be large enough for the tag to be in the far field of the reader. $E$ is the electric field strength of the reader at the tag location. The efficiency of the matching network will be taken as unity and ignored (losses in the network may also be accounted for in the value of $G_T$). Antenna gains $G_R$ and $G_T$ are expressed relative to an isotropic antenna. From considerations of power flux density at the tag, with $\lambda$ as the wavelength, we get:

$$P_{Tag} = \left( \frac{E^2}{120\pi} \right) \left( \frac{\lambda^2}{4\pi} \right) G_T = \frac{V_{Tag}^2}{R_c} \tag{2.4} \text{[3]}$$

And

$$\frac{E^2}{120\pi} = \frac{P_R G_R}{4\pi r^2} \tag{2.5} \text{[3]}$$

After manipulation of the two equations above, we obtain:

$$P_{Tag} = \left( \frac{P_R G_R}{4\pi R^2} \right) \left( \frac{\lambda^2 G_T}{4\pi} \right) = \frac{P_R G_R G_T \lambda^2}{(4\pi)^2 r^2} \tag{2.6} \text{[3]}$$

The typical maximum reader output is 500mW, 2W (ERP, CEPT), and 4W (EIRP, FCC). Converted to dBm, the permitted maximum limits are about 29 dBm (500 mW. ERP, 825 mW EIRP), 35 dBm (2W ERP, 3.3 W EIRP), and 36 dBm (4W EIRP). The tag available power versus distance can be seen in figure 7 below:
The power received by the tag is then divided in two parts: the reflected power and the available power used by the chip. The distribution of these two parts is very critical for a maximum distance. For dipole antennas present in the best orientation, $G_T$ may be taken as 2 dBi (gain over isotropic with allowance for losses, approximately 1.6)$^3$

We can also say that:

$$V_{Tag} = \left( \frac{\lambda}{4\pi r} \right) \sqrt{P_R G_R G_T R_C} \quad \ldots \quad (2.7) \quad [3]$$

Note that $P_R G_R$ is the EIRP of the reader. The maximum practical value of $R_C$ is 600Ω. The received voltage $V_{Tag}$ must be large enough to be rectified and power the tag; a voltage in excess of 1.2 $V_{rms}$ may be required. This is with the tag presented to the interrogating field in the ideal orientation and with no power margin.

2.3.1.1: Radar Equation

Radar principles tell us that the amount of energy reflected by an object is dependent on the reflective area of the object—the larger the area, the greater the reflection. This property is referred to as the radar cross section (RCS). The RCS is an equivalent area from which energy is collected by the target and retransmitted (backscattered) back to the source. For an RFID system in which the tag changes its reflectivity in order to convey its stored identity and data to the reader, this is referred to as differential radar cross section or ΔRCS.
For the antenna to transfer maximum energy to the chip, the impedance of the chip must be a conjugate of the antenna impedance. However, it is important to remember that the logic circuits of a chip used in a tag draw very little power relative to the amount of power consumed by the chip RF input circuits. As the modulator switches between two states, the load impedance of the chip $Z_c$ will switch between two states. The reflection due to a mismatch between antenna and load in a backscatter tag is analogous to the reflection found in transmission lines and may be expressed in terms of a coefficient of reflection. The coefficient of reflection $\rho$ will therefore change as the modulator switches between two states. When the tag modulator is in the off state, the chip input impedance will be closely matched to the antenna impedance; therefore, the reflectivity will be low and hence the SWR will approach 1. When the modulator is in the on state, the tag antenna impedance will be mismatched and so the reflectivity will be high, and the SWR will tend to infinity, causing the maximum amount of power to be reflected, i.e:

$$\rho = \frac{Z_c-Z_A^*}{Z_c+Z_A}$$ .................................................................................................. (2.8) [3]

The tag varies its RCS by changing the impedance match of the tag antenna between two (or more) states. The ratio between the states is called the differential coefficient of reflectivity, represented by the symbol $\Delta \rho$, and it can be calculated using transmission line theory. Signal propagation follows the Friis transmission formula; analytical approaches such as the Friis equation assume undisturbed near-field conditions (i.e., no proximity of dielectric and metal objects), known antenna characteristics, and no diffraction and reflection effects. An antenna of gain $G$ has an effective aperture as calculated here:

$$A_e = \frac{\lambda^2 G T}{4\pi}$$ .................................................................................................. (2.9) [3]

The $\Delta \rho$ is the differential reflection coefficient of the tag modulating circuitry and can be calculated as shown:

$$\Delta \rho = p_1 (1 - |\rho_1|^2) + p_2 (1 - |\rho_2|^2)$$ ......................... (3.0) [3]

Where the IC in states 1 and 2 for a fraction of and of time $p_1$ and $p_2$ of time, respectively.

### 2.3.2: Data transfer between a tag and a reader

#### 2.3.2.1: Signal transmission
For an RFID system to work, we need three processes: energy transfer, downlink and uplink. According to this, we can divide RFID systems into three groups: full-duplex, half-duplex and sequential [3]. During full and half-duplex operation, the energy is transferred constantly, compared to sequential operation when energy is first transferred by the reader ans then the tag responds. In half-duplex systems, the information is sent in turns either transferred inductively through load modulation or as electromagnetic backscatter, such as with radar.

In full duplex systems uplink information is sent on a separate frequency, either a sub-harmonic or not, so the flow of information can be bidirectional and continuous. Sequential transfer
consists of two phases: first, energy is sent to the tag that stores it in a capacitor, then, utilizing
the power received, it can function for some time and send its reply. This has the advantage that
by extending the charging time and enlarging the capacitor it is possible to acquire more energy
for the electronics.

2.3.2.1: Data transfer rate
A further influence of carrier frequency is with respect to data transfer, for which it is very
important to understand the bit rate (data rate) concept. Whereas in theory it is possible to transfer
binary data at twice the carrier frequency, in practice it is usually to use many cycles of the
carrier to represent a binary digit or group of digits. Generally, the higher the carrier frequency,
the higher the data transfer rate that can be achieved. So, a low frequency system operating at
125kHz may transfer data at a rate of between 200 and 4000 bps depending on the type of
system, while rates up to greater than 100Kbps are possible for microwave systems. A finite
bandwidth is required in practice to transfer data, this being a consequence of the modulation that
is used. Also consequential to transfer capability is the data capacity of the tag. Loosely speaking,
the lower the frequency, the lower the data capacity of the tags, simply because of the amount of
data required to be transferred in a defined time period. The capacity can also be determined by
the manner in which the tag is designed to be read or written to (for read/write tags), be it in total
or part. The choice of data transfer rate has to be considered in relation to system transfer
requirements. This is determined by the maximum number of tags that may be expected to be
read in a unit interval of time multiplied by the amount of data that is required to be read from
each tag. Where a write function is also involved, the number of tags and write requirements
must also be considered.

The manner in which the tags are interrogated is also important. It can be done singularly (one at
a time in the interrogation zone) or as a batch (a number of tags in the interrogation zone at the
same time). The latter requires that the tags and associated system have anti-contention (anti-
collision) facilities so that collisions between responses from tags in the zone at the same time
can be resolved and contention avoided. Various anti-collision protocols have been devised and
applied with various levels of performance with respect to the number of tags that can be handled
and the time required to handle them. So, the anti-collision performance may be an important
consideration in many applications.

2.3.2.2: Read/Write range
The read/write range is the communication distance between the reader (interrogator) and tag.
Specifically, the read range is the maximum distance to read data out from the tag, and the write
range is the maximum distance to write data from the interrogator to the tag. The read/write range
is, among other effects, mainly related to [3]:

- Electromagnetic coupling of the reader and tag antennas
- The RF output power level of the reader
- Carrier frequency bands
The power consumption of the device
- Antenna orientation
- The distance between the reader and tag
- Operating environmental conditions (metallic, electric noise, multiple tags, multiple readers, and so on)
- The tag and the tag’s dwell time, i.e. the time a tag is in the reader’s RF field.

An RFID interrogator’s read range is the distance between the interrogator and the RFID tag at which the signals from the tag can be read properly. Similarly, an RFID interrogator’s write range is the maximum distance at which information within the RF signal from the interrogator can be received correctly and stored within the memory of the tag’s microchip. More power is needed to write to a tag than to read it; as a result, the tags need to be closer to the antenna to write than to read. The general rule is that the write range is 50% to 70% of the read range of a particular interrogation zone. [3]

The electromagnetic coupling of the reader and tag antennas increases, using a similar size of antenna with high $Q$ on both sides. The read range is improved by increasing the carrier frequency. This is due to the gain in the radiation efficiency of the antenna as the frequency increases. However, the dis-advantage of high-frequency (900-MHz to 2.4-GHz) application is shallow skin depth and narrower antenna beam width causing less penetration and more directional problems, respectively. Low-frequency application, on the other hand, has an advantage in the penetration and directivity, but a disadvantage in the antenna performance. Read range increases by reducing the current consumption in the silicon device. This is because the LC antenna circuit couples less energy from the reader at further distances. A lower power device can make use of less energy for the operation.

For LF and HF (near-field) systems, to increase the magnetic field at the tag’s position, the reader/writer antenna coil’s radius must be increased, or the current in the antenna coil must be increased, or both. The strength of the magnetic field is attenuated in proportion to the inverse of the cube of distance. By increasing the diameter of the RFID tag’s antenna coil, the signal induced in the tag’s coil can be increased. Accordingly, for applications that require long-range operation, the reader/writer antenna coil’s radius and tag antenna coil’s dimensions must be increased. In tests comparing coin-sized and IC card-sized tags using the same reader/writer, the IC card-sized tag had an operating area several times larger than the coin-sized tag.

The read range of a UHF-based RFID (propagation) system can be calculated by the Friis free-space equation as follows:

$$r = \frac{\lambda \cos \theta}{4\pi} \sqrt{\frac{P_R G_R G_T (1-(\Delta \rho)^2)}{P_{th}}}$$

for $0 \leq (\Delta \rho)^2 \leq 1$ ....................................................... (3.0) [3]

Where:
- $G_T$ is the gain of the tag antenna,
- $P_R G_R$ is the EIRP for the reader,
\( \lambda \) is the wavelength

\( P_{th} \) is the minimum threshold power required to power an RFID tag,

\( \theta \) is the angle made by the tag with the reader plane,

\((\Delta \rho)^2\) is the power reflection coefficient, which is the ratio of reflected power to incident power by the tag.

The power reflected by the tag is inversely proportional to the square of the distance between the tag and the reader’s antenna. The orientation of the tag in the RF field affects its read range. In the specific context of a directivity pattern, a perfectly parallel tag, relative to the base station antenna, yields the maximum read range, whereas a tag perpendicular to the base station antenna’s field has minimum zero read range. Thus, efforts are made to make the tag more parallel to the reader antenna by deploying one or more of the following measures:

- Change in orientation of the reader antenna to suit the orientation of the tag antenna
- Use of redundant antennas for ensuring proper alignment of at least one reader antenna to the tag antenna
- Increase reader antenna power (within the limits allowed by the authority) to reduce the effect of tag orientation
- Increase the polling rate of the antenna to make more reads in the same sampling time.

The far-field formula is correct, subject to the assumption that the polarization of the reader antenna and the polarization of the tag antenna are perfectly matched. However, in fact, the polarization mismatch is essential and required in most RFID applications. The point is that in the majority of applications the tag is allowed to appear in an almost arbitrary position in the field of the reader antenna while the polarization of the tag antenna is usually linear because of the pre-required small size of the tag.
2.3.3: UHF Reader Electronic Circuitry
The figure 8 below shows the typical block diagram of an RFID reader

![Functional Blocks of an RFID Reader](image)

2.3.3.1: UHF Source module
The purpose of the source module is to provide a synthesized local oscillator (LO) for transmitting (Tx) and receiving (Rx) paths in an RFID reader. It is necessary to amplify the signal after the synthesizer, in order to provide adequate LO input to the Tx and Rx signal paths due to typical synthesizer output powers and the loss of the power divider. Using an integrated synthesizer/ voltage-controlled oscillator (VCO) IC, it is possible to center the VCO bands by using different inductor values.
2.3.3.2: UHF Reader Transmission Module
A typical transmitting module would include a double balanced modulator (DBM), LO amplifier, preamplifier, power amplifier, and impedance transforming network (ITN). The high level of integration, with over 50 dB of available small-signal gain, requires careful module layout. To maintain stability, it is necessary to keep the preamplifier located as far as possible from the power amplifier. The DBM provides a means to modulate the carrier signal. An LO amplifier is included to raise the signal available from the source module to a level sufficient to drive the mixers. Additionally, having the LO amplifier provide a 50Ω interface allows for simple interconnection to the source module.

The modulated RF output from the mixer goes to a preamplifier and then to a power amplifier. The preamplifier has a gain of 17 dB and the power amplifier, implemented as a three-stage device, provides a small signal gain of 35 dB Also included in the transmit module is an impedance transforming net-work (ITN). The purpose of this network is to transform the 50Ω load impedance to a level that the power amplifier needs to drive in order to produce the desired output power at the available supply voltage. For a typical supply of 3.6V, this impedance is only a few ohms, creating large circulating currents. These low impedances necessitate proper handling of circuit parasitics. This circuit requires careful design and implementation from performance and reliability perspectives.

To be able to provide the desired 1W RF level at the antenna terminals typical for UHF readers, the power amplifier needs to be capable of providing sufficient power output capability to overcome the signal losses introduced between the transmitting module output and the antenna. These losses would include any coupler, filter, circulator, connector, and cabling used in the path to the antenna. It is desirable to control the power in order both to set the output level to various requirements and to implement a commonly used form of carrier amplitude modulation called pulse-interval modulation, which is used to interrogate tags. The modulation bandwidth must be sufficient for the intended data rates without significant distortion, but as much circuitry as possible should be broadband. The transmitter transmits encoding data with ASK modulation, including DSB-ASK, and SSB-ASK for forward link, and sends an unmodulated carrier for the return link. The maximum output power from the PA is restricted to 30 dBm (1W). [3]

2.3.3.3: UHF Reader Receiving Module
Most modern wireless communication receivers use digital modulation and demodulation techniques because they provide an increased channel capacity and greater accuracy in the transmitted and received messages in the presence of noise and distortion. In digital communication systems, a finite number of electrical waveforms or symbols are transmitted, where each symbol can represent one or more bits. It is the job of the receiver to identify which symbol was sent by the transmitter even after the addition of noise and distortion. Distortion in wireless communication can be caused by several things such as passing a signal through filters having insufficient bandwidth or inefficient switching of non-linear elements. The effects of such events are termed inter-symbol interference (ISI). In addition to ISI, there are other types of distortion more notably termed delay spread and noise. Delay spread occurs when multiple versions of the same signal are received at different times. This occurs when the transmitted
signal reflects off multiple objects on its way to the receiver (multipath). System designers are focusing their attention on their transceivers in search of a method or components that might help them achieve a superior signal-to-noise ratio, resulting in a lower bit error rate.

In addition, RFID systems operating in the UHF band have unique attributes; during operation, the reader antenna emits electromagnetic energy in the form of radio waves that are directed toward an RFID tag. The tag absorbs energy, and through its in-built microchip/diode, uses it to change the load on the antenna, which in turn reflects an altered signal to the reader. This method, known as backscatter, is the basis by which a passive an RFID tag identifies its presence. The backscattered signal antenna received is sent to the receiver through a directional coupler. The receiver noise needs to be low enough that the system has sufficient dynamic range to allow error-free direction of low-level responding tag signals.

Homodyne detection, whereby a sample of the transmitted signal prior to modulation is used as the LO source for the receiving I/Q demodulator, is utilized. Having both the transmitted and received signals at the same frequency exacerbates the difficulty of recovering the weak reflected signal, because it has to be identified in the presence of the higher powered carrier frequency. Consequently, it is an advantageous to choose transceiver components that help improve the overall signal-to-noise ratio as well as minimize LO carrier leakage. The I/Q demodulator is a key element that can be used to maximize the signal-to-noise ratio and to minimize LO carrier leakage. Direct conversion to baseband frequency with the lowest bit error rate and the highest sensitivity possible is crucial, not only for reader accuracy, but also to its range of usage.

2.3.4: RFID Power Sources
RFID tags need power to sense, compute, and communicate, which is further classified into three categories: storage (batteries, capacitors), energy harvesting mechanisms (vibrations/movement, photovoltaic, thermal gradient, etc.) and energy transfer (inductive coupling, capacitive coupling and backscatter). Because many of these devices are expected to operate with a minimum of human intervention, optimizing power consumption is a very important research area. RFID tags may derive the energy to operate either from an on-tag battery or by scavenging power from the electromagnetic radiation emitted by tag readers. Storage refers to the way devices store power for their operation, done by means of batteries or capacitors. Batteries are used when a longer life is required, and capacitors are used in applications that require energy bursts for very short durations.

Power harvesting (sometimes termed energy scavenging) is the process of acquiring energy from the surrounding environment (ambient energy) and converting it into usable electrical energy. Energy transfer is the way by which passive RF devices are powered. The energy transfer mechanisms are inductive coupling, capacitive coupling, and passive backscattering. Inductive coupling is the transfer of energy between two electronic circuits due to mutual inductance between them. Passive backscattering is a way of reflecting back the energy from one circuit to another.

Passive RFID tags obtain their operating power by harvesting energy from the electromagnetic field of the reader’s communication signal. The limited resources of a passive tag require it to both harvest its energy and communicate with a reader within narrow frequency band as
permitted by regulatory agencies. A passive tag’s power comes from the communication signal either through inductive coupling or far-field energy harvesting. Inductive coupling uses the magnetic field generated by the communication signal to induce a current in its coupling element (usually a coiled antenna and a capacitor). The current induced in the coupling element charges the on-tag capacitor that provides the operating voltage, and power, for the tag. In this way, inductively coupled systems behave like loosely coupled transformers. Consequently, inductive coupling works only in the near field of the communication signal.

![Diagram](image)

*Figure 9: Power supply to an inductively coupled transponder from the energy of the magnetic alternating field generated by the reader [1]*

Far-field energy harvesting uses the energy from the interrogation signal’s far-field signal to power the tag. The signal incident on the tag antenna induces a voltage at the input terminals of the tag. This voltage is detected by the RF front-end circuitry of the tag and is used to charge a capacitor that provides the operating voltage for the tag. In the far-field, tag-to-reader communication is achieved by modulating the RCS of the tag antenna (backscatter modulation).

A reader communicates with, and powers a passive tag using the same signal. The fact that the same signal is used to transmit power and communicate data creates some challenging trade-offs. Firstly, any modulation of the signal causes a reduction in power to the tag. Second, modulating information onto an otherwise spectrally pure sinusoid spreads the signal in the frequency domain. This spread, known as sideband, along with the maximum power transmitted at any frequency, is regulated by local regulatory bodies.

The signaling from the tag to the reader in passive RFID systems is not achieved by active transmission. Because passive tags do not actively transmit a signal, they do not have a regulated limit on the rate of information that can be sent from the passive tag to the reader. Passive tags obtain impinging energy during reader interrogation periods, and this energy is used to power tag ICs. In near field, tag-to-reader communication is achieved by modulating the impedance (load modulation) of the tag as seen by the reader. For maximum reading range, one has to ensure maximum power transfer efficiency from the reader to the tag. What makes the problem challenging is that in the case of an inductively coupled reader-tag, the reader must deal with a
changing effective load due to the location-dependent mutual coupling effect between the reader and tag as well as the unpredictable number of tags in the read zone of the reader. [3]

Battery-assisted backscatter tags have their own source to pre-energize the silicon chip. The data is otherwise sent and received from the reader in the same way as a passive tag. This is of benefit when many tags are present in an interrogation zone; if they are all passive, the all need a lot of energy initially to reach sufficient voltage to turn on. With metals and fluids near tags, this is even harder due to interference and blind spots in the field. An on-board power source on each tag helps to overcome this.

For RFID tag systems, primary lithium/manganese dioxide (Li-MnO₂) and lithium-thionyl chloride (Li-SOCL₂) are the two types of batteries that are most common. These lithium batteries offer a set of performance and safety characteristics that is optimal for RFID tag applications. Li-MnO₂ is relatively safe compared to volatile lithium batteries, such as lithium-sulphur dioxide (Li-SO₂) and Li-SOCL₂ and does not develop any gas or pressure during battery operation.[3]

However, one main disadvantage is that single Li-MnO₂ cell cannot operate at voltages greater than 3.0V. Therefore, because most electronic components used in RFID tags require a minimum operating voltage of 3V, at least two Li-MnO₂ cells must be connected in series to ensure a proper margin of safety for system reliability. This requirement adds weight and cost while potentially decreasing reliability due to increased part count. [3]

2.3.5: 1-Bit Transponder

1-bit transponder-based systems can only represent two states, i.e ‘transponder in interrogation zone’ and ‘no transponder in interrogation zone’. The main application of 1-bit transponders have widespread use in electronic anti-theft devices in shops (EAS, electronic article surveillance). An EAS system is made up of the following components: the antenna of a reader or interrogator, the security element or tag, and an optional deactivation device for deactivating the tag after payment. In modern systems deactivation takes place when the price is registered at the till. Some systems also incorporate an activator, which is used to reactivate the security element after deactivation. The main performance characteristic for all systems is the recognition rate in relation to the gate width (maximum distance between transponder and interrogator antenna).

2.3.6: Full and Half Duplex Procedure

In contrast to 1-bit transponders, which normally exploit simple physical effects (oscillation stimulation procedures, stimulation of harmonic processes by the non-linear characteristic of diodes or the nonlinear hysteresis curve of metals), the transponders described here use an electronic microchip as the data-carrying device, which has a data storage capacity between a few bytes and more than 100kilobytes. To read from or write to the data-carrying device, it must be possible to transfer data between the reader ans the transponder and then back from the transponder to the reader. This transfer takes place according to one of the two main procedures: full-duplex and half-duplex procedures.

In the half-duplex procedure (HDX), the data transfer from the transponder to the reader alternates with data transfer from the reader to the transponder. At frequencies below 30MHz, this is most often used with the load modulation procedure, wither with or without a subcarrier.
Closely related to this is the modulated reflected cross-section procedure that is familiar from radar technology and is used at frequencies above 100MHz. Load modulation and modulated reflected cross-section procedures directly influence the magnetic or electromagnetic field generated by the reader and belong therefore among the harmonic procedures.

In the full-duplex procedures (FDX) the data transfer from the transponder to the reader (up-link) takes place at the same time as the data transfer from the reader to the transponder (down-link). This includes procedures in which data is transmitted from the transponder at a fraction of the frequency of the reader, i.e. a sub-harmonic, or at a completely independent, i.e. an anharmonic frequency.

Both procedures, however, have in common the fact that the transfer of energy from the reader to the transponder is continuous, i.e it is independent of the direction of data flow. In sequential systems (SEQ), on the other hand, the transfer of energy form the transponder to the reader takes place for a limited period of time only (pulse operation → pulsed system). Data transfer from the transponder to the reader occurs in the pauses between the power supply to the transponder. Figure 2.11 below differentiates the half-duplex, full-duplex and sequential systems.

**Figure 10:** Representation of full-duplex, half-duplex and sequential systems over time. Data transfer from the reader to the transponder is termed down-link, while data transfer from the transponder to the reader is termed up-link [1]
2.4: Interference and Interference Cancellation in RFID Systems
The nonlinearity of the RFID system will cause many noises, such as the distortion of harmonic components and intermediation, the Adjacent Channel Interference (ACI). All this would raise the Bit Error Rate (BER). Also, the isolation from the transmitter to the receiver is generally less than 20dB, which makes the information disturbed by the leakage carrier, so the RFID system must be linear enough. [4]

Interference in RFID systems can broadly be classified into three kinds:

- Tag to tag interference- occurs when multiple tags are being read at the same time. Strong tags may generate a signal that drowns all the signal generated by a very weak tag and the reader will not be able to isolate that particular tag. Readers are today incorporating anti-collision algorithms that can isolate one tag in a very large population of tags. Nevertheless, most readers choke up with tags exceeding 900.
- Reader to tag interference- occurs when a small number of tags (usually less than 10) are trying to communicate with more than one reader. The energy level produced by a reader is pretty high (about one million times that of a tag) because it has to read a high number of tags. Since there is more than one reader trying to communicate in the same zone, the tag is completely drowned out by the presence of other readers.
- Reader to reader interference- this is an argument based on the geography and UHF bands, e.g. for Europe, the UHF band is 865MHz-868MHz and would accommodate four readers transmitting at the same time in full power and close proximity. If we have more readers transmitting at the same power level and in close proximity, they interfere with each other. In the USA, the 26MHz bandwidth (902MHz-928MHz) allows fifty readers installed in close proximity with minimal interference with each other. [5]

In general, interference in RFID systems have two major effects in the supply chain:

- False alarm/false declaration: this is the situation where the identification system identifies an inventory item as present, but physically, the item is not present.
- False dismissal- this is the situation where the identification system dismisses an inventory item as absent, while physically, the item is available on the shelves.

Interference can come from a variety of sources, impairing the communication between readers and tags (or any RF communication, for that matter). The following are the common types of such interference: [6-How to cheat at deploying and securing RFID- Frank Thornton]

a) Adjacent Channel interference
b) Band congestion interference
c) Environmental interference
d) Jamming
e) Spurious emissions interference
2.4.1: Adjacent Channel Interference
This is interference from a signal with a frequency close to the operating frequency of the RFID system. So, this is the interference between two frequency channels (bands). This is avoided by introducing even and odd numbered data channels. [7]

Miller-modulated subcarriers (MMS) encoding may be used to limit reader interference. Miller encoding has the effect of displacing the tag spectrum on a subcarrier away from the carrier. The benefit of this approach is to increase the spectral separation between reader and tag signals, in the process reducing the possibility of interference between tag signals and unwanted reader signals. In the ETSI regulatory environment, a scheme has already been proposed whereby readers may only occupy every third reader channel in order to limit adjacent channel interference. This implication is that the associated tag communications will effectively take place in channels where no reader communications are allowed (as the MMS technique will effectively displace the tag spectrum from the reader carrier into the adjacent channels). Any number of readers can therefore operate in the designated reader channels as their signals will have no spectral overlap with tag spectra occurring in the adjacent channels. The problems of reader interference and of too few available channels are effectively eliminated in the process. [8]

2.4.2: Band Congestion Interference
This is interference resulting from overcrowding of a given frequency band, i.e. too many devices operating within a specified shared frequency band.

2.4.3: Environmental Interference
Interference from natural sources of electromagnetic radiation such as lightning and solar radiation.

2.4.4: Jamming
Interference or noise caused by an intentional emission of radiation by another device or system. This is done to limit the effectiveness of other communications or detection equipment.

2.4.5: Spurious emissions interference
Spurious emissions are the interfering radiation transmitted outside the operating frequency band in the form of narrow-band signals or wideband noise. An example is the emission of harmonics at multiples of fundamental frequencies.
Chapter Three

Methodology

In this project, MATLAB/ Simulink was used to investigate the working of an RFID system, interference in RFID system and interference cancellation in RFID systems. For the project, a passive tag was used as the transponder since it was easy to simulate compared to the active tag. In the simulation, the RFID system was partitioned into three blocks; reader, tag and wireless channel. Figure 11 below shows the block diagram for the whole circuit, which are explained below

**Figure 11: Block diagram for the whole circuit**
Figure 12 below is the simulation environment of the transmitter in Simulink. The tag code is generated by using a repeating sequence block. The code is modulated with a continuous carrier signal of 1V Amplitude and frequency of 900MHz. The modulated tag code is used to enable the tag and the continuous carrier signal is used for backscatter of tag ID during the return link. Double Side-Band Amplitude Modulation is used as the modulation scheme. The modulated signal is amplified, band-limited between 860MHz and 960MHz using a fourth order Band pass Bessel’s filter and transmitted through the antenna. Single Side Band-Amplitude Modulation is derived by removing one of the sidebands of DSB-AM and occupies one half bandwidth of the DSB-AM. The signal power of the SSB is half of the DSB modulation. The noise power in the bandwidth is also half of DSB. Therefore, the SNR of SSB and DSB are the same. [9]

**Figure 12: Simulation Environment of the Transmitter in Simulink**

Figure 13 shows the simulation environment of the channel, which is the wireless medium between the reader and the tag. The free space is modelled by pass loss with phase changing due to distance between the reader and tag. (System Modeling and Simulation of RFID) Here, Additive White Gaussian Noise is incorporated into the signal to represent interference as discussed earlier. This noise is simulated by incorporating a Random Number Generation block. As the noise is additive, it is added with the signal by a summing block. (RFID model and study its performances [9]
Figure 14 shows the simulation environment for the passive tag and the return link. The tag has to first identify the code transmitted by the reader and match the code with its own code stored in memory. If matching occurs, the tag will be enabled and backscatter the continuous carrier with modulated tag ID by changing the reflection coefficient of the tag antenna. The code detection is done by either peak detector or a demodulator with locally generated carrier. To reshape the signal to form the code in the bit pattern, ‘Gain’, ‘Saturation’, ‘Wrap to Zero’, ‘Boolean Converter’ and ‘Logical operator Not’ blocks are used.

The saturation block saturates the signal to an upper and lower threshold values. The Wrap to zero block checks the signal threshold value and forms a pattern which is inverted pattern on the code. So, the actual code is obtained using a Not operation after Boolean Converter converts the signal. For comparison, a ‘Queue’ block is used with push, pop signals and Input and output bit lines. When the start bit is sensed, the clock signal starts to push the code bits of the received signal. After all the 10 bits have being pushed, the clock gives pop signal. At the same time, the tag code is generated by the tag. This is done to synchronize the start bit of the receiver code and the tag code. The comparison is done by correlating the two codes using a ‘XNOR’ operation. If the 10 bits totally matches the code word time segment, the output will be ‘1’. To obtain this output, a signal block is used. The running sum taken over the code word time period will be 10, if the tag code and the reader code matches, provided sum is taken at the bit rate of the code, which is known. A running sum block and a converter are used for this. For running sum value greater than 9.5 (the switching threshold value) a 3-input switch enables the tag ID transmitter part. Switching from input 3 to input 1 occurs if the signal in input 2 crosses the threshold (9.5). Input 1 is the signal transmitted by the reader in the Return link, i.e, the continuous carrier, input 2 is the running sum signal and input 3 is connected to ground. If the tag code matches, the
Figure 14: Simulation Environment for the Passive Tag and Return Link
continuous carrier signal modulated with the tag ID is reflected back to the receiver by changing the reflection coefficient of the tag antenna. The simulation is done using a PN sequence generator (generated tag ID), product and Gain blocks. [9]

Figure 15 represents the simulation environment for the receiver block. The reader receives direct signal from the transmitter and the reflected one from the surrounding environment. [The receiving power due to direct coupling from TX to RX is modeled by a proper gain and phase delay.] [10- System Modeling and Simulation of RFID] However, strength of the signal reflected from the surrounding environment is weak and consequently can be neglected, it is essential to have a high isolation between the transmitting and receiving antennas of the reader. The receiver includes band pass filter, Low Noise Amplifier (LNA), Mixer, AC Coupling, channel select filter and variable gain stages. The receiver circuit should have a large dynamic range to handle the relatively large direct signal and detect the weak backscattered signal from the tag [9]

![Figure 15: Simulation environment for the receiver block](image)

Figure 16 represents the simulation environment for the QAM to cancel out the interference. The interference, introduced in form of AWGN by a Gaussian Random Number Generator, i.e: Additive as the noise gets ‘added’ (and not multiplied) to the received signal; White as the spectrum of the noise is flat for all frequencies and Gaussian because the values of the noise follow the Gaussian probability distribution function below:

\[ p(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \] ................................. (3.1) [3]

To cancel out the interference, Quadrature Amplitude Modulation was used as shown in figure 16.
QAM is the broadly used scheme in today’s wireless telecommunication, where we transmit a series of bits between the transmitter and the receiver. Additionally, it is possible to view the extent of bit error rate or signal noise by visual analysis, since the scatter plots are supposed to be in specific quadrants.

In simulation, AWGN is used to simulate the noise during transmission and thus the standard deviation of points on the scatter plots is normally distributed. At the receiver level, the decision to be made on scattering spread brings about the concept of bit error rate.

**Figure 16: Simulation of AWGN and its cancellation**
Chapter Four

Results and Analysis

From the simulation, the following were observed: figure 17 shows the waveform output of the transmitter.

![Figure 17: Output of the Transmitter](image)

The output of the transmitter is a sine wave at a frequency of 900MHz, well within the UHF band used for the RFID system. Initially, the signal has variations on amplitude due to non-linearities and noise in the transmitter. However, the signal stabilizes in time as the Band Pass filter ensures transmission of the desired frequency level of 900MHz, masking out noisy frequencies.
Figure 18 above shows the output of the receiver in the presence of noise. The receiver has two signal inputs, one directly from the transmitter and the other backscattered by the tag through the wireless channel. This signal received from the tag contains noise/interference from the environment through the wireless channel.

Figure 19 shows the output of the receiver when a random number generator that produces the interference in form of AWGN was incorporated.

In simulation, Additive White Gaussian Noise is used to emulate the noise/interference during transmission. Visibly, the deviation of the scatter points on the plot is spread too much such that
the decisions at the receiver, about what quadrant to place a scatter point, are bad hence a visibly high BER. This is an indication of high noise in the system. In the project, QAM-4 was used, and the probability of making a bad decision (higher BER for a specific SNR) is lower compared to use of higher level QAMs (QAM-8, QAM-16, QAM-32 etc.) Radio transmitters and receivers with higher Signal to Noise Ratios (SNRs) are thus better suited for higher data rate transmission.

Figure 20 below shows the output of the receiver when the Quadrature Amplitude Modulation has been incorporated to eliminate the noise.

**Figure 20: Signal after QAM**

Upon modulation, the scatter plots are well within the decision-making bounds, such that we can clearly map out in what quadrant a scatter point lies, indicating a reduction in BER and interference.
Challenges

Some of the challenges faced during the period of the project were:

- Lack of some blocks of the circuit elements in the Simulink Simulation platform that was used. This resulted in overlooking some of the circuit elements of the RFID system or using other blocks to replace the intended system blocks, thus resulting to observations that were close to, instead of, exactly like the expected results.
- Time - the project was issued late into the first semester and was only doable during the second semester. Considering other student responsibilities such as study for other course units, the time was not enough to do a satisfactory project as was expected.
- Additionally, the RFID technology is a developing technology. At the beginning of the project period, my understanding of the technology and what was required of the project were rather unclear. This resulted in long months of study to familiarize with the technology and the project required, thus leaving little time for the actual project design and implementation.
Conclusion and Recommendations for Further Work

In spite of the challenges faced, the project was able to achieve interference cancellation for an RFID system. An RFID system operating at 900MHz was simulated. From the simulation, the transmitter, wireless channel, tag and receiver were successfully designed and demonstrated in Simulink, together with interference in form of Additive White Gaussian Noise. To eliminate this interference, a modulator for QAM was used, and the interference was reduced to.

Future work should include actual physical implementation of the interference canceller, to see its effect on improved reader efficiency.
References


List of Acronyms
ACI-Adjacent Channel Interference
AWGN- Additive White Gaussian Noise
BAP- Battery Assisted Passive
BER- Bit Error Rate
DSB-ASK- Double Side Band Amplitude Shift Keying
EAS- Electronic Article Surveillance
EEPROM- Electronically Erasable Programmable Read Only Memory
EM-Electromagnetic Wave
EPC- Electronic Product Code
FDX- Full Duplex
FSK-Frequency Shift Keying
GRNG- Gaussian Random Number Generator
HDX- Half Duplex
HF- High Frequency
IC- Integrated Circuit
ISI- Inter-Symbol Interference
ISO- International Standards Organisation
ITN- Impedance Transformation Network
LAN- Local Area Network
LC- Local Oscillator
LNA-Low Noise Amplifier
LO- Local Oscillator
MMS- Miller-Modulated Subcarriers
NRZ- Non-Return to Zero
OCR- Optical Character Recognition
OTP- One- Time Programmable
PCB- Printed Circuit Board
PSK- Phase Shift Keying
QAM- Quadrature Amplitude Modulation
RAM- Random Access Memory
RCS- Radar Cross Section
RFID- Radio Frequency Identification
ROM- Read Only Memory
RTLS- Real Time Locating System
SNR- Signal to Noise Ratio
SSB-ASK- Single Side Band Amplitude Shift Keying
TCP/IP- Transmission Control Protocol/ Internet Protocol
VC O- Voltage Controlled Oscillator