An Electromagnetic Measurement Tool for UHF RFID Diagnostics

by

Richard Michael Redemske

Submitted to the Department of Electrical Engineering and Computer Science in partial fulfillment of the requirements for the degree of Master of Engineering in Computer Science and Electrical Engineering at the MASSACHUSETTS INSTITUTE OF TECHNOLOGY September 2005

© Massachusetts Institute of Technology 2005. All rights reserved.

Author . . .

Department of Electrical Engineering and Computer Science

September 1, 2005

Certified by........

Daniel W. Engels
Research Scientist

Accepted by .

Arthur C. Smith
Chairman, Department Committee on Graduate Students
An Electromagnetic Measurement Tool
for UHF RFID Diagnostics

by

Richard Michael Redemske

Submitted to the Department of
Electrical Engineering and Computer Science
on September 1, 2005, in partial fulfillment of the
requirements for the degree of
Master of Engineering in Computer Science and Electrical Engineering

Abstract

This thesis presents the design and analysis of a radio frequency identification (RFID) passive UHF emulation tag designed to be used as an environment evaluation tool. The tag implements the Auto-ID Center/EPCglobal Generation 1 RFID passive UHF tag protocol, and it implements a power detector on the received UHF signals. The power detector enables the tag to operate as a Field Probe providing instantaneous power level feedback at its location. Power level feedback is provided visually through on-probe LEDs (light emitting diodes), audibly through an on-probe speaker, and electronically as part of the communication protocol between the Field Probe and the reader. Experimental results presented here as well as the use of the Field Probe in real-world installations by the project sponsors have already shown that the Field Probe is a valuable tool in the design and analysis of RFID system installations and gross product packaging design.

Thesis Supervisor: Daniel W. Engels
Title: Research Scientist
Acknowledgments

I would first like to thank all the people at the MIT Auto-ID Lab who helped me during the course of my research, and made Auto-ID Labs a fun place to work. In particular, thanks to my fellow researchers in the Packaging SIG, Jonathan Wolk, Uttara Marti, and Alki Delichatsios. Thanks also to Toni-Marie Pommett and David Rodriguera for helping me with orders and sending out equipment to sponsors. I'd also like to thank Tom Scharfeld, who over the course of my research, provided me with good advice, and was always there to help out with setting up demonstrations.

In particular, I'd like to thank my thesis advisor, Dr. Dan Engels, for his constant support and encouragement during the writing of my thesis. His advice and comments have helped to shape my thesis, provide focus and clarity, and thankfully make it readable through the correction of many of my countless grammatical errors.

I also want to give a special thanks to my research supervisor, Dr. Rich Fletcher. Three years ago he introduced me to the wacky world of RFID. Since then, under his guidance, I've developed a deeper understanding and appreciation for the fundamentals behind RFID, in particular with regards to circuit design and electromagnetic theory.

Thanks to everyone who helped me overcome my struggles with Latex, including Jade Wang, Ian Lai, and Mat Willmott.

Finally, I'd like to thank my family for their constant love and support and encouragement for continuing in my studies. I owe my biggest thanks to the love of my life, Alicia, who has been there beside me, every day, helping me in every possible way as I struggled to get this thesis written. She has listened to my complaints, comforted me through my bad moods, provided me with dinner when I otherwise would not have had time to eat, and encouraged me when I really needed it most. This thesis is dedicated to her.
## Contents

1 Introduction ........................................................................................................... 13
   1.1 Introduction ........................................................................................................ 13
   1.2 RFID Overview .................................................................................................. 14
      1.2.1 RFID and Packaging .................................................................................. 14
      1.2.2 Challenges of Pallet and Case Tagging ....................................................... 15
   1.3 Problem Statement ............................................................................................. 17
   1.4 The Field Probe ................................................................................................. 18
   1.5 Thesis Overview ................................................................................................. 19

2 Electromagnetic Theory ......................................................................................... 23
   2.1 Introduction ........................................................................................................ 23
   2.2 Fundamentals of Electromagnetic Wave Propagation ........................................... 23
   2.3 Electromagnetic Phenomenon in UHF RFID ..................................................... 26
      2.3.1 Antennas .................................................................................................... 27
      2.3.2 Backscatter ................................................................................................. 29
   2.4 Conclusion ........................................................................................................ 31

3 EPC Class 1 Generation 1 Protocol ...................................................................... 33
   3.1 Introduction ........................................................................................................ 33
   3.2 Air Interface ...................................................................................................... 33
      3.2.1 Reader to Tag Channel .............................................................................. 34
      3.2.2 Tag to Reader Channel .............................................................................. 34
   3.3 Protocol Commands .......................................................................................... 35
3.3.1 Command Format .................................................................. 36
3.3.2 Command Overview ............................................................. 36
3.3.3 Tag Response ................................................................. 37

4 Field Probe System Design and Implementation 39

4.1 Introduction ....................................................................... 39
4.2 Hardware Design .............................................................. 39
  4.2.1 Microprocessor ............................................................ 40
  4.2.2 Power Management ...................................................... 40
  4.2.3 Antenna .................................................................... 41
  4.2.4 Field Strength Indicator ................................................. 41
  4.2.5 Edge Detector .............................................................. 42
  4.2.6 Backscatter Modulator .................................................. 43
4.3 Firmware Design ............................................................... 44
  4.3.1 Data Communication .................................................... 44
  4.3.2 Periphery Devices ........................................................ 48
  4.3.3 Data Formatting ........................................................... 50
4.4 Data Visualization Program ............................................... 51

5 Applications and Experimental Results 55

5.1 Introduction .................................................................... 55
5.2 Electromagnetic Characterization of Room .......................... 56
5.3 Diagnostics ....................................................................... 58
5.4 Sinusoidal Behavior of Power Transmission through Layers of Varying Thickness ................................................. 59

6 Conclusions and Future Work 63

6.1 Conclusions .................................................................... 63
6.2 Future Work ................................................................. 64
  6.2.1 Read Range Improvement ............................................. 65
  6.2.2 EPC Class 1 Generation 2 ............................................. 65
List of Figures

2-1 Radiation patterns of an isotropic emitter and a dipole antenna . . . . 28
2-2 Equivalent circuit for a UHF tag with a dipole antenna ............. 30

3-1 Data encoding for reader to tag communication ..................... 35
3-2 Data encoding for tag to reader communication ..................... 35
3-3 EPC Class 1 Generation 1 reader command format .................... 36
3-4 Abridged state diagram for EPC Class 1 Generation 1 tag ........... 37
3-5 Tag response to ScrollID command .................................. 38

4-1 Schematic of analog circuitry in Field Probe ....................... 40
4-2 Finite state machine for reader command processing ............... 47
4-3 Data format for Field Probe’s EPC ID ............................... 53
4-4 Data format for Field Probe’s EPC ID ............................... 53

5-1 Setup for electromagnetic characterization of corridor ............ 56
5-2 Results for electromagnetic characterization of corridor ........... 57
5-3 Setup for fish tank experiment .................................... 60
5-4 Data results from fish tank experiment. The plot shows the induced voltage on the field as a function of the depth of the water in the fish tank. .................................................. 61
Chapter 1

Introduction

1.1 Introduction

This thesis presents the design, implementation, and application for a low cost, diagnostic hardware device that will be referred to as the Field Probe. This device emulates the functionality of a Class 1 Generation 1 UHF EPC radio frequency identification (RFID) tag. The Field Probe has an on board battery to power its logical and emulation functionality, a field strength sensor to detect the level of electromagnetic power received at its antenna, and several means by which to communicate this information to a user. Two human oriented feedback indicators are designed on the device: a LED bar to provide visual feedback of the field strength, and a pitch variable beeper to provide auditory feedback of the field strength.

The Field Probe is able to transmit its field strength data back to a reader using the RFID protocol. A computer program that interfaces with the reader software can then aggregate the data sent by all the Field Probes located within the reading zone of the reader, and generate a three dimensional view of the field strength in the environment, providing the user with the ability to “see” the electromagnetic field.

With the ability to visualize the electromagnetic field, the user now has the ability to see where the null points are that may be causing certain tags not to read. Using this image, the user can make subtle changes to the RFID portal (e.g., turn one reader antenna at a slight angle), and see what effect this has on the electromagnetic field.
distribution. Perhaps the null spot is removed, or perhaps it is moved to a point in space that is never occupied by a tag. The instantaneous feedback supplied by the Field Probe allows the user to make more informed decisions when designing RFID portals.

1.2 RFID Overview

RFID is a technology that has been around for over 60 years, and has generated increased interest in the past decade for a number of different applications. While RFID systems come in several different varieties, this thesis is primarily focused on passive UHF RFID systems. In such a system, an object is tagged by placing a battery-less (passive) tag with an embedded silicon chip and antenna on it. A device known as a reader emits a powerful UHF electromagnetic field through its own antenna. When the tag is within the reading zone of the reader, the reader’s electromagnetic field induces a voltage strong enough in the tag to activate the silicon chip. At this point, both reader and tag use the reader’s electromagnetic field as a channel to communicate information with each other. This allows the reader to identify the object to which the tag is attached. If multiple tags are present, the reader implements an arbitration algorithm that allows it to identify every tag.

1.2.1 RFID and Packaging

One application for RFID in particular has created a great deal of buzz in the past few years: inventory tracking in the supply chain. RFID promises to be a more efficient and ultimately more cost effective alternative to bar codes for tracking products inside the warehouse and as they are shipped from manufacturer to distributor. Since RFID does not require line of sight, each tagged case on a pallet could be identified nearly instantaneously without the need for someone to break down the pallet and scan each case individually. This minimization of human intervention in the inventory tracking process removes human error, speeds up the process of receiving and deploying tagged shipments, and automates the process of detecting stolen or misplaced
goods. Furthermore, with the use of shelf readers, product orders can be automatically generated when a certain product is nearly out of stock. All of these features help to greatly reduce many of the losses inherent to bar code inventory tracking.

In late 2003, Wal-Mart issued a mandate for its top 100 suppliers to place RFID tags on all the cases and pallets they shipped to Wal-Mart. The aim of this mandate was to 'jump-start' the widespread adoption of RFID in the supply chain. It helps establish a standard by which companies could begin to introduce RFID into their own warehouses. In particular, it requires that companies use EPC (Electronic Product Code) compliant tags for their products. Developed at the Auto-ID Center at MIT and licensed to EPCglobal, Inc., this open standard defines and standardizes several RFID protocols, as well as a versatile numbering system that integrates with the current UPC system encoded in bar codes. One of the RFID protocols developed by the Auto-ID Center was UHF EPC Class 1 Generation 1 (C1G1).

1.2.2 Challenges of Pallet and Case Tagging

While companies have many options as to how they want to integrate RFID into their existing infrastructure, they all face a similar set of fundamental challenges. The easiest method of integration is what is known as the ‘slap & ship’ method [11]. The basic idea is to keep their entire inventory process exactly the same up until the point when a pallet is ready to be shipped. Then the pallet is broken down, each case is identified, tags are programmed accordingly and applied to the cases, the tags are verified, the pallet is rebuilt, a pallet tag is generated and applied, and then the pallet load is shipped. Though a more integrated RFID implementation would be more beneficial and cost-effective in the long run, no matter what approach is taken, most companies have to deal with several fundamental issues to guarantee the highest possible readability when the pallet load reaches the Wal-Mart distribution center:

- Tag placement on cases
- Product stacking within cases
- Case stacking on the pallet
- The use of special tags for certain products containing water or metal.

For companies that want to optimize reading tags also at their own facilities, they must also consider: reader antenna placement, proximity of sources of electromagnetic interference, and proximity of walls and other objects in the environment (including humans).

For the most part, the largest problem with reading tags on a pallet is that not enough power is reaching the tag in question. Oftentimes, the tags on cases embedded inside the pallet are the ones that end up not being read. Assuming that the tag is within range in which it should be able to be read, there are several factors that might cause a particular tag not to receive enough power:

- Reflections at media boundaries between tag and reader antenna
- Multi-path interference
- De-tuning of tag antenna from nearby conductive objects

Reflections play a major role in reduced performance of RFID systems. For any incident wave onto a media boundary, a certain percentage of the power will be transmitted in the media, and the rest is reflected back. Those percentages depend on the angle of incidence, and the relative permittivity and permeability of the two media. A good example of an instance where this may be a problem is at the boundary between air and water. Water has a much higher permittivity than air, making it more difficult for higher frequency electromagnetic waves to penetrate.

Reflections from objects in the environment can also cause multi-path interference. For example, a nearby wall might reflect some of the energy produced by the reader, causing the incident and reflected waves to interfere with one another. At points where the two waves are 180° out of phase, they will cancel each other, producing a null point where very little to no power is available for the tag.

Certain antenna topologies can be very prone to de-tuning from nearby metals. Tag antennas are designed to be very resonant in the frequency ranges of operation (for example 902 to 928 MHz) to allow for the maximal transfer of power from the
electromagnetic wave to the tag's silicon chip. If the antenna becomes de-tuned, the antenna will not draw as much energy, and the tag may no longer operate in the reader's frequency range.

1.3 Problem Statement

The greatest benefits RFID offers to the supply chain are achieved with nearly 100% tag read rates. Setting up and maintaining systems that achieve this level of read reliability can be very difficult, largely due to the fact that the propagation of UHF electromagnetic waves is greatly affected by the various materials it encounters. In other words, a particular setup which works well for identifying tagged cases of breakfast cereal may suddenly experience lower readability when a forklift is nearby, or may have no readability at all for tagged cases of bottled water. The interactions between electromagnetic waves and media can be very complicated and nonintuitive to the typical user of such systems. As a result, a market for RFID consulting has emerged to help companies install these systems in their facilities.

However, a growing number of companies have become interested in developing their own RFID processes internally so that they become better educated about RFID technology and less dependent on RFID consultants. To do this, they need to develop an intuition for how electromagnetic waves are generally going to work in particular situations, and be able to evaluate how their set-ups are performing. Up until now, the only practical way of doing this has been by a trial and error process where the only measurable parameter of success is the percentage of read tags in a pallet. What is needed is something to provide a more detailed picture of how the electromagnetic field is propagating within a certain volume of space.

This is the motivation behind the development of the Field Probe. This device is meant to be used as a diagnostic tool, and as an education tool for developing intuitions when it comes to how electromagnetic fields are going to behave in the presence of certain materials. A good analogy is that of lighting a theater stage. The lighting director wants to position his lights in such a way to eliminate as many
shadows as possible. Similarly, an RFID user wants to eliminate as many shadows, or energy null points, from his pallet of products as possible in order to maximize readability.

1.4 The Field Probe

The Field Probe goes farther than currently available commercial systems that are simple energy detectors. In addition to having a LED bar to provide immediate visual feedback of the field strength, the Field Probe also is able to communicate to an RFID reader using the EPC UHF Class 1 Generation 1 protocol. Thus, the Field Probe is a tag emulator. This innovation allows for greater flexibility in how the data the field probe collects can be used.

Powered by a lithium cell battery, the Field Probe consists of a micro-strip folded dipole antenna connected to discrete RF circuitry and a microprocessor to handle the protocol and sample a voltage doubling circuit that is proportional to the strength of the electromagnetic field. This value is then stored in the two least significant bytes of the Field Probe’s 8 byte EPC ID. In addition, a special header byte is used in the ID to distinguish the field probe from a typical EPC tag. When an RFID reader issues a command for all the tags nearby to report their ID, the Field Probe responds with its ID. Once the reader has the Field Probe’s ID, the user can directly read the field strength value, or a third party software program interacting with the reader could collect all the data reported by multiple Field Probes, and then display a three dimensional color plot of the field strength. This detailed information provides instantaneous feedback as to how certain actions (such as moving the position of one reader antenna) are effecting the overall propagation of electromagnetic energy into the pallet.

The Field Probe can also be used a research platform where other sensors or metrics can be added in order to quantify both the strength of the field as well as the quality of the EPC protocol signals it’s receiving. Physical quantities such as temperature and humidity, as well as quantities that characterize the noisiness of
the communication channel between the Field Probe and the reader could also be measured and encoded in the Field Probe ID. Such information would be invaluable for diagnostic testing.

1.5 Thesis Overview

This thesis has been organized to provide the reader with a fundamental, general understanding of the principles behind RFID before delving into the specifics of the Field Probe and its applications.

Chapter 2 provides an introduction to electromagnetics, and some of the important principles that make UHF RFID possible. Though it is not a detailed treatment, this chapter provides a good foundation for understanding some electromagnetic fundamentals, and provides pointers to references that go more in depth. Additionally, this chapter gives a broad overview of antennas, and presents the topic of backscatter modulation, a critical principle for the design and operation of UHF tags.

The EPC Class 1 Generation 1 Protocol is presented in Chapter 3. This chapter presents the modulation schemes used by both the reader and the tag, along with the command protocol. The information in this chapter is important for understanding the firmware code in Chapter 4. The key points are that the protocol is a reader talk first (RTF) protocol, meaning that tags are designed to listen, and only respond when a command is issued to them. All responses and state transitions are entirely determined by the reader, and this is reflected in the design of the Field Probe's firmware.

Chapter 4 details the design and implementation of the entire field probe system. This chapter encompasses the majority of the development work that went into designing the various components of the Field Probe system, and is divided into three main sections: hardware, firmware, and software.

First, the hardware of the Field Probe is presented and discussed. The field probe's hardware went through many different generations, starting first as a simple, cheap field strength indicator with a single LED and no ability to communicate through
an RFID protocol. Then a demodulator and modulator were added, providing the ability to communicate data; though initially, these reads were sporadic, and only occurred at close range. Finally, additional feedback was added in the form of an LED bar and beeper. Ultimately, the majority of the work done on hardware design was spent on designing and redesigning the backscatter modulator in an attempt to improve the read range.

An overview of the Field Probe’s firmware is given next. The firmware can be divided up into several major components: implementing the EPC C1G1 protocol, periphery device control, and updating the EPC ID to transmit field strength measurements. By far, implementing EPC C1G1 was the largest, and most difficult piece of firmware to write. It required very careful timing not only to properly receive reader commands, but also for responding, because if the Field Probes did not respond at the exact right time, the ability of the reader to implement anti-collision among a mixed population of tags and Field Probes was entirely thrown off. Eventually, after many revisions, the firmware performed all of these duties quite well.

Finally, a brief summary is given of the Visual Basic program used to aggregate the field strength results of multiple Field Probes simultaneously. Though not the most exceptional piece of code writing (the author is not a software programmer by nature), the VB program demonstrated how the field strength readings stored in the Field Probe IDs could be color coded and displayed in a three dimensional grid, providing detailed feedback to the user on the quality of the electromagnetic field within a volume of interest, such as a pallet for example.

Applications for the Field Probe, along with some experimental results obtained with the Field Probe are given in Chapter 5. First, an experiment designed to demonstrate the Field Probe’s abilities and limitations is presented along with results. Then, several research projects and demonstrations conducted at the MIT Auto-ID Labs with the aid of the Field Probe are summarized, providing several different applications in which the Field Probe can be used.

Finally, Chapter 6 provides some conclusions drawn from the development of the Field Probe, along with some future work that could be done to improve it. The
three key conclusions drawn from this research are as follows. First, as the use of RFID technology becomes more widespread, so must a general sense of intuition with regards to the physics behind RFID. The interactions between electromagnetic fields and materials can be complicated and difficult to analyze, but oftentimes there are generalized principles that explain certain behaviors, and being able to interactively explore these principles can greatly improve understanding and influence better RFID design. Second, the Field Probe, in spite of some known limitations, does provide useful data that provides not only useful feedback to the electromagnetic performance of a particular setup or environment, but also aids in the development of this intuition. This device gives the user the ability to visualize the electromagnetic field, and thus immediately see the effects certain environmental configurations have on electromagnetic field propagation. Finally, just as there is no single solution to tagging cases in pallets, the Field Probe itself is not in it of itself a complete solution to RFID diagnostics, but rather is used best in conjunction with other diagnostic tools, such as an RFID graphical simulation package. The Field Probe is great for getting quick experimental results, but sometimes its quicker to gain insight through simulations, which can then be verified by the Field Probe.
Chapter 2

Electromagnetic Theory

2.1 Introduction

A deeper understanding into the inner workings of RFID requires some basic electromagnetic and antenna theory. This chapter is organized to provide a brief overview of some of the principles and corresponding equations relevant to RFID. For a more detailed treatment, the author recommends any introductory electromagnetism book, and in particular [9] which focuses primarily on electromagnetism in the UHF range.

2.2 Fundamentals of Electromagnetic Wave Propagation

Most introductions to basic electromagnetism begin with Maxwell’s equations. These equations, in either integral or differential form, provide the foundation upon which all of electromagnetic theory is based. They equations describe the coupled nature of the electric and magnetic fields, and relate them to their two sources: the electric current density $\vec{J}$ and the electric charge density $\rho$. Most of the derivations that follow in this chapter come from [6].
\[ \nabla \times \vec{H}(\vec{r}, t) = \frac{\partial}{\partial t} \vec{D}(\vec{r}, t) + \vec{J}(\vec{r}, t) \]  
(2.1)

\[ \nabla \times \vec{E}(\vec{r}, t) = -\frac{\partial}{\partial t} \vec{B}(\vec{r}, t) \]  
(2.2)

\[ \nabla \cdot \vec{D}(\vec{r}, t) = \rho(\vec{r}, t) \]  
(2.3)

\[ \nabla \cdot \vec{B} = 0 \]  
(2.4)

Equations (2.1) - (2.4) are linear, but not independent. By taking the divergence of (2.2), we arrive at (2.4). Similarly, by taking the divergence of (2.1), we derive the continuity of charge of law:

\[ \nabla \cdot \vec{J}(\vec{r}, t) = -\frac{\partial}{\partial t} \rho(\vec{r}, t) \]  
(2.5)

This law simply states that the decrease in charge density at a single point is equivalent to the divergence of current from an infinitesimal volume around that point.

From this point on, the field dependencies on space and time will be assumed, and left out of the notation.

The constitutive equations characterize the media that electromagnetic waves travel through by relating the electric field and magnetic field intensities to the electric and magnetic flux densities. In their most general form, they are:

\[ \vec{D} = \varepsilon \cdot \vec{E} + \xi \cdot \vec{H} \]  
(2.6)

\[ \vec{B} = \mu \cdot \vec{H} + \mu \cdot \vec{E} \]  
(2.7)

The most general form of media, bianisotropic media, is described by (2.6) and (2.7). In this kind of media, the electric and magnetic fields can be cross-coupled, and \( \vec{E} \) and \( \vec{H} \) are not necessarily parallel to \( \vec{D} \) and \( \vec{B} \) respectively. In general, however, most media can be modeled as isotropic media, where the cross coupling does not exist and
the permittivity tensor $\bar{\varepsilon}$ and the permeability tensor $\bar{\mu}$ are replaced by scalar values:

\begin{align}
\bar{D} &= \varepsilon\bar{E} \\
\bar{B} &= \mu\bar{H}
\end{align}

(2.8) \hspace{1cm} (2.9)

In isotropic free space, $\varepsilon = \varepsilon_o \approx 8.85 \times 10^{-12}$ farad/meter, and $\mu = \mu_o = 4\pi \times 10^{-7}$ henry/meter.

If we consider a source free region of space, where $\rho = 0$ and $\bar{J} = 0$, equations (2.1) - (2.4) simplify to:

\begin{align}
\nabla \times \bar{H} &= -\frac{\partial}{\partial t} \bar{E} \\
\nabla \times \bar{E} &= -\mu_o \frac{\partial}{\partial t} \bar{H} \\
\nabla \cdot \bar{E} &= 0 \\
\nabla \cdot \bar{H} &= 0
\end{align}

(2.10) \hspace{1cm} (2.11) \hspace{1cm} (2.12) \hspace{1cm} (2.13)

By substituting (2.11) into (2.10), and doing some rearranging, we arrive at the Helmholtz wave equation:

\begin{equation}
\nabla^2 \bar{E} - \mu_o \varepsilon_o \frac{\partial^2}{\partial t^2} \bar{E} = 0 \\
\end{equation}

(2.14)

From this equation we can solve for the electric field, and consequently, the magnetic field. If we choose our coordinate system such that the electromagnetic wave propagates in the $\hat{z}$ direction, and the electric field points in the $\hat{x}$ direction, the simplest solution takes the form:

\begin{equation}
\bar{E} = \hat{x}E_x(z, t) = \hat{x}E_x \cos(kz - \omega t)
\end{equation}

(2.15)

where $k$ is the spatial frequency of the electromagnetic wave, or wavenumber, and $\omega$ is the temporal or angular frequency. The wavenumber $k$ is related to the
wavelength $\lambda$ by:

\[ k = \frac{2\pi}{\lambda} \tag{2.16} \]

and the angular frequency $\omega$ is related to the Hertzian frequency $f$ by:

\[ \omega = 2\pi f \tag{2.17} \]

Substituting (2.15) into (2.14) yields the dispersion relation for free space:

\[ k^2 = \omega^2 \mu_0 \varepsilon_0 \tag{2.18} \]

The dispersion relation provides insight as to how the electromagnetic wave will propagate through a particular medium.

By plugging the solution for the electric field (2.15) into (2.11), we find a solution for the magnetic field:

\[ \vec{H} = \hat{y} \sqrt{\frac{\varepsilon_0}{\mu_0}} E_0 \cos(kz - \omega t) \tag{2.19} \]

The electric and magnetic fields are orthogonal to one another.

The Poynting vector, calculated as the cross product of the electric and magnetic fields, defines the direction of energy flow for an electromagnetic wave, with its magnitude equal to the power density through a surface normal to its direction. For the electric and magnetic fields in (2.15) and (2.19), the Poynting vector is:

\[ \vec{S} = \vec{E} \times \vec{H} = \hat{z} \frac{\varepsilon_0}{\mu_0} E_0^2 \cos^2(kz - \omega t) \tag{2.20} \]

\section*{2.3 Electromagnetic Phenomenon in UHF RFID}

This section will highlight several key areas of electromagnetism relevant to UHF RFID systems. The background here will provide a foundation for understanding the design of the field probe and the principles behind its operation. First I will give a
brief overview of antennas and their characterizing parameters. Then I will explore the principle of backscatter and how it allows UHF tags to passively transmit data back to the reader.

2.3.1 Antennas

John D. Kraus, whose book on antennas is considered by many to be one of the best, defines a radio antenna as a "structure associated with the region of transition between a guided wave and a free-space wave, or vice versa." [7] In terms of radio waves, antennas are the link between either the transmitter or receiver, and free space. This is of fundamental importance for RFID, because not only is data transmitted from a reader antenna to a tag antenna, but power as well. The topic of antennas is vast and detailed; this section will only provide a brief overview of some of the key parameters that help characterize antennas.

One key parameter that characterizes an antenna is its radiation pattern. First, let's consider the simplest antenna, a point source emitting perfectly spherical electromagnetic waves, known as an isotropic emitter. Though such an antenna does not exist in reality (a point source violates the law of electric conversation!), it provides a useful comparison for real antennas.

If we define the total radiated power by an isotropic emitter as \( P_{EIRP} \) (where EIRP stands for the effective isotropic radiated power), we can calculate the power density at a given distance \( r \) as:

\[
S = \frac{P_{EIRP}}{4\pi r^2} \tag{2.21}
\]

Since the radiated power density is equivalent in all directions for a particular distance \( r \), this antenna has a spherical radiation pattern.

Real antennas cannot achieve a spherical radiation pattern. In the case of a dipole antenna, as shown in Figure 2-1 (taken from [3]), the radiation pattern takes on torus-like shape. Also shown in this figure is an isotropic radiator that is emitting the same total radiated power (the surface integral of the power density over a closed surface...
around the antenna) as the dipole antenna.

Figure 2-1: Radiation patterns of an isotropic emitter and a dipole antenna

Comparing the two radiation patterns, we can now define two useful quantities: directivity and gain. Gain is the ratio between the radiated power density of the antenna of interest in a particular direction and some reference antenna of known gain that has the same transmission power. In this example, we are using an isotropic radiator as our reference antenna, and the resulting gain would be expressed in units of dBi (decibels over isotropic). Directivity, on the other hand, is the ratio between the maximum power density of a particular antenna over its average directional power density (or equivalently, the maximum theoretical gain of an antenna), and is always greater than unity, with higher values corresponding to more strongly directional antennas. In practice, directivity is an ideal value which defines how strongly an antenna focuses its radiation power in one particular direction, while gain is an actual quantity that includes not just the radiation pattern of the antenna, but losses that are causes by impedance mismatching and heat dissipation in the antenna. An antenna’s efficiency factor is the ratio of the antenna’s gain to its directivity, and is always less than unity.

So far we have only looked at how the energy is transmitted and received by
the antenna through free space. Another important antenna parameter is its input impedance. This is the impedance of that a circuit connected to the antenna sees. If the impedances of the antenna and the corresponding circuit are not matched (i.e., the real component is equal, and the imaginary component are opposite in sign), power can be reflected or dissipated, thus lowering the antenna’s effective gain and efficiency. This is of great importance for tag antennas, where maximal power transfer is needed to achieve the greatest possible read distance.

### 2.3.2 Backscatter

RFID tags that operate in the HF range are able to passively communicate data by switching their load impedance, which in turn is detectable on the reader’s antenna due to the inductive coupling between the two antennas. For UHF tags, however, since no such coupling exists, tags must use a technique similar to how radar antennas can detect distant objects: backscatter.

First I shall define the effective and scatter apertures of a UHF tag. Let $P_e$ be the power absorbed by the tag. The effective aperture defines the equivalent area over which the power density $S$ travels through to generate the power $P_e$ received by the tag. The equation for effective aperture is given as:

$$A_e = \frac{P_e}{S}$$

(2.22)

Similarly, the power that is reflected, or scattered, by the tag is a product of the power density $S$ and the scattering aperture $A_s$:

$$A_s = \frac{P_r}{S}$$

(2.23)

We will now derive more precise expressions for these apertures to gain some insight into how backscatter modulation. Figure 2-2 from [3] shows an equivalent circuit model of a UHF tag. On one side of the figure is the load transponder circuitry corresponding to the UHF tag, represented as an impedance with real component $R_t$, and imaginary component $X_t$. On the other side is the antenna, represented as an
impedance, with real component \( R_r \) and imaginary component \( X_a \), in series with a loss resistance \( R_o \). The loss resistance represents all the ohmic losses that dissipate as heat on the antenna. The real part of the antenna impedance \( R_a \) is also known as the radiation resistance. The power that flows through it is radiated, becoming the scattered power that the UHF tag uses to communicate data. The voltage \( U_o \) is the voltage induced on the antenna by an incoming electromagnetic wave.

![Fig 2-2: Equivalent circuit for a UHF tag with a dipole antenna](image)

From [3] the effective and scatter apertures for the UHF tag in Figure 2-2 are as follows:

\[
A_e = \frac{U_o^2 \cdot R_t}{S \cdot [(R_r + R_t + R_r)^2 + (X_a + X_t)^2]} \quad (2.24)
\]

\[
A_s = \frac{U_o^2 \cdot R_r}{S \cdot [(R_r + R_t + R_r)^2 + (X_a + X_t)^2]} \quad (2.25)
\]

Let’s first assume impedance matching conditions, with a lossless antenna, as follows:

\[
R_t = R_r \quad (2.26)
\]

\[
X_t = -X_a \quad (2.27)
\]

\[
R_o = 0 \quad (2.28)
\]
Then (2.24) and (2.25) reduce to:

\[ A_e = A_s = \frac{U_0^2}{4SR_r} \]  

(2.29)

We see that half of the total power drawn from the electromagnetic field by the antenna is delivered to the tag’s circuitry, while the other half is scattered. This condition is referred to as maximum power transfer [7].

Now let’s look at the scatter aperture for two special cases of load resistances [3].

For \( Z_t = 0 \):

\[ A_{s_{max}} = \frac{U_0^2}{SR_r} \]  

(2.30)

For \( Z_t = \infty \):

\[ A_{s_{min}} = 0 \]  

(2.31)

Thus, depending on the load impedance, the scatter aperture can take on a wide range of values. This is the principle behind backscatter modulation: using a transistor, a load (resistive, capacitive, or a short) can be switched across the antenna terminal. The resulting change in scattered power is detected by the reader antenna, and demodulated into a data signal.

### 2.4 Conclusion

This chapter touched on several important electromagnetic principles that UHF RFID systems rely on to work. In particular, for designing a UHF tag, two of the most important components that determine overall performance are the tag’s antenna, and the matching network used to match it to the load circuit. The antenna’s geometry, the material it’s made from, the substrate on which it’s placed all factor into its radiation pattern, the size of its apertures, and its resonance. The matching between the antenna and the load circuit determine how much power received by the antenna is transferred to the tag’s circuit, as well as how strongly data can be backscattered.
to the reader’s antenna.
Chapter 3

EPC Class 1 Generation 1 Protocol

3.1 Introduction

One of the standards that the Auto-ID Center created was the EPC Class 1 Generation 1 protocol. Two requirements that a sustainable, cost-effective EPC RFID system needed in its protocol were that the command set should be small and simple in order to keep chip costs low on the tag side, but not so small that quick anti-collision algorithms could not be realized. The EPC Class 1 Generation 1 protocol achieves these requirements with a rather straightforward and intuitive implementation. This chapter will highlight the features of this protocol, and provide the framework for how the firmware of the field probe was designed in order to interpret the signals it received from the reader, and send data back.

3.2 Air Interface

The air interface of the protocol is the physical means by which data is transmitted between two objects. The electromagnetic waves emitted by the reader to power the tag serve also as a data carrier. A number of different methods can be used to send data over a radio wave, including amplitude shift keying (ASK), frequency shift keying (FSK), and phase shift keying (PSK). In each of these methods, some particular parameter of the electromagnetic wave is shifted between several states.
(often just two binary states) at some data rate. In the case of the reader to tag data channel, ASK is implemented on the electromagnetic waves the reader antenna is producing. In the case of the tag to reader data channel, the tag uses FSK to alter its backscatter cross-section and thus transmit data back to the reader via the changes in reflected energy that the reader receives.

The various timing parameters associated with the protocol differ between the European and North American implementations. All research was focused on North American readers and tags, so only the North American version of the protocol was implemented on the field probe. This section will only focus on several key parameters, such as data rate and the signal representation of the bits 1 and 0. For further timing parameters such as rise and fall times etc., consult [8] found at the EPCGlobal website.

3.2.1 Reader to Tag Channel

There are several major parameters that define the reader to tag channel. As stated, data is communicated through ASK modulation with a modulation depth of 100%. For North America, the data rate is 62.5 bps, with a bit period \( T_o \) being 16 microseconds nominally. This protocol allows for variations of the bit rate within a given (though somewhat unclear) tolerance; a compliant tag must be able to sync up to the appropriate data rate. Bits themselves are encoded as pulses of differing widths within the bit frame. A zero is represented by a pulse with a width of \( \frac{1}{8} T_o \), and a one is represented by a pulse with a width of \( \frac{3}{8} T_o \), as shown in Figure 3-1.

3.2.2 Tag to Reader Channel

There are several major parameters that define the tag to reader channel. The data is communicated through FSK modulation, with the tag switching its backscatter cross-section between two states (matched and mismatched). For North America, the specification defines the bit period as 14.25 \( \mu s \), though in practice it is typically 16 \( \mu s \). Additionally, the protocol allows for the data rate of this channel to shift up or down up to 25% of its nominal value to account for oscillator drift that may
occur in the tag. A 'zero' bit is represented by a frequency of approximately 70.2 KHz according to the specification (62.5 KHz typically in practice). A 'one' bit is represented by a frequency of approximately 140.4 KHz according to the specification (125 KHz typically in practice). The timing for both a 'one' and 'zero' bit is shown in Figure 3-2.

Figure 3-1: Data encoding for reader to tag communication

Figure 3-2: Data encoding for tag to reader communication

3.3 Protocol Commands

The protocol is designed to have a small, simple command set. This limits the amount of state information that tags must retain when they begin communicating with the reader, and simplifies the amount of circuitry needed by the tag to process
the commands, saving in both tag cost, and amount of power needed to operate.

### 3.3.1 Command Format

```
CLKSYNC SOF COMMAND P1 POINTER P2 LENGTH P3 VALUE P4 P5 EOF
```

Figure 3-3: EPC Class 1 Generation 1 reader command format

All commands follow the general format in Figure 3-3. The [CLKSYNC] field (also known as [SPINUP]) is a 10-20 bit length field, consisting entirely of logical zeroes. This field is meant to provide a sync clock for the UHF tag. The [SOF] is a single logical one. The command field [CMD] contains an eight bit command, like the ones listed above. This is followed by an odd parity bit [P1], calculated over [CMD]. The pointer field [PTR] points to the starting bit address in the Tag ID to which the mask value is to be compared. This is followed by an odd parity bit [P2], calculated over [PTR]. The length field [LEN] contains the length, in bits, of the [VALUE] field. This is followed by an odd parity bit [P3], calculated over [LEN]. The value field [VALUE] contains the mask value which the tag uses to compare to its own ID (starting at the bit address pointed to by [PTR]). This is followed by an odd parity bit [P4], calculated over [VALUE]. This is followed by another odd parity bit [P5], calculated over the previous four parity bits. Finally, the [EOF] is a single logical one.

### 3.3.2 Command Overview

For purposes of this thesis, there are only three tag states of interest (other states not mentioned pertain to the programming and killing the tag). The following commands are used in identifying tags in the reader's field:

- Quiet Command
- Talk Command
- ScrollID Command
• PingID Command

Figure 3-4 shows an abbreviated state transition diagram for the tag. When the tag first powers up, it is in the Awake state. This means that the tag will respond to any command with a mask matching its own ID. If it receives a Quiet Command, it will transit to the Asleep state. In this state, the tag will only respond to a Talk command. From the Awake state, the tag will respond to either the ScrollID or PingID commands. Both commands put the tag into the Reply state, and elicit some kind of response from the tag. Upon completing the response, the tag returns to the Awake state.

![State Transition Diagram](image)

Figure 3-4: Abridged state diagram for EPC Class 1 Generation 1 tag

3.3.3 Tag Response

Only two of the commands of interest elicit a response from the tag: the ScrollID command and the PingID command. In the case of the ScrollID command, the tag will respond with its entire ID. The tag reply to this command is shown in Figure 3-5. The preamble is a one byte value that is always set to 0xFE. The crc-16 is a two byte cyclic redundancy check, calculated over the entire length of the tag’s ID as specified in [8]. The ID is either a 64 bit or 96 bit long EPC ID.

In response to the PingID command, the tag only transmits the 8 bits that follow the last bit of the ID mask sent by the reader. Additionally, the tag uses the three
most significant bits of these 8 bits to determine which of 8 time bins to respond in after the PingID command. This command is meant to aid in the process of anti-collision.
Chapter 4

Field Probe System Design and Implementation

4.1 Introduction

Designing the Field Probe required building a number of smaller systems. First the hardware needed to be designed such that the RF field could be measured, and signals could be demodulated and modulated. Then the firmware had to be designed to control the field strength sampling, interpret the received signals, and implement the EPC Class 1 Generation 1 protocol. Finally, a software program needed to be written to interact with a standard reader, organize the data being received from the Field Probes, and graphically display it. This overall system could then be used as a powerful tool for both learning about RFID, and performing diagnostics.

4.2 Hardware Design

The hardware design itself contains a number of components that were designed and redesigned over the course of a year. The Field Probe PCB board went through a number of iterations as various analog circuit topologies were tested and evaluated. There are six main components to the Field Probe: the microprocessor, the power management chip, the antenna, field strength measurement circuit, the edge detector
circuit, and the backscatter circuit. A schematic of the analog circuitry is given in Figure 4-1. The components are grouped together into their corresponding circuits. The names DIN (data input), DOUT (data output), and FS (field strength reading) correspond to points which connect to I/O pins of the microprocessor.

![Schematic of analog circuitry in Field Probe](image)

Figure 4-1: Schematic of analog circuitry in Field Probe

### 4.2.1 Microprocessor

The most important requirement for the microprocessor was that it needed to have the computation power to handle implementing the EPC protocol, low power consumption, and a certain number of I/O pins to handle periphery devices, such as an LED bar, a beeper, or dip switches to control setting the Field Probe’s ID. The PIC16F876A was chosen for two main reasons: it reasonably satisfied these requirements, and the author possessed a great deal of familiarity with this chip. Certainly though, a number of processors exist that may have been better suited for this application (either due to lower cost, smaller size, or lower power consumption). However, this microprocessor has proven to be reliable and fairly straightforward to use.

### 4.2.2 Power Management

The Field Probe was designed to be battery operated since semi-passive tags should have a huge read distance (upwards of 10 meters), making the Field Probe well suited
for applications where measurements are needed deep inside a pallet of electromagnetic unfriendly material. A single 3-volt lithium coin cell battery was chosen over other types of batteries because of its light weight and thin profile. On average, this battery seemed to provide several hours of life for the final version of the Field Probe, though some leaking current did exist, causing it to be necessary to remove the battery when the Field Probe was not to be used for long periods of time.

One concern with the Field Probe being battery operated was that as the battery began to drain of power, the field strength measurements would begin to be skewed. Thus it was important to have a rectifying chip with a stable output voltage over a range of input voltages. Two chips were tested for this purpose, both from TI: the TPS60204 which outputted $3.3$ V, and the TPS60140 which outputted $5$ V. Ultimately the TPS60204 was chosen as the better of the two chips because the other chip dissipated the lithium coin cell battery much too fast, and the increased voltage did nothing to improve the read range as I thought it might.

4.2.3 Antenna

Two different antenna types were used on the Field Probe: the half-lambda dipole, and the folded half-lambda dipole. The former was used in earlier implementations of the Field Probe, but later I switched over to the folded half-lambda dipole because the real part of its impedance was larger (approximately 300 ohms, as compared to 75 ohms) which ultimately matched better with my circuitry. One of the nice abilities one has with the Field Probe is to fabricate a board with no antenna, and then using a copper tape cutter, try out various antenna designs that may be well suited for particular applications.

4.2.4 Field Strength Indicator

To measure the field strength, a simple rectification circuit known as a Schottky diode doubler is used. All passive RFID tags must have some kind of rectifying circuit connected to the antenna from which it can derive a DC voltage. The Field
Probe has its own power source, so it simply uses this rectified voltage as an indicator of the strength of the electromagnetic field in the vicinity of the Field Probe. The microprocessor samples the analog voltage on the line FS, and sends the corresponding digital value to the reader. This digital value can then be correlated to an approximate field strength through the use of correlation graphs found in [1] or by taking some experimental measurements.

4.2.5 Edge Detector

The edge detector circuit takes an incoming modulated RF signal, and effectively filters out the carrier and amplifies the modulation itself up to logic power levels. The topology of this circuit remained unchanged through the many board iterations, but the values of the components were often tweaked to maximize read distance.

The circuit functions as follows. Referring back to Figure 4-1, each input of the op-amp has a resistor-capacitor pair with a particular time constant. The time constant of R2 and C2 on the negative input is designed to be several orders of magnitude smaller than the time constant of R4 and C4 on the positive input. Additionally, R3 and R4 create a resistor divider network such that in steady state, the voltage across C2 is slightly larger than the voltage across C4. Thus, when the electromagnetic field is on without any modulation, the output of the op-amp will be high.

When the 100% modulation appears, the voltage input into this circuit drops down to zero. The voltage across C2 will drop almost immediately due to the fast time constant, while the voltage across C4 will hold longer due to its slow time constant. The result is that the output of the op-amp drops to the negative rail (in this case zero), where it stays until the field turns back on. The slow time constant must be much longer than the length of the longest expected modulated pulse, which is 6 μs, otherwise glitches will appear.

The values of the components of this circuit must be chosen carefully, because a very robust circuit (one which causes few glitches) may not be sensitive enough to detect a weak signal, whereas a sensitive circuit might be too vulnerable to a noisy
4.2.6 Backscatter Modulator

Perhaps one of the most difficult tasks in creating the Field Probe was designing a good backscatter circuit. The backscatter circuit must be able to switch the radar cross-section of the Field Probe as seen by the reader. One way of doing this is to switch between the antenna and the circuitry being matched and mismatched. When matched, the circuit absorbs more energy and reflects less back to the reader. When mismatched, more energy is reflected at the boundary between the antenna and the circuit. The reader can detect these changes, and interpret the frequency-modulated signal that is being sent.

Early on, based on some theoretical circuit diagrams I had encountered in my research, I designed this circuit by placing a transistor directly across the terminals of the antenna. The idea was that when the transistor was off, the circuit was matched, and when the transistor was on, it shorted the antenna terminals and the circuit was mismatched. This had a very poor performance in terms of any power being induced on the field strength detector circuit, or seeing any signals coming from the reader. I put a medium sized resistor (about 2 KΩ) in series with the transistor, which improved the performance somewhat, yielding approximately 1 meter of read range.

Ultimately, the backscatter circuit had to be redesigned, because I had made the implicit assumption that in its off state, the transistor was behaving like an open circuit. However, it appears to only behave like an open circuit at DC frequencies, and increasingly more like a short circuit at higher frequencies (in particular at 915 MHz). As a result, I began researching other possible backscatter topologies.

Ultimately I implemented a circuit similar to one discussed in a paper by RFID researcher Dr. Peter Cole from the University of Adelaide, Australia [2]. This design, shown in Figure 4-1 puts the backscatter transistor after a diode rectifying circuitry, instead of across the antenna terminals. Thus, the transistor only sees a DC signal across it, resolving the issue of shorting the entire circuit at high frequencies. When
the transistor switches on, the load resistance as seen by the antenna drops dramatically, creating the mismatch necessary to modulate data back to the reader. This new circuit allowed for a greater read range (approximately 2 to 3 meters), though still short of the desired goal of greater than 10 meters.

4.3 Firmware Design

Designing the firmware to implement the EPC Class 1 Generation 1 protocol was a difficult task in itself; a lot of careful timing was needed in order to properly interpret the commands as they were being sent. Additionally, receiving and sending data had to be coordinated with controlling periphery devices (field strength indicator, LED, beeper, etc.), and inserting the field strength readings into the EPC ID format. The implementation of each of these parts of the firmware is described in depth in the following subsections. All of the firmware was written in either the PIC assembly language, or in PIC C (a variant of the C programming language designed specifically for the PIC microprocessor). Within the text of this thesis however, pseudo-code is used to illustrate the overall firmware architecture and program flow.

4.3.1 Data Communication

The bulk of the PIC microprocessor’s firmware code is dedicated to implementing the EPC Class 1 Generation 1 protocol. This is handled entirely by one of the PIC microprocessor’s interrupt service routines (ISR). The interrupt is triggered by a falling edge on the external interrupt input pin, DIN. Referring back to Figure 3-1, a falling edge corresponds to the start of a data bit. The ISR is designed to process each of the reader’s data bits, one at a time.

The functions of the ISR are divided up into three sections. Section 4.3.1 describes how the bit is read and validated based on the timing parameters listed in [8]. Section 4.3.1 describes how the ISR processes the data bit in the context of the current field of the reader command packet being received using a finite state machine (FSM). Finally, Section 4.3.1 describes how, once the entire reader command packet has been...
received, the ISR decides the appropriate action to take.

Data Bit Interpretation and Validation

The microprocessor must be able to distinguish valid data signals from random noise in the environment. To accomplish this, the Timer 1 Module of the PIC microprocessor is used to measure the duration of the pulses and elapsed time between pulses. The output of the edge detector circuit is fed into two pins of the microprocessor. One pin is set as the external interrupt pin; whenever a falling edge is detected on this pin, the interrupt is triggered. The other pin is set as a capture pin; whenever a rising edge is detected, the current value of the Timer 1 is stored in a special capture register.

The interrupt is triggered at the beginning (falling edge) of a data pulse. The current value of Timer 1 is immediately stored, and then Timer 1 is cleared. This stored value corresponds to the total time duration of the bit frame (the time between two consecutive falling edges). Likewise, the value in the Timer 1 capture register is stored, and the Timer 1 capture register is cleared. This value corresponds to the time duration of the data pulse of the previous bit.

Once these values have been read in, the bit is validated and identified. Since most UHF EPC C1G1 readers seem to use a bit frame of either 14.25 or 16 microseconds, this tolerance is set to approximately between 13 and 17 microseconds. If the bit frame is invalid, the ISR ignores the bit, exits, and waits for a new falling edge. Otherwise, if the bit frame is valid, the pulse width (the value derived from the Timer 1 capture register) is then used to determine whether the bit is a zero or one. If the pulse width is longer than a certain tolerance, the bit is considered a 'one.' Otherwise, it is considered as a 'zero.'

Command Interpretation

Once it’s determined whether a one or zero has been sent, the microprocessor must then interpret the data stream it is receiving. This entails being able to identify and sync up to the very beginning of the reader command (the section known as the
interpreting the command byte, comparing the mask bits with its own ID, and then setting the proper flags such that the correct response or action is taken. One possible way of implementing these tasks would have been to store the entire command sequence before doing any processing and interpretation. While this would have simplified the firmware considerably, the drawback would have been that by the time the command sequence had been interpreted, it would have been too late for the Field Probe to respond with its ID.

Instead, all the processing is done in the interrupt routine, as each bit is received. The one constraint is that the processing for any one bit cannot take longer the duration of the bit frame. For this particular microprocessor running at its maximum clock speed of 20 MHz, this means for a 14.25 μs bit frame there is enough time for about 70 instruction cycles (and 80 instruction cycles for a 16 μs bit frame). With this in mind, the interrupt routine was written entirely in assembly language and optimized such that each bit is processed within this limitation.

Furthermore, the ISR implements a FSM to keep track of what part of the reader command packet is currently being received. The state information consists of the current field (e.g. [CMD], or [PTR]), and the number of bits currently received in that field. Figure 4-2 illustrates the finite state machine.

In this FSM, a transition must occur whenever a bit is received. If from any state there is no condition which allows for a transition according to the diagram, this is interpreted as an error, and the ISR transitions back to the initial state, "Wait for reader command."

The FSM is pretty straightforward, and is derived entirely from the structure of the EPC C1G1 reader command. As each field is received, the parity is verified. In the case of the [VALUE] field, the information retrieved from [PTR] and [LEN] is used to determine over what bits in the Field Probe’s ID the bit mask in [VALUE] is to be compared to. If the bits do not match, i.e. the reader is not addressing an ID range that the Field Probe falls in, the field probe ignores the command.

On the other hand, if all the parity bits are verified, and the ID of the Field Probe is within the range specified by the mask, the ISR transitions into the "Respond to
Figure 4-2: Finite state machine for reader command processing
reader command" state, where it will take some action based on the type of command received from the reader. Once the action has been taken, the ISR transitions back to the initial state.

Field Probe Response

Once a reader command has been received, and if the Field Probe's ID is within the range of IDs being addressed by the reader, the field probe must carry out some action. This consists of one of two types of actions: a change of state in the Field Probe, or transmitting some kind of response.

The Talk and Quiet commands cause a change in state and require no response from the Field Probe. The Talk command puts the field probe into the active state and causes the Field Probe to actively respond to ScrollID and PingID commands which are addressed to it. The Quiet command puts the Field Probe into the quiet state and causes the Field Probe to not respond to any ScrollID and PingID commands, even if they are addressed to it.

The ScrollID command causes the Field Probe to respond with its entire ID. The Field Probe transmits its ID one bit at a time, using one period of a 125 KHz square wave to send a 'zero' bit, and two periods of a 250 KHz square wave to send a 'one' bit.

The response to the PingID command is slightly more complicated than that of the ScrollID command. The response is an 8 bit portion of the ID, sent during one of the 8 ping bins, as determined by the 3 most significant bits of the 8 bit reply. The 8 bit portion are the 8 bits that follow the last bit of the mask contained in the [VALUE] field.

4.3.2 Periphery Devices

All of the other periphery devices on the Field Probe were considered lower priority than the transmission and reception of data from the reader. As such, the control of these devices was handled mostly by a programming loop in the Main() routine of the
firmware, while the higher priority tasks of receiving and transmitting data was mostly handled through interrupts. The three primary devices that the microprocessor had to control were the LED, the beeper, and the field strength indicator.

LED

The LED is the primary means of instantaneous user feedback with regards to signal strength and signal quality. In some applications, the user may only be interested quickly checking the operation of a particular reader, or testing how far away from the reader antenna in a particular direction the field strength is high enough to turn on a tag. In these simple applications, the most effective way to communicate information was through an LED. The Field Probe could be programmed into several different display modes: LED bar field strength, single LED field strength, and single LED command received.

In the LED bar field strength mode, the several LEDs are used to provide a relative field strength reading. When all the LEDs are lit, the field strength is high, and as the field strength decreases, so do the number of lit LEDs, until they are all off. This mode, while the easiest way to convey field strength information, is also the most power consuming, since several LEDs are powered at the same time.

In the single LED field strength mode, a single blinking LED is used to convey field strength information. As the field strength increases, so does the frequency with which the LED blinks. While this mode is much less power consuming, it is more difficult to compare reading at different locations.

In the final mode, the LED blinks whenever a valid command is received. While this mode doesn’t provide information regarding the field strength, it does allow the user to verify that a reader is properly implementing the EPC Class 1 Generation 1 protocol, and that the reader signal quality is good enough to be received by the Field Probe.
Beeper

The beeper is meant as a secondary instantaneous feedback source to the LED, specifically for situations where the LED is not within the line of sight of the user, such as in the case where the Field Probe is embedded within a pallet. As the field strength increases, so does the pitch of the beeper. Unfortunately, the beeper used in this particular implementation was not particular loud, and would not have been audible in a warehouse environment. Louder beepers could be used, though likely at the expense of power consumption.

Field Strength Indicator

The field strength is measured off of the rectifier circuit by one of the microprocessor’s analog to digital converter (ADC) pins. To smooth out some of the noise caused by the 100% ASK modulation, the eight most recent field strength readings are averaged together. Also, the Field Probe schedules additional readings immediately following the successful reception of a reader command, because during these periods there won’t be any modulation present in the signal.

4.3.3 Data Formatting

The final task the Field Probe’s firmware has to do is to include the readings it takes into the data it transmits to the reader. Unfortunately the EPC Class 1 Generation 1 protocol does not provide the ability to open a communication channel between the reader and the tag where data can be sent freely back and forth, such as exists in the ISO14443 protocols at 13.56 MHz. The only way to actually transmit information using the built-in protocol command set was to encode the field strength readings directly into the Field Probe’s EPC ID.

The ID format used is shown in Figure 4-3. An arbitrary value (0xB8) was chosen for the first byte of the EPC ID to distinguish Field Probes from normal EPC tags. The next two bytes were used to encode a shortened Field Probe ID. The next three bytes are reserved, and could be used to send other sensor information. The last two
bytes contained the 10-bit precision voltage reading as measured by the microprocessors analog to digital sample unit. Using one of the unused built in timers, the field probe updates its ID with a new field strength reading every second.

4.4 Data Visualization Program

The last component in the Field Probe system is the program that interfaces with the UHF reader, aggregates the data from multiple Field Probes, and displays it in an some intuitive manner. The program was developed in Visual Basic because of the author's familiarity with this language; otherwise, there is nothing special about this choice of programming languages. Ideally, this program would be able to interface with any manufacturer's UHF reader. Unfortunately, there is not as of yet a standard reader interface, though such a standard is currently under development. For this particular implementation, the program was developed to interface only with the ThingMagic Mercury 4 reader, though interfaces to other readers can be easily added.

The visualization program is relatively straightforward in implementation. First the VB program establishes a telnet connection with the Mercury 4 reader. Then, using a special interface developed by ThingMagic called RQL (Reader Query Language), the VB program sends a query command every few hundred millisecond. This command causes the reader to report all tags it sees with a header byte equal to "0xB8", the header byte used to distinguish the Field Probe from typical EPC tags.

The GUI is set up to display a three-dimensional 3x3x6 grid. Each point on the grid represents. The dimensions are fixed in this implementation, but could easily be adjusted in a more versatile implementation. Below the image, the user enters in the Field Probe ID, and the xyz-coordinates

The VB program then parses this response, extracting the 2-byte Field Probe ID and the 10-bit field strength from each tag response. Using this information, the point in the grid corresponding to the location of the Field Probe ID is enlarged and given a color based on the field strength intensity. The color is updated with each
new packet from the Field Probe. Figure 4-4 shows a screenshot from the program.
Figure 4-3: Data format for Field Probe's EPC ID

| Header | Probe ID{1} | Probe ID{2} | RFU | RFU | Field{1} | Field{2} |

Figure 4-4: Data format for Field Probe's EPC ID
Chapter 5

Applications and Experimental Results

5.1 Introduction

As a general purpose RFID diagnostics platform, the Field Probe can and has been used in a number of different applications. Its primary application is as a diagnostics tool for RFID systems. A single Field Probe can be used to measure at one point in space the strength of the field produced by one or more reader antennas. Multiple Field Probes can be used to create an image or map of the field strength produced by one or more reader antennas within a volume of space. Ultimately, this information will help with the design and deployment of RFID supply tracking systems. While these types of applications have a number of commercial benefits in terms of RFID gateway and pallet design, they only represent a fraction of the Field Probe’s potential value. In several research projects conducted at the MIT Auto-ID Labs, experimental results were measured using the Field Probe. Since the primary focus of these experiments was to study various electromagnetic phenomena that can impact performance in RFID systems, the Field Probe was an apt choice of measuring tool due to its close resemblance to an actual RFID tag.

The following sections highlight several of the PackSIG research projects and demonstrations that utilized the Field Probe. First, Section 5.2 presents an exper-
iment that showcases the Field Probe’s ability to characterize the electromagnetic propagation in a tunnel-like space. Section 5.3 will present using multiple Field Probes for diagnostic applications. Finally, section 5.4 will summarize an experiment that explored the sinusoidal behavior of power transmission through layers of varying length.

5.2 Electromagnetic Characterization of Room

In this experiment, a ThingMagic Mecury 4 reader and antenna were setup in the center of a long corridor, pointing down a passage unobstructed for at least 100 feet. The corridor measured about 8 feet in width, and 11 feet in height. The walls and ceiling were made of concrete, and there were several metal door frames along the length of the corridor. The Field Probe was placed in center at the hallway in front of the reader antenna, and measurements were made in 4.5 inch increments away from the front of the antenna. The experimental setup is shown in Figure 5-1.

![Figure 5-1: Setup for electromagnetic characterization of corridor](image)

The measurements taken at each distance had to be averaged over a twenty second window. The reason is that due to FCC regulations, UHF RFID readers must implement frequency hopping, jumping between a minimum of 50 channels in the band 902-928 MHz, never staying on any one frequency for longer than 400 ms. Different frequencies over this band are received differently by the Field Probe, so it is necessary to either set the reader to produce only one frequency, or to average over
every frequency to obtain good results. Unfortunately, the reader used for this experiment does not allow for frequency hopping to be shut off, so the results had to be averaged. Since the ThingMagic Mecury 4 implements the minimum 50 channels and maximum 400 ms, that means that every frequency channel is visited once during a twenty second time period. Thus, field probe readings were recorded for exactly 20 seconds at each distance. The results are graphed in Figure 5-2.

![Graph of Voltage Induced on Field Probe](image)

**Figure 5-2: Results for electromagnetic characterization of corridor**

The first obvious feature of this graph is the fall off of power with distance. What is more interesting to note, however, is the small bump that occurs at about 32 inches away from the reader. At this location, there is some kind destructive interference that appears to be caused by the geometry of the room. The concrete in the walls acts reflects a great deal of the electromagnetic energy, turning the corridor into a rectangular waveguide, and it appears that this point corresponds to a quasi-null in the electromagnetic field.

This experiment provides a small taste of the kind of experiments that the Field Probe can be very useful for, helping to detect non-obvious null points in the electromagnetic field.
5.3 Diagnostics

One the biggest concerns companies trying to deploy RFID technology must face is the issue of readability. The whole point of case level inventory tracking is to know exactly where any case is at any given time. If only 3 out of 4 cases passing through a particular portal are read (or less), then it's practically impossible to tell whether a particular case has been stolen or misplaced, or merely was not read by the reader without some human intervention. But once someone has to go and scan each case individually, the benefit of automation that RFID provides is entirely lost.

The Field Probe can help in the design of both RFID gateways and pallets in order to maximize readability. The key assumption is that the majority of tag read failures are the result of not enough localized power being available in the area where the tag is located to power it up. This lack of power can be due to a number of factors, such as electromagnetic reflections at the boundaries between air and the cases, or multi-path interference caused by reflections from objects in the environment. The Field Probe provides field strength information that can be used to evaluate a particular RFID gateway and pallet setup. It illuminates where the 'hot' and 'cold' spots are in terms of power, providing feedback with regard to effectiveness of a particular setup. Using this information to carefully design pallets so that the electromagnetic properties of the products contained inside enhance rather than degrade the RFID performance, deeper electromagnetic propagation can be achieved. Additionally, reader antenna placement can be optimized to transmit power all around the pallet, and to minimize destructive interference.

For the final meeting of the 2004 PackSIG, a demonstration was designed to showcase the Field Probe as a diagnostic tool. Several Field Probes were scattered in a pallet of empty, but tagged boxes. A gateway frame was used to mount four reader antennas, two on each side of the pallet. Using the Visual Basic program described in 4.4, the data read by the Field Probes was shown as colored circles superimposed on a grid representing the pallet. It could be seen that as the pallet was pushed through the gateway, the colors changed appropriately as each Field Probe passed by each
This demonstration gives just a taste for the potential of the field probe as a diagnostic tool. Entire pallets full of Field Probes can be used to the field strength throughout an entire pallet. Improvements in future generation Field Probes could allow for more sensor measurements, as well as detecting what particular frequency the reader is using at any given time. This frequency measurement, though difficult to make, would be very useful for correlating the field strength readings since they are dependent on frequency. With additions to the Visual Basic program, field strength maps from different gateway/pallet configurations could be stored, analyzed, and compared to determine an optimal design for a given product. And perhaps most importantly, the interactive nature of the system allows users to see results immediately, helping to build intuitions to the complicated interactions that occur between electromagnetic waves and materials.

5.4 Sinusoidal Behavior of Power Transmission through Layers of Varying Thickness

Research conducted in conjunction with fellow graduate student Uttara Marti illustrated an important phenomenon related to electromagnetic wave reflections that occurs due to layered media [4]. Essentially, the amount of power that is transmitted through a layer of water is a decaying, periodic function of the depth of the water. Both the Field Probe, and an Alien UHF EPC tag were used to measure the results and demonstrate this phenomenon.

For the experiment, a ThingMagic Mecury 2 reader and a linearly polarized antenna with an 8 dBi gain were used to supply electromagnetic energy. With the antenna lying prone on the floor, a fish tank was propped 40 cm above it. The fish tank was used to hold varying depths of water. Suspended 100 cm above the reader antenna was the measuring device (either the Field Probe or the UHF tag). The setup is shown in Figure 5-3.
The thickness of the layer of water in the fish tank was varied from 0 to 37 cm, in 1 cm increments. At each water depth, measurements were made with the reader set to three different transmit frequencies representing the low, mid, and high values within the range of frequencies a typical North American UHF reader sweeps through: 903 MHz, 915 MHz, and 927 MHz. Measurements were done with both the Field Probe (using a relative field strength reading), and the UHF tag (using the number of reads per minute as an indicator of field strength).

The results from this experiment are shown in Figure 5-4. As can be seen from the two graphs, the transmission of power through the water has a clear periodic dependency on the thickness of the water. This correlates well with theory, because the layer of water can be treated as two boundaries; one between the water and air below the tank (boundary 1), and one between the water and air above the tank (boundary 2). The electromagnetic waves that propagate through the water are a combination of the waves that were transmitted without any reflection, plus the waves that reflected from boundary 2, and then reflected back from boundary 1, and the infinite sequence of reflections between boundaries 1 and 2 that eventually transmit...
Figure 5-4: Data results from fish tank experiment. The plot shows the induced voltage on the field as a function of the depth of the water in the fish tank.

Through boundary 2. If the depth of water is not a multiple of half of the wavelength of the transmit frequency, this infinite combination will add in a destructive manner, because the phases will not align. If the depth is a multiple, then the reflections that transmit through will be mostly in phase, and add constructively.

The exponential decay that can be seen in the Figure 5-4 is a result of the power absorption of water. However, it’s clear that this rate of decay is much slower as compared to the degradation caused by a water depth corresponding to one of the troughs in the graph. The overall result that can be taken from this experiment is that the thickness of packaging materials, and to what extent they can be controlled, the thickness of the materials in the products, should be designed such that maximize the transmission of electromagnetic energy.

The comparison of the two graphs also reveals how much more useful the Field Probe is as a measuring device than is the read rate of a UHF tag. The Field Probe allows for more far more resolution than the read rate of a tag. A similar, perhaps more precise, graph could have been generated with a spectrum analyzer, but the field probe has the obvious advantage of being far cheaper.
Chapter 6

Conclusions and Future Work

6.1 Conclusions

The Field Probe has proven to be a useful measurement device for fundamental RFID research, as well as a useful diagnostic tool for RFID system evaluation. Unlike current available commercial systems, the Field Probe can provide data from deep within a pallet; it does not require line of sight to be useful. Furthermore, it goes a step further than other systems by actually providing data with more resolution than is possible with a simple LED bar, and organizing this data over several Field Probes in order to build three dimensional maps of the field strength.

Over the course of this research, three main conclusions were drawn.

First, for RFID diagnostics to be performed well, there is a need for the development of intuition with regards to the electromagnetic field, and its interaction with materials. Perhaps a good metaphor is that a though a mechanic may not have a formal training in mechanical engineering, a good mechanic will develop over years of experience a deeper intuition that allows them to efficiently diagnose problems that arise with a car and fix them. Electromagnetism is a complicated and involved subject that can require years to gain understanding. However, certain principles derived from fundamental electromagnetic equations, can not only be appreciated by a more general audience, but can be of great use in diagnosing problems in RFID systems. Some of the principles may seem non-intuitive at first, as in the case of the fish tank.
experiment which demonstrated that power transmission through a layer of material is partly a periodic function of the thickness of that layer. More fundamental electromagnetic research that is geared directly toward RFID is needed, and that research needs to be accessible to all people involved with the development, integration, and maintaining of RFID systems.

Second, the Field Probe has proven itself to be a useful measurement and diagnostics tool. In its current version, it does have some fundamental limitations such as only a 2 m read range. In spite of that, it has been able to provide good, consistent experimental results that provide useful information such as the location of null points in a particular setup. These results help to build up the intuition discussed above.

Finally, the Field Probe in it of itself is not a complete solution to RFID diagnostics, or the development of RFID intuition. In conjunction with fundamental research such as was conducted by Packaging SIG researcher Uttara Marti, and graphical simulation software developed by Packaging SIG researcher Jonathan Wolk, the Field Probe plays an important role in verifying results obtained from these other projects. The goal of the Packaging SIG was to provide companies with a set of RFID diagnostic tools, and the Field Probe has proven itself a very useful component in that set of tools.

6.2 Future Work

As an RFID diagnostic tool, the Field Probe along with the software I’ve developed is a complete and functional system, though some parameters such as read range need improvement. As a tool for fundamental RFID research, further development is still necessary to realize the full potential of the Field Probe. In this section I’ll present some of the Field Probe’s limitations with some suggestions for how to improve these limitations, as well as discuss some features that can and should be added to make the Field Probe a more powerful research tool.
6.2.1 Read Range Improvement

Perhaps the most important improvement needed for the Field Probe is increasing its read range. With a maximum range of approximately 2 meters, the Field Probe as a semi-passive tag has worse performance than an average passive tag. There are several solutions to this. One is to develop some better techniques for doing impedance matching between the antenna and the Field Probe’s circuitry. Another approach that may improve the read range is using a commercial RF detector chip to demodulate the signal. These chips have a number of voltage doublers and transistor gain stages that would be impractical to implement with discrete components on a PCB. Thus, even with less than perfect impedance matching, the greater sensitivity may allow for longer read ranges.

6.2.2 EPC Class 1 Generation 2

In December of 2004, EPCGlobal ratified a new protocol standard, EPC Class 1 Generation 2. This protocol has a number of significant improvements over EPC Class 1 Generation 1, and is expected to dominate the RFID supply chain market within the next year or two as tag production increases. Some of these improvements include faster tag write and read speeds, added security including a longer password, improved air interfaces that are less sensitive to noise, and a more flexible command set for improved anti-collision algorithms. In order to accommodate this new protocol, the field probe needs more than a firmware upgrade. The air interface, which allows for a number of different modulation schemes, requires entirely new circuitry.

6.2.3 Sensors

Finally, the Field Probe could become a more powerful research tool by adding sensors besides the field strength detector. Further research is needed to explore the effects that environmental conditions such as humidity and temperature may have on RFID performance. The Field Probe is the perfect instrument for such research, using the protocol as a means to communicate any kind of environmental information the
researcher is interested in exploring.
Bibliography


