An Open Architecture Radio Frequency System for Electromagnetic Tag Detection

by

Olufemi Abidemi Omojola

Submitted to the Department of Electrical Engineering and Computer Science
in partial fulfillment of the requirements for the degree of

Master of Engineering in Electrical Engineering and Computer Science

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

February 2001

Author .....
Department of Electrical Engineering and Computer Science
February 05, 2001

Certified by .....
Neil A. Gershenfeld
Professor of Media Arts and Sciences
Thesis Supervisor

Accepted by .....
Arthur C. Smith
Chairman, Department Committee on Graduate Students,
Department of Electrical Engineering and Computer Science

An Open Architecture Radio Frequency System for Electromagnetic Tag Detection

by

Olufemi Abidemi Omojola

Submitted to the Department of Electrical Engineering and Computer Science
on February 05, 2001, in partial fulfillment of the
requirements for the degree of
Master of Engineering in Electrical Engineering and Computer Science

Abstract

In this thesis, I describe the design and implementation of a radio frequency identification device (RFID) controller system that is capable of interacting with both silicon-based RFID devices and physical structures that require different frequencies and modulation schemes. The system is capable of interrogating not only traditional RFID devices made of silicon using VLSI processes but also structures that use interesting material properties to encode information about identity and environmental state at much lower cost. I first present the issues motivating the design, the 4 target RFID devices this thesis addresses and the bounds these devices place on the system. I then describe in detail the component level implementation of the system and a byte-level communication and control protocol for the prototype open architecture RFID controller system. Finally, I discuss further research required to make the system manufacturable.

Thesis Supervisor: Neil A. Gershenfeld
Title: Professor of Media Arts and Sciences

Acknowledgments

This thesis would not be possible without the help and support of many people. My heartfelt thanks go to Neil Gershenfeld for providing a place in the Media Laboratory within which this work was possible. Thanks to Jim Kirtley, my academic advisor, for providing the appropriate viewpoints at the appropriate times. Thanks to Rich Fletcher, Matt Reynolds, and Yael Maguire for providing truly invaluable knowledge that I probably would never have found on my own without a lot of ineffectual flailing about. My thanks to the Physics and Media community, the three mentioned above as well as all the other stalwart souls who suffered my presence for so long: Bernd Schoner, Matt Hancher, Ravikanth Pappu, Ben Vigoda, Peter Russo, Rehmi Post, John Paul Strachan, Kelly Dobson, Jason Taylor, Aram Harrow, John DiFrancesco and Esa Mahmood, and the alums, Josh Smith, Ed Boyden and Joey Richards. Thanks to Susan Bottari for truly making sense out of nonsense: NOTHING would have been possible without her. Much love to my parents and family for bearing with me for so long: I told you I'd finish one day. My people at school; to the graduated: I'm with you now; to the suffering souls still locked down: I'm with you forever, we will all get to the sunshine one day, I'm just getting there a little ahead of you. Thanks to the Things That Think Consortium, the Media Laboratory and all the sponsors: none of this would be real without you.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

RFID (Radio Frequency Identification Device) in its conventional use refers to a group of technologies in which a device (usually a VLSI chip connected to an appropriate antenna structure, powered either by energy remotely coupled into the device via an electromagnetic (EM) field or using a battery) is attached to another object or structure. The general class of problems these are traditionally used for fall into what is called Automatic Identification (Auto ID), in which the presence and/or position of the RFID device (commonly called a tag or transponder) is detected, and by extension the object or structure the device is attached to is identified without manual intervention. The detection is typically done using an EM field created by sending a radio frequency (RF) excitation signal at a specific frequency into a coil or patch antenna as an interrogation signal and detecting the response of the transponder: it either applies a modulation to the original signal or transmits its response at another frequency. Resolving the identity of the transponder is done by interpreting information encoded into the response of the transponder using some protocol. Extensions of this scheme involve attaching a sensor of some kind to the RFID IC to provide information about environmental factors in the local area of the tag.

With variations on the power supply and antenna geometry of the detector creating the EM field and the design of the chip-antenna pair used in the transponder these systems can work over areas ranging from a few inches to a few hundreds of meters (the transmit-respond principle is used in many applications, an example being

aircraft transponders, but such applications are not of interest here).

Applications of auto ID procedures range from access control for buildings (in the form of RFID badges) to electronic article surveillance (anti-theft tags) to mobile contactless identification (such as drive-through toll systems).

1.1 RFID Device Costs

Many RFID devices are conventional microprocessors with extra circuitry added to provide for things like power harvesting and RF modulation. These are typically manufactured using mature silicon VLSI processes and have order of magnitude chip costs of around 10 cents. These can be configured to work in a wide number of ways. The major differences between tags are:

- The frequency of operation of the tag.
- The type of channel the tag uses to communicate with the detector: a near-field magnetic field created by the detector using a coil antenna, a near-field electrostatic field created using a patch antenna, a far-field RF modulation of the detector's RF signal, or a far-field RF signal generated by the tag using its own power source (such as a battery).
- Power source: the tag may be active (self-powered using a battery or power-supply derived from the object it is attached to), or passive (powered inductively or electrostatically from the electromagnetic or electrostatic field generated by the detector).
- Channel sharing capability: the capability for multiple tags to be within communication range of the same detector and still be successfully distinguished (anticollision).
- Orientation dependence: whether or not the detection of the tag is affected by the relative orientation of the tag antenna with respect to the detector's

antenna. Tags that use an electrostatic or far-field RF channel are typically orientation independent.

For most tags an external antenna is needed and the parts and labor costs to make this antenna and attach it to the chip increase significantly the price of the tag. While what is referred to as a significant price increase may result in a tag cost of less than $1, for many applications of interest this price point is too high. As an example, many ticketing applications currently use cards that store information in a magnetic stripe and require the user to swipe the card through an appropriate card reader at toll points. Contactless versions of these cards would result in a vast improvement in efficiency (by reducing the need for users to spend time getting the cards out and swiping them through the readers). However, since these tickets must be disposable, a cost of 20 cents places the tag solution out of reach of this application. Table 1.1 shows examples of different RFID devices and their properties.

1.2 Beyond Silicon - Materials and Structures

Gordon Moore, the founder of Intel Corporation, made a number of predictions about the rates of advances in the semiconductor industry (known as Moore's Laws). Of interest here is Moore's Second Law, which states that the cost of the fabrication plant to build semiconductor microprocessors will double every two years until they are fiscally infeasible to build [2]. With applications driven by sub-cent cost requirements (such as packaging products), no product of any manufacturing process that obeys such a law can be applied. As a result, for applications with properties similar to those of the ticketing application described in Section 1.1, silicon scaling limits will never allow the use of conventional silicon VLSI-based RFID devices. The question then becomes: what type of manufacturing process can be used to produce what type of tag that will satisfy these cost requirements?

To satisfy such cost requirements, bulk manufacturing processes need to be used. Such processes are typically unable to produce devices or structures with design complexity approaching that of any VLSI process, and can only produce simple material

Name	Frequency	Channel	Power Source	Modulation	Anticollision
Motorola BiStatix	125kHz	Electrostatic	Passive	AM	No
Philips I-Code	13.56MHz	Inductive	Passive	AM	Yes
Microchip MCRF250	125kHz	Inductive	Passive	AM,FM or PM	Yes
Intermec 500 Series	900MHz or 2.45GHz	Far-field RF	Passive or Active	AM	Yes
Philips Hitag 1	125kHz	Inductive	Passive	AM	Yes
Temic e5550	125kHz	Inductive	Passive	AM	Yes
TI Tag-IT	13.56MHz	Inductive	Passive	FM	No

Table 1.1: Sample RFID devices

structures.

The key concept, however, is design complexity. A VLSI-based RFID device may contain a few thousand transistors laid out in specific patterns that handle RF communications and implement microprocessing and memory: these are ultimately used to encode information that can be retrieved on demand by the detector. The goal is to achieve similar functionality without the need for the transistor architecture. But what is this desired functionality, and how can it be achieved?

1.2.1 Identity

The primary desire for most RFID applications is identity: to discriminate between multiple objects. Traditional silicon RFID devices do this by implementing some

arbitrary-sized segment of memory that stores a specific, often unique, bitstring: when queried for its identity, the device will return this string to the detector. Applications that require identity typically connect to some back-end storage system, such as a database server, that stores information associated with a particular identity. Alternatively, all the relevant information may be stored in the tag's memory.

Modifications to the information associated with a specific tag can be done by either modifying the data stored on the tag or modifying the record stored in the back-end. The ability to write data to the tag comes at an increased cost over a read-only device, but offers better performance in the absence of a reliable connection to the back-end. The back-end record modification is cheaper on a per-device basis, but requires a more reliable connection to the back-end.

From the materials and structures perspective, without the flexibility of digital memory the ability to write data to the tag is limited. As such, the approach is to encode identity with a distinct signature that is a function of either the material the tag is made of and/or the tag's structure. The term signature refers to the tag's response to the presence of an electromagnetic field at a specific frequency, detected in a particular fashion. An example would be to distinguish between resonant structures using their resonant frequencies: the measurement taken could be the standing wave ratio (SWR) at an antenna placed beneath the tag. This and a number of other approaches are discussed in Chapter 3.

1.2.2 State from Material Properties

As mentioned in the beginning of the chapter on page 10, of increasing interest is the idea of not only extracting identity information from the tag, but also information about the current and past state of the tag's environment. As an example, a tag could be integrated into the packaging for a fragile object that would store an indication of the maximum weight borne by the package during shipping, as a means of checking whether damage to the package occured from faulty packing before shipping or excessive loading of the package during shipping.

The approach to this using conventional silicon RFID devices is to provide a data

channel into the chip that an attached sensor can use to transmit digital information to the device: when queried by a detector the device returns the data from the sensor embedded in a particular place in the bitstring it sends back to the detector. Once again this functionality comes at a greatly increased cost and complexity of the device.

However, using materials and structures this can be accomplished in a much simpler fashion. By building structures with signatures that vary in different ways based on a particular environmental property (such as temperature or humidity) [3],[4], simple, cheap, non-contact sensors can be built that allow interesting measurements to be made.

1.3 Open Architecture Radio Frequency Systems

Materials and simple structures have a number of restrictions on their use. Applications that desire capabilities such as storage of arbitrary digital data, easy reprogramming or long-range self-powered operation generally have to use conventional silicon devices to provide the desired capability and reliability. In general, depending on the application and operating environment a wide range of variables including operating frequency and tag antenna geometry influence the optimal choice of tag to use.

Standardization can drive the adoption of technology by lowering the costs of manufacturing, but in the tagging regime this would result in poor performance in most application domains.

To mitigate against this, we propose the concept of an Open Architecture Radio Frequency system: in Section 1 we described the basic principle behind all RF tags; an open architecture tag reader is a system that implements that principle over a number of frequencies, allowing a single system to detect and interrogate multiple types of tags.

1.3.1 Requirements

Tag readers today are largely analog circuits: these are cheap and simple to design and control. In Section 1.2, we quoted Moore's Second Law as a reason why VLSI-

based devices will never be able to reach a price-point that allows for widespread adoption of tagging technology. However, Moore's First Law states that there will (roughly) be a doubling in the amount of processing power available within the same chip area every 18 months. This trend has resulted in the increased popularity in the last few years of digital signal processing and software radio techniques in systems that were predominantly analog.

To build an open architecture RF system, a number of things are of importance:

- The ability to generate (and possibly modulate) a stable RF excitation signal at a number of different frequencies.
- The ability to detect and separate the response of tags at a number of different frequencies.
- The ability to detect (and demodulate) multiple modulation schemes (possibly at the same frequency).

These could be done with multiple analog circuits for each such frequency and/or modulation scheme, but such a system is inherently limited in its ability to deal with new tags and modulation schemes. However, this is an area optimally suited to software radio design.

Although the cost of tag readers is not as significant a barrier as the cost of the tags, until recently the use of significant amounts of digital logic in tag readers has been restricted by the cost of the devices. With the advent of low cost reprogrammable devices such as field-programmable gate arrays (FPGAs) and complex programmable logic devices (CPLDs) these barriers no longer exist. In concert with recent advances in direct digital synthesis (DDS) technologies and low-cost, high speed analog-to-digital converter (ADC) chips, all the pieces necessary to develop low-cost software radio tag readers are now present.

1.4 Outline of this Thesis

This thesis describes an implementation of an open architecture tag reader controller. Chapter two describes the electromagnetic principles that govern the interactions between the detector and the tag and outlines the physical structures and communications channels used to transmit information both from the tag to the detector and vice versa for a range of tags. Chapter three describes the target devices that the prototype tag reader will be addressing, covering the basic operating principles of these tags in greater detail and the rationale used to make these choices. Chapter four discusses the tag reader design considerations, describing in greater detail the effect of the choice of tags on the physical and electronic structures that comprise the reader. Chapter five describes the specific implementation of the prototype tag reader. It discusses a precursor to this system, details the "hardware" radio subsystems, their interconnections and the detection strategies employed for each tag. Chapter six describes the communication protocol written to control the tag reader. Chapter seven discusses the implementation results and the functional requirements beyond this implementation for a practical tag reader. The summary at the end discusses future work in the domain of open architecture radio frequency systems.

Chapter 2

Physical Principles

Fundamentally, RFID systems are differentiated by the channel between the detector and the tag (also called a transponder). Most RFID systems operate using the principle of inductive coupling, and this chapter places emphasis on this mode of operation (all the tags covered in this thesis use this channel). A later section gives a brief discussion of far-field electromagnetic propagation; the treatment of capacitive coupling is analogous to that of inductive coupling, but with a time-varying electric field rather than a time-varying magnetic field and induced voltage in a dipole rather than induced current in a loop.

The channel can be used for power transfer (for passive tags) and/or data transfer[1]. In all the tags covered in this thesis a single channel is used.

2.1 Inductive Coupling

2.1.1 Magnetic Fields in Conductors

Moving charge in a wire (a flow of electric current) induces a magnetic field. The magnitude of the magnetic field is described by the magnetic field strength H, regardless of the material properties of the surrounding space.

[1]Some systems use separate or multiple channels for both, such as the TI transponder used for the Mobil Speedpass applicaton, which uses a 134 kHz channel to power and interrogate the tag and a 900 MHz channel for the tag's response.

The contour integral of the magnetic field strength along a closed curve is equal to the sum of the currents within the curve,

$$\sum I = \oint \vec{H} \cdot \vec{ds} \tag{2.1}$$

From this, the field strength H at any point in the vicinity of an antenna can be determined. Inductively coupled systems exploit this magnetic field for power and communication.

For a circular loop antenna, the field strength along the x-axis of the loop can be calculated by

$$H = \frac{I \cdot N \cdot R^2}{2\sqrt{(R^2 + x^2)^3}} \tag{2.2}$$

where N is the number of windings, R is the radius of the loop, x is the distance from the center of the loop and I is the current in the loop. This equation holds when the vertical thickness of the loop is much less than the loop radius and the distance from the loop's center is less than $\lambda/2\pi$. This distance is the region around the antenna that is considered the *near field*, in which changes in the primary magnetic field around an antenna can induce changes in the current flowing through the antenna as a result of tight coupling between the varying magnetic and electric fields and the antenna. Passive tags that use inductive coupling operate in this region. From this equation it can be determined that for a distance x from the center of the loop, the magnetic field strength is highest when $R \approx x$.

For rectangular loops, this equation takes the form

$$H = \frac{N \cdot I \cdot ab}{4\pi\sqrt{(a/2)^2 + (b/2)^2 + x^2}} \cdot \left(\frac{1}{(a/2)^2 + x^2} + \frac{1}{(b/2)^2 + x^2}\right) \tag{2.3}$$

where a and b are the lengths of the loop edges.

2.1.2 Magnetic Flux and Flux Density

For a given field passing through space, a vector field B is defined in terms of the force produced on a small current element of length dl carrying current I such that

$$df = IdlBsin\theta \tag{2.4}$$

where θ is the angle between dl and B[5]. B is known as the *magnetic flux density*, and its association with the magnetic field strength is expressed as

$$B = \mu_0 \mu_r H = \mu H \tag{2.5}$$

μ_0 is a constant associated with the *permeability* (or magnetic conductivity) of a vacuum. μ_r is a constant factor called *relative permeability* and indicates the relative increase or decrease in permeability (with respect to that of a vacuum) of the material through with the magnetic field is propagating. For a certain planar area A in space, the magnetic flux through that area is expressed as

$$\Phi = B \cdot A \tag{2.6}$$

2.1.3 Inductance

Given a loop of area A_1 with N turns through which the same current flows, each of the turns will contribute the same proportion of flux Φ to the area of the loop, where the total flux Ψ is expressed as

$$\Psi = \sum_N \Phi_N = N \cdot \Phi = N \cdot \mu \cdot H \cdot A_1 \tag{2.7}$$

The *inductance* of a loop is the ratio between Ψ and the current I flowing through the loop,

$$L = \frac{\Psi}{I} = \frac{N \cdot \mu \cdot H \cdot A_1}{I} \tag{2.8}$$

If a second loop with area A_2 is placed near a loop with a current I_1 and area A_1, a portion of the magnetic flux Φ will flow through A_2. This *coupling flux* connects both loops together, with a magnitude dependent on the relative sizes and positions of the loops and the permeability of the medium the flux is propagating through. The

mutual inductance of the second loop, M_{21} in relation to the first loop M_{12} can be defined as

$$M_{21} = \frac{\Psi_{21}(I_1)}{I_1} = \oint_{A_2} \frac{B_2(I_1)}{I_1} \cdot dA_2 \tag{2.9}$$

This coupling generates a current I_2 through the second coil, and the mutual inductance property is commutative, i.e.

$$M = M_{21} = M_{12} \tag{2.10}$$

2.1.4 Power Supply

This coupling is exploited by RFID systems. An RF excitation current in the antenna loop generates an alternating magnetic field. To generate power within passive (batteryless) RFID devices, the transponder antenna couples to the transmitter antenna, with an induced current of I_2. This current runs through a load resistor (the internal resistance of the transponder device), generating a voltage $u2$. To improve the efficiency of the power harvesting circuitry, a capacitor C_2 is typically added in parallel with the transponder loop to form a parallel resonant circuit with a resonant frequency equal to the RFID system's operating frequency. Figure 2-1 shows an equivalent circuit diagram of a transponder and transmitter: the capacitor C_p represent parasitic elements in the real circuit.

In practice, the transponder uses a low-loss bridge rectifier to convert the AC voltage $u2$ into a DC voltage. From Equation 2.2, it can be generally assumed that the read range of a specific antenna roughly corresponds to its radius. The specific range of an antenna will depend on the sensitivity of the electronics that detect and interpret the data: an antenna may be able to power a transponder at a certain distance, but unable to detect and demodulate the transponder's response.

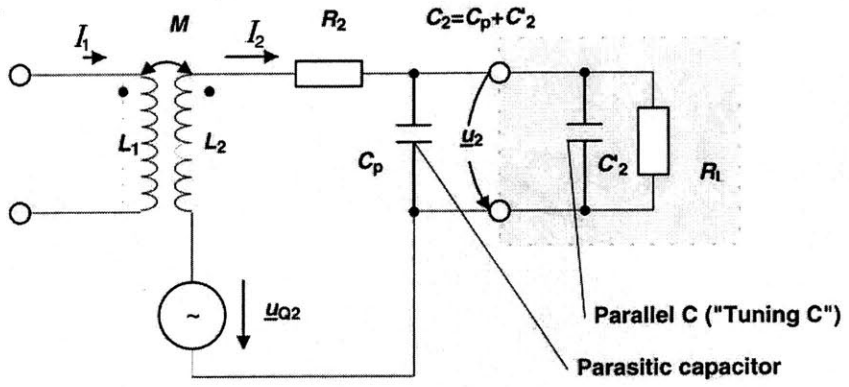


Figure 2-1: Equivalent circuit diagram for magnetic coupling between transmitter and transponder.

2.1.5 Data Communication

Most tags that operate in this regime use amplitude modulation schemes to transmit data between the controller and the transponder. In the direction from the controller to the transponder, this often takes the form of amplitude modulation of the RF excitation signal into the loop antenna. The specific coding algorithms are RFID device specific; an example can be found in [6].

In the direction from the transponder to the antenna, *load modulation* is most often used to transmit the data. As noted in Section 2.1.1, in the near field region changes in the magnetic field around a loop are reflected as changes in the current flowing through the loop. The introduction of the transponder antenna into the transmitter's near field region results in a detectable change in the amplitude of the current flowing through the loop. The relationship between this change and the transponder's antenna can be modeled as an *impedance*; this impedance is dependent on a number of factors, including the inductance of the transponder antenna, the value of the parallel capacitance used to set the resonant frequency for the transponder's antenna, and the load resistance of the transponder. The inductance of the transponder

antenna is typically fixed, but by varying the load resistance (ohmic or resistive load modulation) or parallel capacitance (capacitive load modulation) this impedance can be changed. Data transfer is then done by using the data within the transponder to control the rate of this variation (using a simple state machine or microcontroller controlling a switch). An appropriate encoding scheme can be chosen to represent different binary values in the data stream: Sections 3.2 and 3.3 show examples of different modulation schemes.

2.1.6 Physical Structures

For physical structures that do not implement modulation schemes (such as tags for EAS applications), the change in the magnetic field around the transmitter antenna is instead a constant difference, rather than a time-varying change, and can still be detected by measuring the change in the characteristics of the current flowing through the transmitter antenna. Bridge imbalance detection schemes can be used here, and examples of such schemes are discussed in Sections 3.4 and 3.5.

2.2 Far-field Electromagnetic Propagation

In Section 2.1.1, the near field was mentioned as the region in which changes in the magnetic field around a loop antenna induced changes in the current flowing through the conductor. This region extends out to an area roughly $\lambda/2\pi$ in radius around the antenna. Beyond this distance, the magnetic and electric fields separate from the antenna and propagate into space as an electromagnetic field, with the field strength falling off at a rate inversely proportional to the square of the distance from the antenna. In this form, the electromagnetic field is termed the *far field* and can no longer have a direct effect (by inductive or capacitive coupling) on the antenna that generated it. This represents a hard limit on the range of an inductive or capacitive coupling system.

In the far field, the electromagnetic wave propagation occurs at $3 \times 10^8 m/s$, the speed of light. At high frequencies, where the far field starts very close to the antenna

(as a result of the small wavelength) and the field strengths are high, the propagation range is better than for low frequencies. As such this channel is often used for systems that operate at frequencies above 30 MHz, and is incapable of transmitting sufficient power to power a microcontroller or state machine.

RFID systems that operate in this region use the transmitted energy as either a wake-up signal to the tag (for active tags) which then respond using their own power, or using some modulation of the signal reflected back to the transmitter (usually known as *backscatter* systems, or *modulated radar cross-sections*).

For tags that use modulation of the reflection of the transmitted energy, if the propagation of the transmitter is considered to be uniform in all directions, the *power density* at the location of the transponder is

$$S = \frac{P \cdot G}{4\pi R_2} \tag{2.11}$$

where P is the transmission power of the reader, G is the gain of the transmitter antenna (which measures the directionality of the antenna[7]), and R is the distance from the reader to the transponder. The reflected power is proportional to the power density, and the constant of proportionality is known as the *radar cross section*, σ which is a measure of an object's ability to reflect electromagnetic waves. This is a function of a number of parameters, including the wavelength and polarization of the transmitted signal, as well as the size and shape of the object. The modulation is done by changing σ: this can be done with diodes or switched resistors.

The power density at the transmitter antenna of the reflected signal is

$$S_{back} = \frac{P \cdot G \cdot \sigma}{(4\pi)_2 \cdot R^4} \tag{2.12}$$

and so the reception power is given by the receive antenna's effective area,

$$P_{back} = \frac{P \cdot G \cdot \sigma \cdot A_W}{(4\pi)^2 R^4} = \frac{P \cdot G_2 \cdot \lambda_2 \cdot \sigma}{(4\pi)^3 R^4} \tag{2.13}$$

where $A_W = \lambda \times \frac{G}{4\pi}$. This is the *radar equation* and it shows that the read range of a system using such a reflection system is proportional to the 4th root of the reader's

transmission power. These systems typically employ tag antennas with dimensions comparable to the wavelength of the excitation, which is small in the UHF bands (900 MHz, 2.4 GHz).

Chapter 3

Target Devices

3.1 Regulatory Issues

Operation of radio equipment is regulated based on the equipment's frequency of operation, and RFID systems are no different. Slices of the spectrum are usually allocated based on demand for an application, and since RFID only emerged as a significant user of radio frequencies in recent years there are few frequency bands assigned to RFID implementations. There are a number of frequencies assigned specifically to EAS applications, but the silicon-based RFID ICs invariably operate in the unlicensed ISM (industrial, scientific and medical) frequency bands, such as 13.56 MHz or 2.45 GHz.

In addition, frequency allocations are traditionally managed by individual countries, making it difficult to operate the same equipment in multiple countries; there have however been recent moves to harmonize the allocations of the RF spectrum within certain global regions, such as Europe and Northern America. In the United States of America, RFID systems are covered by the Federal Communications Commission's (FCC) Part 15 licensing requirements[8], which governs all devices that emit low-power radiation, whether intentional or not. Any commercial implementation of this system would have to meet these requirements, but given the research environment in which this development is being done, as long as the system does not interfere with the operation of any licensed users of the spectrum, these concerns may

be temporarily ignored.

However, the development efforts for the proof-of-concept open architecture reader must be informed by these licensing requirements (which typically limit the strength of the electric or magnetic field generated by a radio system at a certain distance away from the transmitter), as well as the currently available RFID implementations. It should demonstrate the ability to read both current, industry standard tags (backward compatibility) as well as new, materials-based tags (flexibility).

Current commercial implementations which operate at frequencies above 1 MHz are licensed to use frequency bands at 1.95 MHz, 3.25 MHz, 4.75 MHz, and 8.2 MHz for EAS applications, while silicon RFID systems largely operate in frequency ranges around 13.56 MHz, which is an ISM band.

Below 1 MHz, the frequency range from 9 kHz to 135 kHz is not reserved as an ISM band but is heavily used for RFID (and many other radio services) as a result of the long wavelengths, higher permissible field strengths and low technical cost of radio frequency generation.Most silicon RFID implementations in this range operate between 125 kHz and 135 kHz. In addition, EAS implementations below 70 kHz are common.

For all these reasons, the following 4 tag types were selected:

- An inductive RFID tag that operates at 125 kHz.
- An inductive RFID tag that operates at 13.56 MHz.
- A mechanical magnetic resonator that operates at 58.5 kHz.
- A planar, distributed inductance and capacitance tag that operates at 8 MHz.

Each of these tags is discussed in further detail below.

3.2 125 kHz Inductive

The 125 kHz frequency is an industry standard for near-field magnetically or electrostatically powered tags. Tags such as these are used in most common access control

systems. The focus of this thesis is on inductive coupling tags, but capacitively coupled devices would only require a different front-end to provide the required electric field to power the tag. Figure 3-1 shows examples of both inductive and electrostatic tags that operate at this frequency.

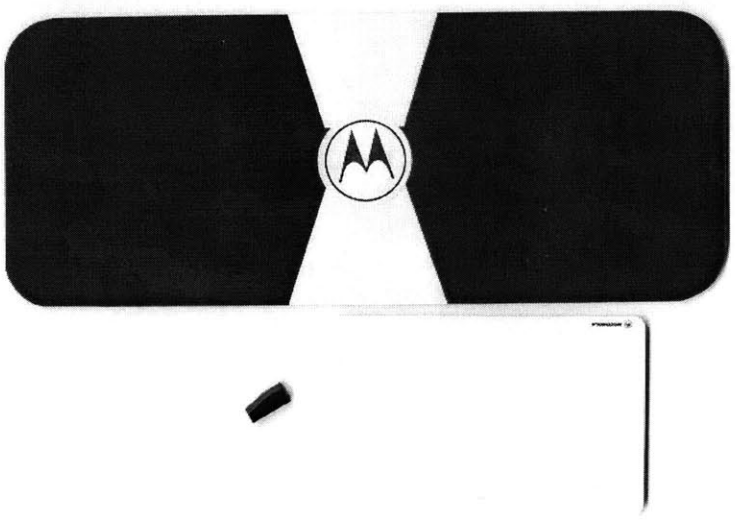


Figure 3-1: Examples of 125 kHz tags. The dipole antenna is typical of capacitive coupling tags, the white rectangle is a common form factor for 125 kHz inductive tags, and the black chip is an example of a 125 kHz RFID IC.

These tags are typically built using a low-speed microcontroller core connected to RF power harvesting circuitry and powered as described in Chapter 2. The microcontroller core within the tag derives its clock from the excitation signal as well.

The tags use a form of non-volatile memory (usually EEPROM) to store an identifying bitstring. This bitstring is sent to the detector using one of a number of modulation schemes, most often amplitude modulation (implementations of these have the lowest cost). Some tags use FM (using Frequency Shift Keying) but these are rarer: the circuitry is much more complex as the tag only has one low clock frequency available to it. To improve robustness of the transmission and reduce RF emissions levels some devices use a second modulation layer on top of the base AM modulation.

The tag used in this thesis is a 125 kHz inductive tag designed by the Motorola Indala Corporation, and it implements a 2-layer modulation scheme in which the primary modulation is an AM signal with a sub-carrier of 62.5 kHz. It uses resistive load modulation, with a typical modulation index at the transmitter of 1 or 2 percent. A secondary modulation (using BiPhase Shift Keying at 7.8125 kHz) is then used to transmit the data, resulting in a data rate of roughly 7.8125 kbps. The subcarrier appears as a change in the amplitude of the carrier signal at the transmitter antenna every other cycle, as can be seen in Figure 3-2. Each data frame is 32 cycles long, with a phase shift of π in the subcarrier amplitude at the end of each frame. This phase shift is visible as 2 consecutive cycles with identical amplitudes. When a '0' is transmitted, the frame is unchanged. When a '1' is transmitted, an additional phase shift of π in the subcarrier amplitude is inserted at the 16th cycle.

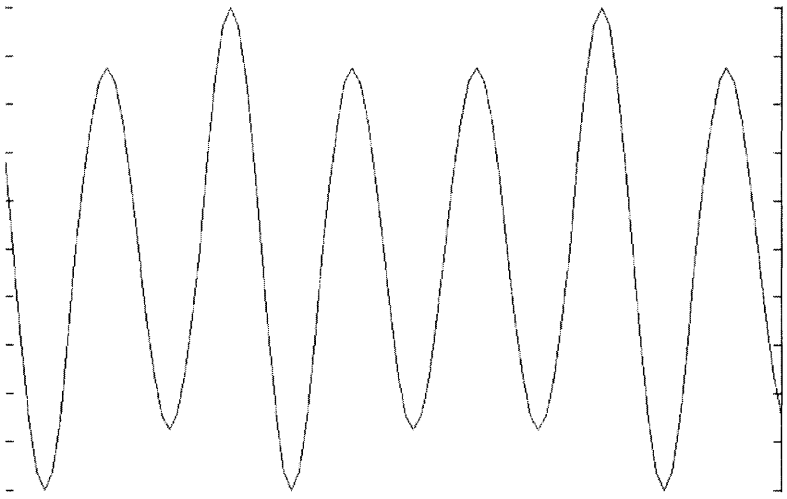


Figure 3-2: BPSK data transmission details. A phase shift of π in the subcarrier amplitude is inserted every 32 cycles to indicate the end of a data frame and at the 16th cycle in a frame to indicate the presence of a '1' bit.

When introduced into the field of the detector, these tags power up and immediately start transmission. The first bytes are synchronization bytes designed to let the detector recognize the polarity of the tag's transmission. After that the tag transmits the bitstring, which for the tags used in this project is 1024 bits long. The tag repeats

the transmission indefinitely, with a small pause between each transmission, for as long as the tag remains within the magnetic field.

3.3 13.56 MHz Inductive

The other industry standard frequency for silicon RFID devices is 13.56 MHz. Examples of such tags are the I-Code from Philips Semiconductor (shown in Figure 3-3) and the Tag-It from Texas Instruments. This frequency is used not only for tags but also for contact smartcards and other similar proximity devices. There are a number of standards that cover this space ([6]).

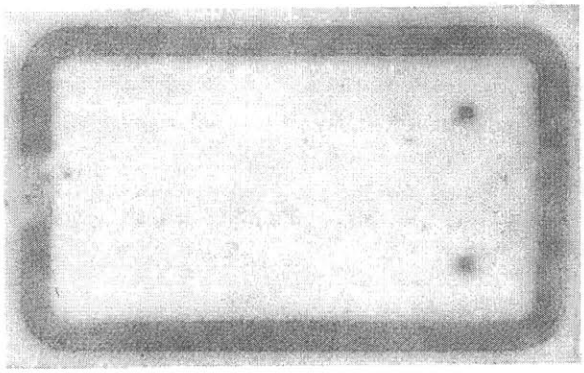


Figure 3-3: Examples of 13.56 MHz inductive tags. The coil antenna is clearly visible, and the transponder IC is in the middle left of the image.

As a result of the much higher frequency, devices in this regime can have much higher data rates (> 10 kbps), and use faster microprocessing cores, enabling data-protection techniques such as encryption. In addition, tags in this range can also implement anti-collision protocols. Typically these use very thin, planar antennas for the tags and single-turn coils for the detectors. The devices also power themselves up from the current induced in the antenna by the magnetic field of the detector antenna. Modulation schemes are more varied in this frequency range: some devices still use AM modulation (using similar load-modulation schemes for cost reasons), but FM modulation schemes such as FSK are also common, as the high clock frequency allows more complex clock division circuitry.

The tag used in this thesis is an I-Code tag from Philips Semiconductor that implements the ISO 15693-2 protocol[6] which is the current standard for contactless integrated circuit cards (also known as vicinity cards). The tags have a 512-bit EEPROM memory, divided into 16 blocks, which can be accessed individually, and a unique, 64-bit serial number. They also implement an anti-collision protocol.

When introduced into the field of the detector, the tag powers up, but unlike the 125 kHz inductive tags, no response is sent until the detector sends a command to the tag. The detector can detect the presence of a tag by the loading presented by the antenna of the tag when it is introduced into the detector's antenna field. The detector then uses an amplitude-modulation coding scheme to send a command to the tag. An example transmission waveform is shown in Figure 3-4. The data rate used can be a standard protocol at 1.655 kbps or a fast mode protocol at 26.5kbps. For the standard protocool, each byte in the transmission occupies a 4.833ms frame, which is further subdivided into 256 segments, where each segment is 18.88μs. In the figure, a byte value of 225 is transmitted via pulse position modulation: the second half of the 225th segment is attenuated.

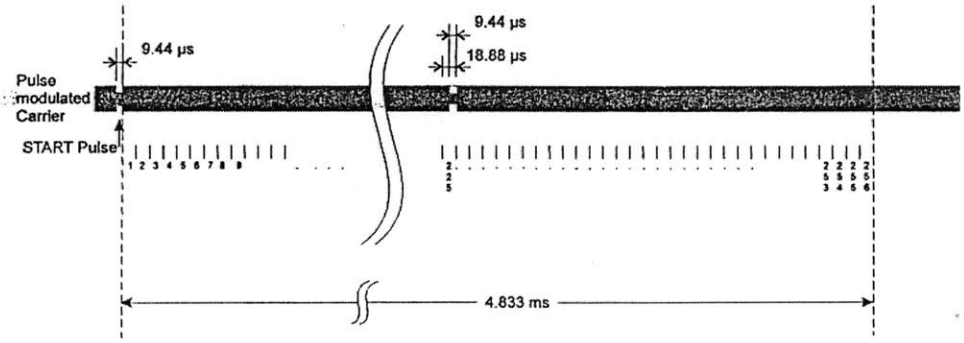


Figure 3-4: I-Code reader to IC standard data transmission protocol details, showing an amplitude modulated single byte frame[1].

Upon receiving the proper read command, the tag responds once with the requested data from its memory at a data rate of 26.5 kbps. Another request is necessary to access the bytes again. The protocol is outlined in Figure 3-5. Each bit occupies a 37.76μs frame. The bits are transmitted using a Manchester coding pro-

tocol on a subcarrier of 423.75 kHz. A '1' is coded by loading the first half of the bit period, and a '0' is coded by loading the second half. This subcarrier is then applied to the carrier, producing an image similar to that shown in the bottom of Figure 3-5.

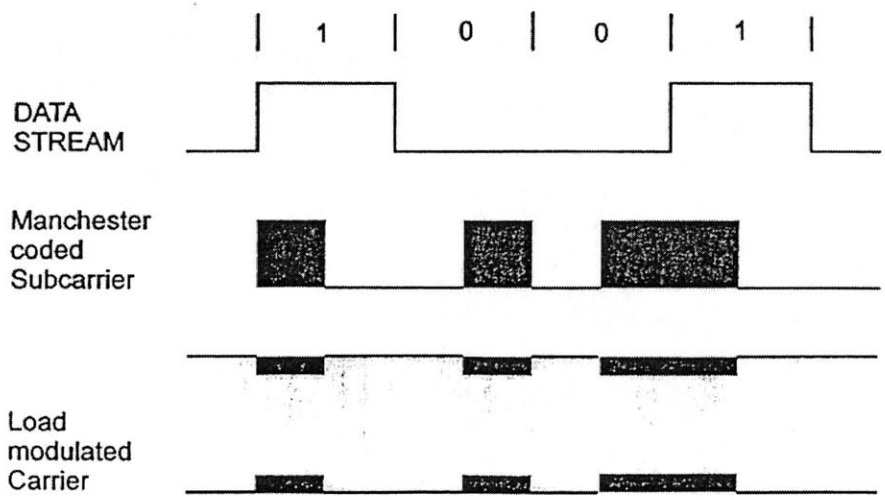


Figure 3-5: I-Code IC to reader data transmission, showing amplitude modulated, Manchester-coded byte frames.

3.4 58.5 kHz Mechanical Magnetic

The 58.5 kHz frequency is one of the two major frequencies used for Electronic Article Surveillance (EAS). The tags in this frequency range are often known as magnetostrictors: these are magnetic particles placed in a medium (usually in a strip form factor) that permits the entire structure to resonate mechanically when placed in a magnetic field at the appropriate frequency. The strip thus stores some of the energy from the magnetic field in the mechanical resonance. This resonant frequency is often a function of the length of the strip and the degree of magnetic bias of the particles. Figure 3-6 shows examples of enclosed and exposed magnetostrictors.

In EAS applications, such as department stores, strips of the appropriate length and magnetic bias are attached to each object of significance. The detectors (typically

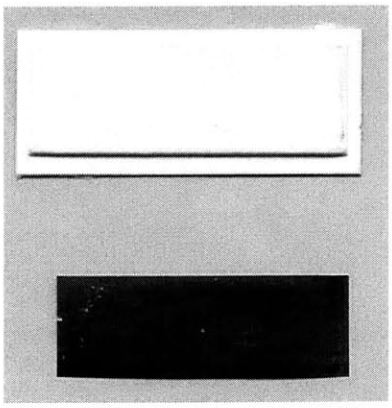


Figure 3-6: Examples of enclosed (top) and exposed mechanically magnetic resonators.

vertical towers) are placed at the store entrances, and provide a magnetic field created by running a signal at a 58.5 kHz excitation frequency through a coil antenna. The detectors operate using a pulse and ringdown method: the detectors broadcast the magnetic field for a certain period of time, allowing the strips to ring up with the supplied magnetic field, then shut off the transmission and listen for the decaying response from the tags. When the object passes through the magnetic field without being deactivated, this response is detected and alarms are set off.

To deactivate the tags, the strips are exposed to a strong magnetic field, usually at the checkout counter. This adjusts the magnetic bias of the particles within the strip, and shifts the resonant frequency of the tag above the excitation frequency provided by the detectors.

3.5 8 MHz Planar Inductive

8 MHz is the other major EAS frequency. Tags that operate in this frequency are typically planar resonators, made of etched copper patches with a dielectric sandwiched between them. An LC resonator is created from the distributed inductance of the copper patches and the distributed capacitance caused by the dielectric. Figure 3-7 shows an example.

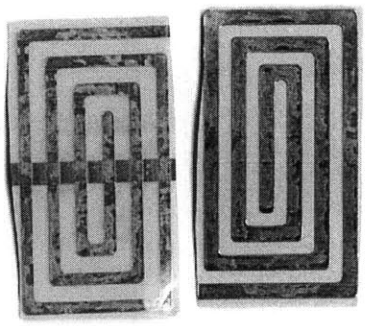


Figure 3-7: Examples of 8 MHz planar inductive tags.

The detector for these tags broadcasts a signal at around 8 MHz and uses a separate receive antenna. The tag presents a resonant tank circuit that couples to the broadcast signal and changes the signal profile at the receive antenna which is often in a bridge configuration. This bridge imbalance is then detected. Figure 5-5 shows a general schematic of a detector configuration.

To deactivate the tags, a strong electric field is applied, which breaks down the insulation between the coils and the horizontal strip, effectively shorting out the coils and eliminating the resonance.

Of interest in the field of planar resonators is the possibility of building planar structures with multiple resonances. The approach is to construct spatial structures which possess interesting spectral characteristics. Identity can then be attached to these spectral characteristics, and this provides a method to encode identity in purely physical structures, without the associated cost of VLSI devices. The detector for the planar inductive tags can be modified to operate at other frequencies within similar ranges (< 100 MHz), providing easy migration of current EAS-only tags and applications to this enhanced scheme. An example of one such tag and its frequency response graph are shown in Figure 3-8. The frequency response was obtained with the Astro reader, discussed in Section 5.1.

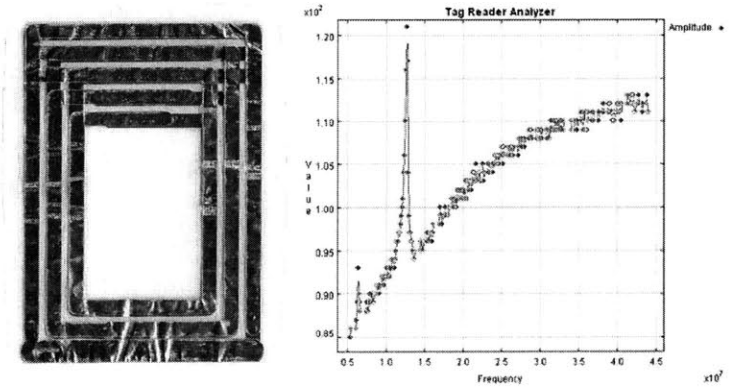


Figure 3-8: Complex spectral structure tag and associated frequency response. 2 of the 3 resonances in this structure are visible on the left side of the plot.

Chapter 4

Tag Reader Design Considerations

As discussed in Chapter 1, the requirements for an open architecture tag reader are the ability to generate a range of radio frequencies, apply varying modulation schemes at these arbitrary frequencies and detect the presence and the return modulation from the tags. The system is roughly separated into 4 components based on the tasks of signal generation, signal propagation and reception, signal detection and demodulation, and system control. The general pieces required for a tag reader are shown in Figure 4-1. The appropriate excitation frequency for the tag is generated by the transmit section. This signal is amplified then propagated through the antenna. The receiver extracts the tag's response and presents it back the control system, which passes it on to the application using the tag. A general schematic is shown in Figure 4-1.

For this thesis, the system was partitioned into four main subsystems, and the target devices place certain requirements on these components; these are discussed below.

4.1 RF Generation

The radio frequency generation subsystem performs the excitation frequency generation and the required modulation under the direction of the control subsystem (discussed in Section 4.4). For each of the tags, a different scheme is utilized:

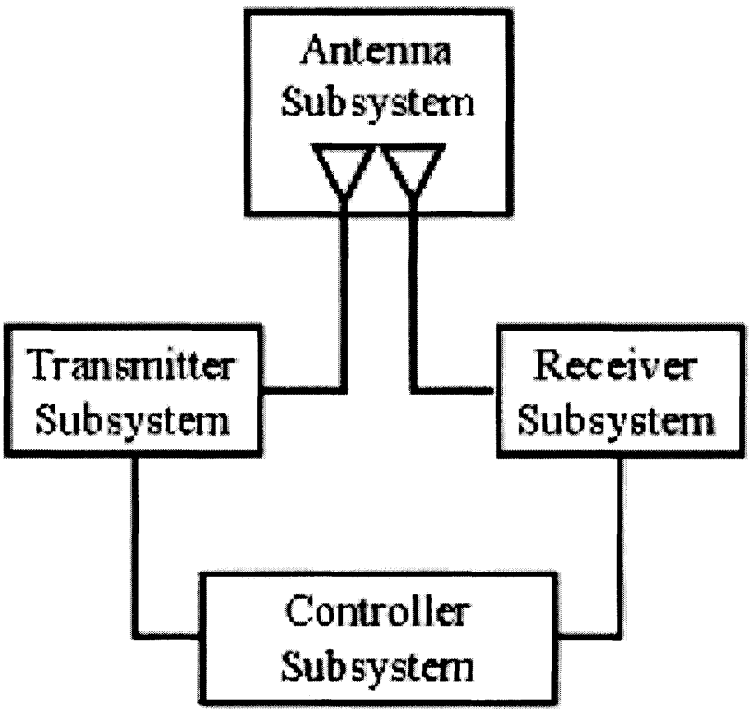


Figure 4-1: General schematic of generic tag reader system.

- To read from the 125 kHz inductive tag, an excitation signal at a frequency of 125 kHz must be generated: because the tag automatically starts transmission once it powers up, no modulation is required. To write to the tag, an amplitude modulation scheme using a 100% modulation index is required. The generation hardware has to be able to fully modulate the excitation signal (i.e. switch the excitation on or off).

- To read to or write from the 13.56 MHz inductive tag, an excitation signal at a frequency of 13.56 MHz is required as well as an amplitude modulation scheme using a modulation index of 14%. The generation hardware has to be able to set the output amplitude levels.

- To detect the 58.5 kHz EAS tag or the 8 MHz EAS tag, an excitation signal at a frequency of 58.5 kHz or 8 MHz is required. No modulation is necessary.

For this prototype, no significant range requirements are placed on the device. In addition, no consideration is being given to the purity of the RF output of the system: production systems would have to consider regulatory limits on side-band and harmonic signal output levels.

4.2 Antenna

For each tag, the antenna varies significantly as a result of the frequency. Commercial tag reader systems are optimized for operation at a single frequency and have antennas that are designed to present a specified impedance (typically 50 Ω) at that frequency. All components in the system (filters, amplifiers, etc) are designed to present and expect the same impedance at their inputs and outputs, and the impedance (and overall antenna performance) at any other frequency is of minimal importance. More often than not the antenna performance is required to degrade at other frequencies (typically to ensure that the system as a whole meets regulatory emissions levels).

In contrast, an open architecture RF tag reader optimally requires a single antenna with broadly even performance over its entire range of operation: however most wideband antennas tend to work equally poorly over the entire frequency range. Alternative strategies to this problem tend to lead to either completely switching the antenna with each different frequency, using an antenna structure which exhibits gain at the desired frequencies (a multiply resonant structure, which are fiendishly difficult to get right) or some kind of active configuration in which the antenna structure is modified (for example through the use of switched capacitor banks to change the antenna response at a desired frequency).

None of these approaches are optimal, and the very different detection methods of the various tags under consideration further complicate the issue:

- For these tags, the detection/demodulation occurs in the presence of the excitation signal from the RF generation subsystem. The modulation index from the tag to the detector is typically as low as 2%, and this amplitude disparity places special demands on the detection subsystem. In traditional readers

for these tags, notch and bandpass filters with significant attenuation outside the frequencies of interest are used to remove the unwanted excitation signal and enhance the weak modulation signal. Building variable filters that work well at all of the given excitation and modulation frequencies is possible, but building such a filter with enough generality to operate at other frequencies is a significantly difficult task.

4.3 Signal Detection

The detection subsystem shares the task of separating the tag response from the excitation signal and background noise with the antenna. It performs the signal conditioning and analog to digital conversion required for the digital signal processing subsystem. All the tags being detected use amplitude modulation schemes so the same basic signal conditioning algorithm can be applied for all the tags.

The signal detection chain is however required to be able to operate at frequencies up to 13.56 MHz, and from the Nyquist sampling theorem the analog-to-digital conversion process must be capable of sampling at least at twice that frequency. It may be necessary to sample at higher rates (depending on the detection requirements), and it may be possible to sample at lower rates (given that the data rate is significantly lower than 13.56 MHz, and for all practical purposes that is what the tag reader is interested in).

4.4 Digital Processing and Control

The digital processing and control subsystem provides the logic to control the RF generation and signal detection subsystems. It provides the digital signal processing required to interpret the output of the signal detection subsystem (which is a digital sample of the received signal amplitude level) and translate the modulation into digital data.

It should operate at frequencies at or above the fastest sampling rate used in

the signal detection subsystem, and it has to perform the translation (i.e. confirm whether or not a tag is present) within certain time frames; for the purposes of this thesis, a 100 ms time frame is the goal, as this is an acceptable detection rate for some human-computer interface (HCI) applications. This system is not geared specifically towards HCI applications (as opposed to commercial or industrial applications), but may be more easily used for applications in that field.

Chapter 5

Implementation Details

5.1 Preceding Work

Prior to the development of this tag reader, much work had been done on tag reader development, with the emphasis on materials-based tags[9]. Of particular interest is the work done on a wide-band tag reader, christened the Astro[1] reader. This reader was designed to perform simple spectral characterization of resonant materials structures. The frequency range of operation is from 5 MHz to 80 MHz. The functional blocks of this tag reader are shown in Figure 5-1. The system is based around a Microchip PIC16C76 microcontroller. The frequency generation is done by a single Analog Devices AD9850 or 9851 Direct Digital Synthesis (DDS) chip, which can output any frequency from DC up to 60 MHz (90 MHz for the 9851) using a lookup table and a digital-to-analog converter. The output of the DDS is passed through a 4-pole low-pass filter to remove the higher-order alias frequency harmonics, and this filtered signal is then amplified using a Analog Devices AD8011 fast operational amplifier.

The Astro reader accomplished resonance detection using a 50 Ω directional coupler configured to measure antenna loading. In this configuration, the untuned single-turn antenna presents an optimally unmatched load and the reflected power is channeled through the directional coupler output. However, when a resonant structure

[1]The name comes from a visitor to our lab, who said the tag reader reminded him of a cartoon dog called Astro; for lack of a better name, it stuck.

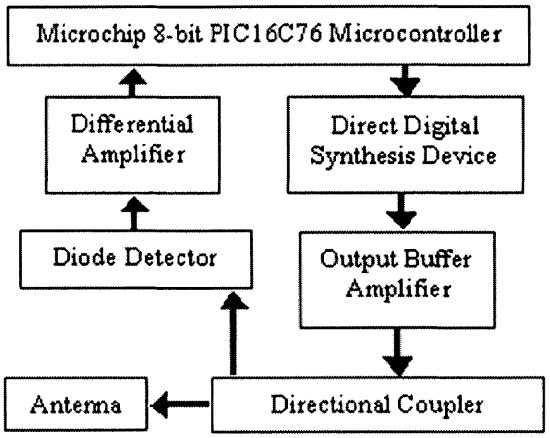


Figure 5-1: Block diagram of the wide-band Astro tag reader.

is placed within range of the antenna the impedance of the resonator dominates the response. When the frequency of the signal into the directional coupler is equal to the resonator's resonant frequency, the resulting modified impedance produces a change in the reflected power. This method of detection eliminates the need for a broad-band tuned antenna, and since the antenna is untuned, the tag reader is immune to spurious responses caused by any stray reactance in the environment.

The directional coupler's output is rectified with a diode-based square-law detector and the signal is sampled using the analog-to-digital converter integrated into the micro controller. The micro controller scans the output of the DDS device between programmable limits using a programmable increment (the interface is discussed in Chapter 6)and records an 8-bit sample at each frequency. The measurement that is transmitted through the serial port is an 80-byte data packet of these samples. This measurement is made once every $105ms$.

For some applications[10], the serial port output is connected directly to a converter device which broadcasts the data on a local Ethernet network. Remote computers connected to the network take the data off the network and can then process the data as desired. The interpreter, shown in Figure 3-8, is written in Java; it receives the broadcast data from the tag reader and plots the data. The device itself is

shown in Figure 5-2.

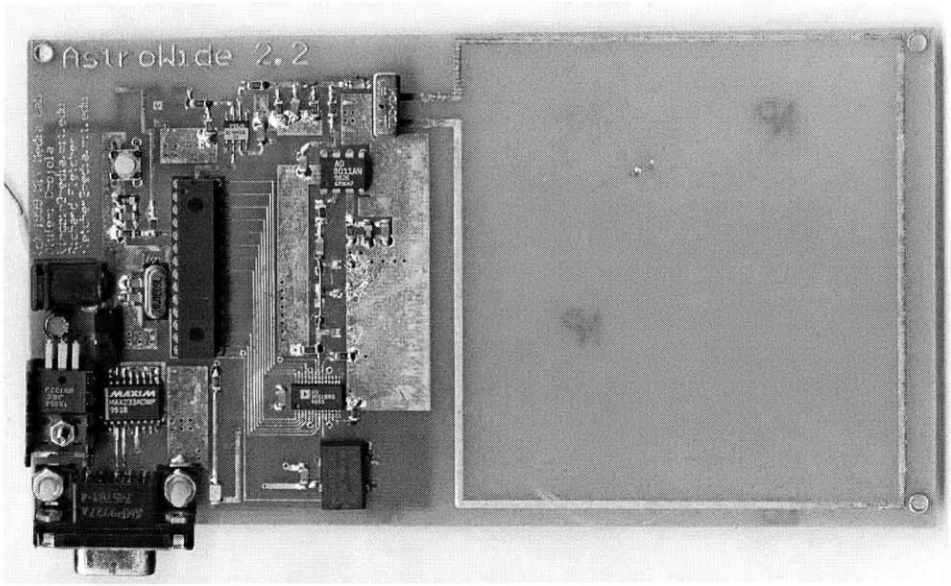


Figure 5-2: Photograph of the wide-band Astro reader.

5.2 Hardware Design

This tag reader is implemented using 3 system boards and an external antenna, where each board roughly corresponds to one of the subsystems introduced in Chapter 4. The functionality of each of the subsystems is discussed below. Each board is designed around a common form factor, in which a 44-pin digital control bus is used to send command signals from the digital control subsystem to the other 2 boards. Each board measures 3.78 inches by 2.34 inches, and the boards are designed to be stacked. The right side of the boards hold the 44-pin connectors for the control bus and digital power and ground, and the RF connections to and from the antenna use SMA connectors mounted on the left side of the RF generation board and signal detection boards.

5.2.1 RF Generation

The RF generation subsystem uses a single Direct Digital Synthesis chip, the AD9852 from Analog Devices to provide wideband, frequency- and phase-agile signal generation for the tag reader. The chip uses a fairly simple digital control protocol to generate complementary sinusoidal outputs with frequencies from DC out to 150 MHz with 48-bit resolution using a variable input clock and an internal clock multiplier: the control lines are all provided by the 44-pin control bus. An onboard comparator is provided for use in generating square waves for agile clock applications. The chip can also perform amplitude control, frequency sweeps (chirps), amplitude modulation and frequency and phase shift keying of the output signal. Figure 5-3 shows a schematic for the design.

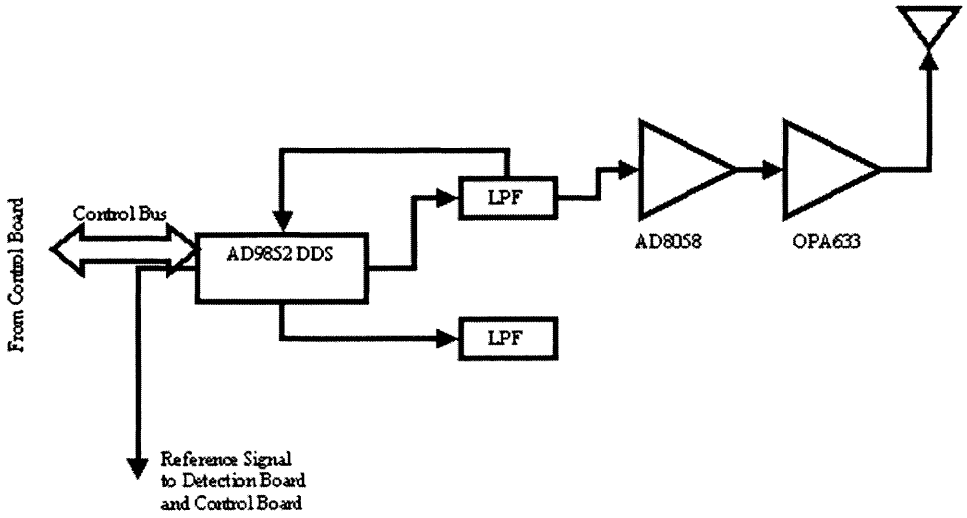


Figure 5-3: General schematic of the RF generation subsystem board.

The complementary signals are run through 7-pole low-pass filters with 3dB points at 120 MHz. The output of the filter on the non-inverted signal is then amplified using one half of an Analog Devices AD8058 high-speed operational amplifier. The output of this amplifier is run into a Burr-Brown OPA633 buffer amplifer which boosts the system's ability to source large currents into low impedance loads, allowing a peak output of $800mW$ into a 50Ω load. The buffer is placed in the feedback loop of the

AD8058 to minimize the effects of the buffer's phase shifts on the signal stability. The output of the buffer is then connected to the antenna through one of the SMA connectors mounted on the edge of the board. This SMA connector is connected to the antenna input.

The high-speed comparator takes the filtered signal outputs (both normal and complementary) and provides a square wave that can be used for high-speed, agile clock applications. In this case, the output of this comparator is connected to the digital signal bus and is used for synchronous demodulation in the signal detection subsystem. This signal is also accessible to the digital processing subsystem for synchronization purposes.

A secondary signal output is available from the chip that can be used to generate sinusoidal signals with frequencies up to 150 MHz, and this is useful for more complex modulation and signal mixing tasks. None of the tags in this thesis required the use of this signal, but the output of this signal is amplified by the second half of the AD8058 operational amplifier and connected to a second SMA connector on the edge of the board to be used if required by another application.

The AD9852 is a very highly integrated chip, and can potentially draw up to $500mA$. For this reason, an onboard regulator for the analog circuitry is present; this uses a Linear Technologies LT1085 low-dropout regulator powered from a 3-pin SIP connector. A photograph of the actual 4-layer board is shown in Figure 5-4: the AD9852 DDS chip is in the middle left. A full schematic is shown in Appendix A.

5.2.2 Antenna

Conventional tagreaders that operate at single frequencies use antennas matched to the signal input and output stages at the specific frequencies of interest. In addition, as discussed in Section 4.2, signal detection chains usually have notch and bandpass filters that are specific to the frequency of interest to eliminate unwanted high amplitude signals. For wide-band tag readers, such filters can not be used, but the signal elimination is still required. The signal elimination becomes even more important in the context of the digital sampling: given the small modulation indices used by

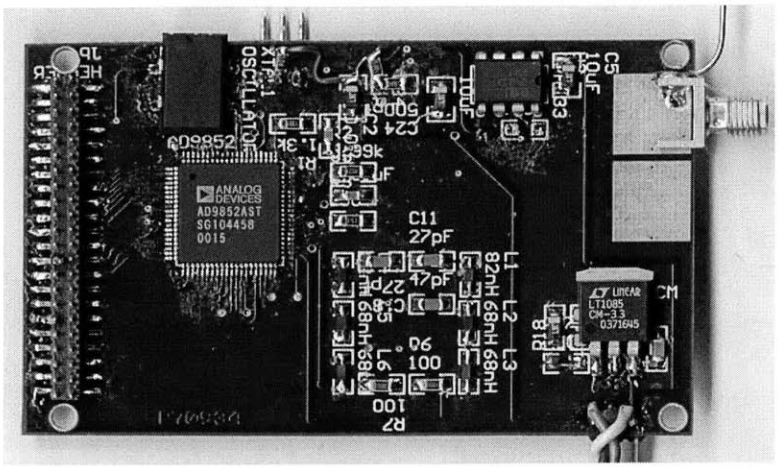


Figure 5-4: RF generation subsystem.

the tags to transmit data, any attempt to sample the signal without eliminating the excitation frequency results in the waste of most of the bits of resolution provided by the analog-to-digital converter. Unless extreme precautions are taken to eliminate noise within the signal chain, no recovery of the modulation will be possible.

This problem, which falls into the general category of extracting a small signal from a large signal, is solved in this implemenation using a bridge structure. A schematic of this is shown in Figure 5-5. Since the common mode signal through both arms of the bridge is the excitation frequency, this can be largely eliminated in the detector subsystem using a differental amplifier, eliminating the need for filters.

There are 2 frequency ranges in use: the first includes frequencies less than 1 MHz (the 58.5 kHz and the 125 kHz frequencies) and the other includes all frequencies above 1 MHz (the 8 MHz and 13.56 MHz frequencies), and a different antenna is used for each range. For the high frequency antenna the structure was produced using a computer-controlled industrial vinyl cutter on a copper substrate; the antenna structure was designed using a CAD program on an personal computer and the pattern is cut out of a thin (40 mils thick) sheet of copper. The pattern is then transferred to a Plexiglas backing for support, and the bridge resistors and signal path SMA connectors are soldered onto the copper. For the low frequency structure a commercial PCB process with tinned copper traces was used.

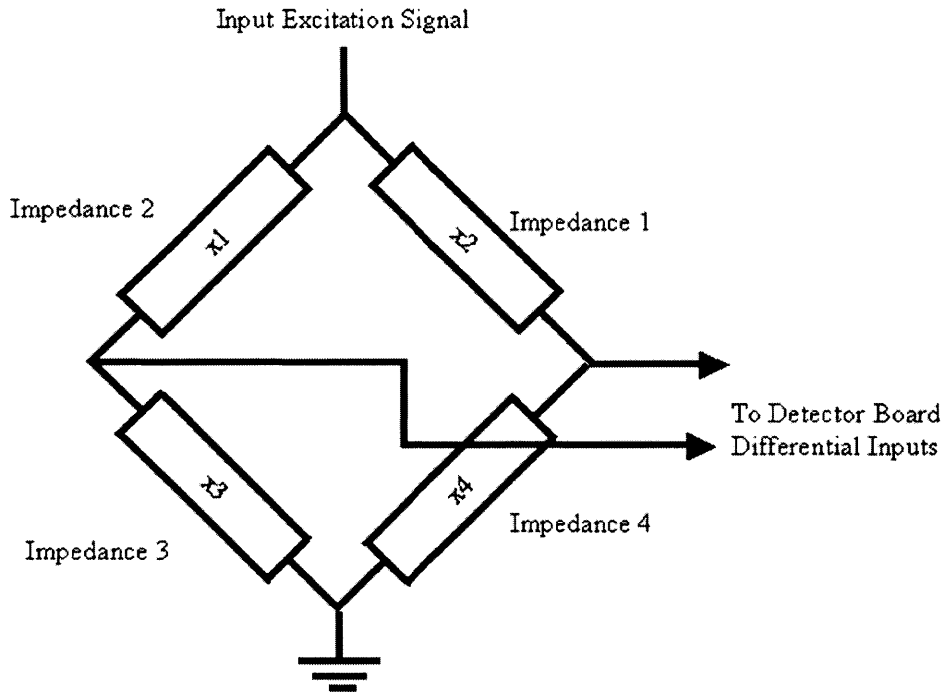


Figure 5-5: General schematic of the bridge antenna.

Each antenna consists of 2 coils, each coil possessing an identical number of turns; for the high frequencies, single turn coils are used. Each coil is connected directly to a common source signal through an SMA connector, and through separate resistors to a commmon ground. The antenna has 2 outputs to the signal detection circuitry, taken from the connection between each coil and resistor. An SMA connector is provided for each of the outputs. Figure 5-6 shows the high frequency antenna; Figure 5-7 shows the low frequency antenna. Each antenna has a DC impedance of 50Ω; the resistive element in each leg of the bridge is 100Ω. The high frequency antenna has a self-resonance at 81.62 MHz with a Q of 43, while the low frequency antenna has a self-resonance at 61 MHz, and an effective Q of 0; the low Q values are a result of the high resistive losses in the bridge.

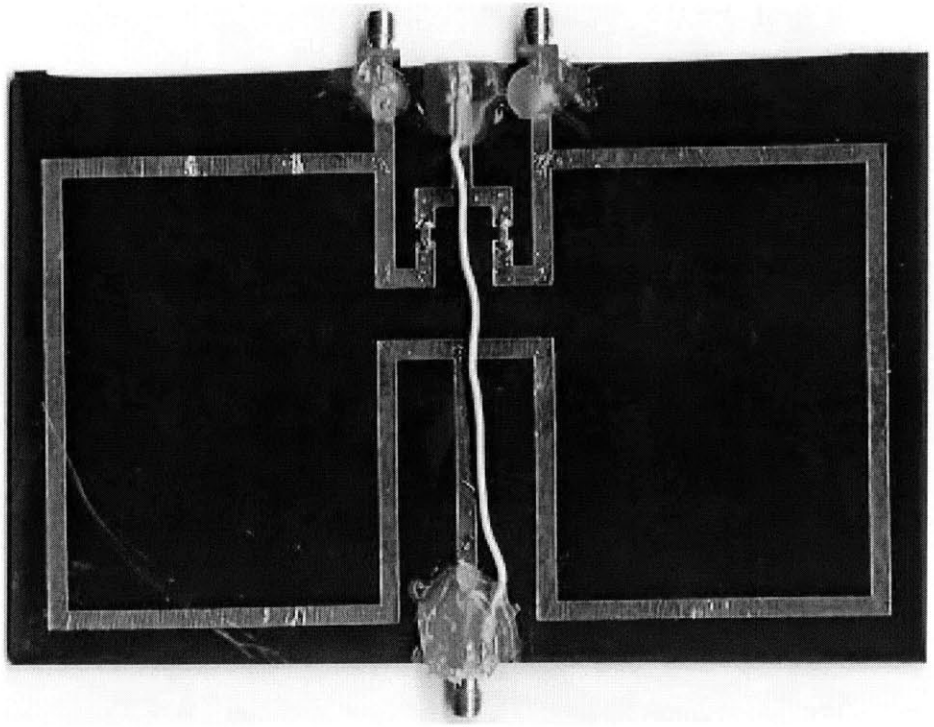


Figure 5-6: High Frequency Antenna.

5.2.3 Signal Detection

The output of the antenna is a signal from each arm of the bridge antenna. The detector board takes these signals using SMA connectors and inputs them into a differential amplifier. The differential amplifier used is an Analog Devices AD8132 high-speed differential amplifier with complementary outputs set to provide 2.5 dB of gain: the low gain setting was picked to provide an output no greater than $300mV$. The output of this is synchronously demodulated using an Analog Devices ADG453 high speed switch, capable of switching in 7 ns: this synchronous demodulation stage is essentially a frequency specific rectifier. The switching control signal is either supplied manually by the control subsystem or from the output of the comparator in the AD9852 signal generation chip on the RF generation subsystem. This allows demodulation to be done to extract signals at frequencies and phases other than the excitation frequency (by using an alternative reference signal generated by the control subsystem). A schematic for the design is shown in Figure 5-8.

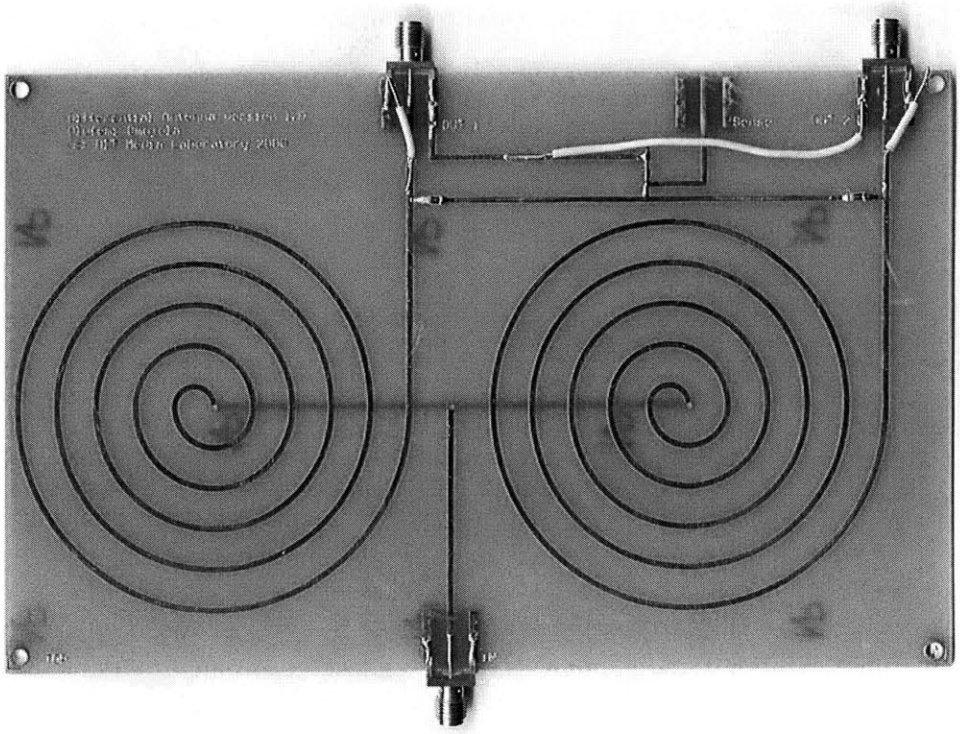


Figure 5-7: Low Frequency Antenna.

The output of the synchronous demodulation stage is connected to a 4-pole variable low-pass active filter, which is a modified Sallen-Key filter using a Linear Technologies LT1630 dual operational amplifier and an Analog Devices AD8403 quad digitally programmable resistor as the control element. This filter allows a variable 3 dB point that can be changed from about 900 Hz to 230 kHz, with up to 80 dB of attenuation per decade.

The filter output is sampled using a Burr-Brown ADS800 analog-to-digital converter, which has a maximum sample rate of 40 MSPS, and the output of the ADC is connected to the digital control bus. A photograph of the actual 4-layer board is shown in Figure 5-9. A full schematic is shown in Appendix A.

5.2.4 Digital Processing and Control

The control signals out to and the data from both the generation subsystem and the detector subsystem are connected through the data bus to the digital processing and

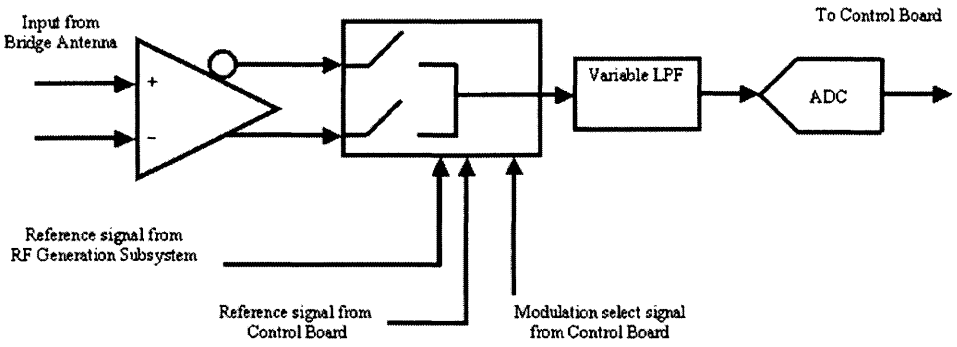


Figure 5-8: General schematic of the RF detection subsystem board.

control board. This board handles both general configuration and control of the entire system, interfacing with external control programs, and digital signal processing of the input from the detector subsystem. A schematic for the design is shown in Figure 5-10.

The central control element used is a Microchip PIC16F876 microcontroller, which is a simple 8-bit microcontroller with a 20 MHz RISC core and 8K instruction words. This controller integrates a Universal Asynchronous Receiver Transmitter (UART) module with 22 I/O pins and provides the external interface and sequencing of the digital signal processing (DSP) element. The microcontroller is connected to a bank of 4 Microchip 24AA256 serial Electrically Erasable Programmable Read-Only Memory (EEPROM) chips which provide 1 Megabit of persistent storage for the system: the device interpreters (discussed in Section 5.3.3) are stored in the EEPROM memory. The microcontroller is connected via an 8-bit parallel port to a Xilinx XCS30XL Field Programmable Gate Array (FPGA) which provides the DSP processing.

The XCS30XL is a 100-pin device that provides the equivalent of 30000 gates: the configuration can be changed by software in real-time (in milliseconds without powering down the system) either through an external port using the Joint Test Access Group (JTAG) protocol, or by the microcontroller through a 5-wire port using a serial protocol. This is discussed in detail in Section 5.3. The XCS30XL handles the physical and logical connections to the system bus, as well as handling the DSP

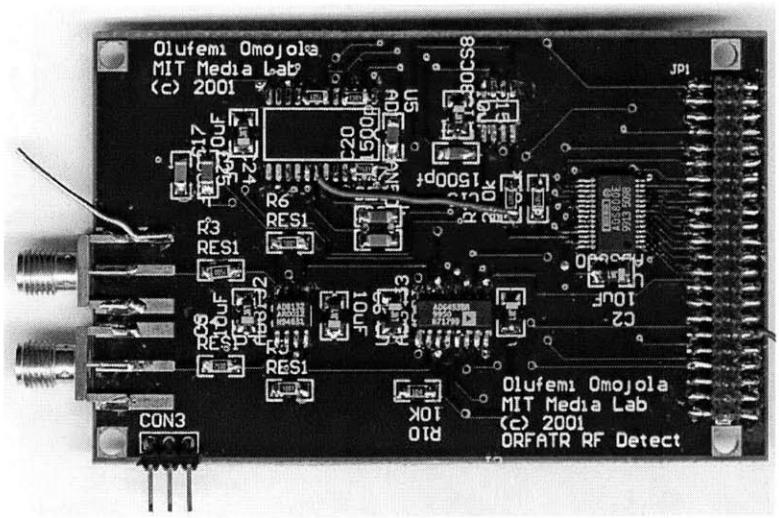


Figure 5-9: RF detection subsystem.

tasks required for different devices, and is at the core of the system's ability to detect and/or demodulate new devices. A photograph of the actual 4-layer board is shown in Figure 5-11. A full schematic is shown in Appendix A.

5.3 Software Design

The controlling software for the tag reader is implemented in 2 different pieces. External control software interacts with the management software running on the PIC16F876 (written in C and compiled to PIC assembly) on the control board. This routine does all the external interfacing, manages the EEPROM-based filesystem and the FPGA configuration, and sequences the operation of the FPGA during detection/demodulation operations.

5.3.1 Controller/External Interface

The external interface to the the tag reader uses the RS-232 protocol as the transport layer: the UART is integrated into the PIC16F876 microcontroller. The design bias of the tag reader is towards embedded applications so the system does not actually use the RS-232 voltage levels: the communications port uses TTL levels, and interfacing

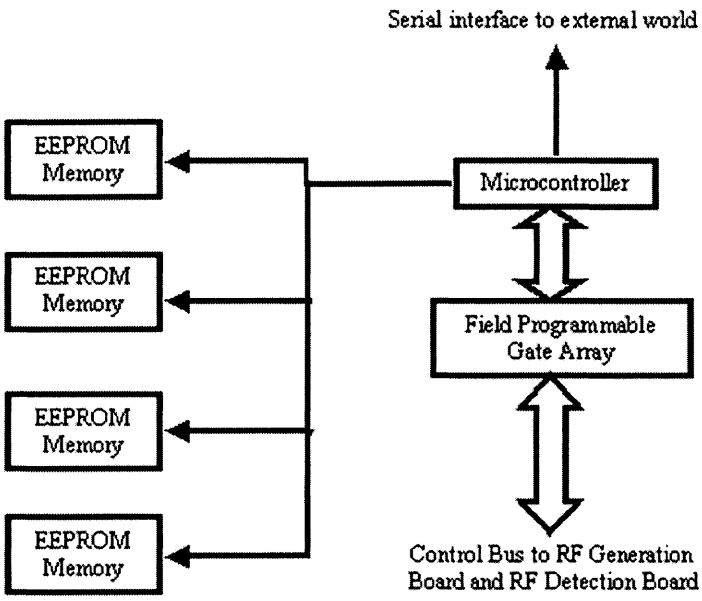


Figure 5-10: General schematic of the digital processing and control subsystem board.

to a PC or other such device requires the use of an external level shifter; Figure 5-12 shows one such device.

The controller software handles the EEPROM filesystem, which is a simple, linked-list structured storage system that is used primarily to store the device interpreters, which are FPGA configuration files specific to the task of detecting/demodulating a specific tag. The filesystem can also be used to store detection data as well.

5.3.2 DSP Configuration

The FPGA in the system is used as a bus interface device (to communicate with and control the other 2 boards), and as a DSP to perform the detection/demodulation functions of the system. The FPGA configuration is developed using an interactive process and then loaded into the system through the external serial port and saved into the EEPROM filesystem. When the system as a whole powers up the FPGA is blank: microcontroller settings are used to select which configuration file is to be loaded on startup, and the microcontroller configures the FPGA using a trivial serial

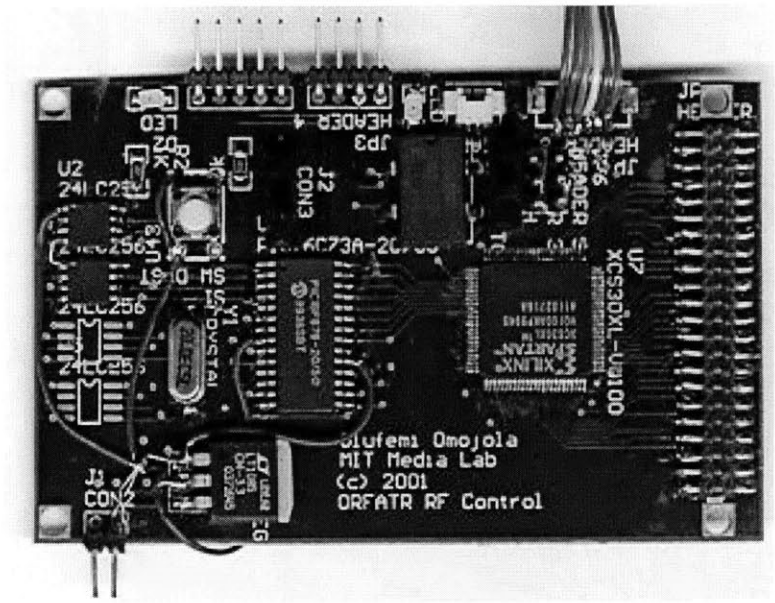


Figure 5-11: Digital processing and control subsystem board.

bit-dribbling protocol to set the appropriate internal configuration registers. Multiple configuration files can be stored, one for each of the tags the reader supports, up to 4 (for this system).

5.3.3 Device Interpreters

The device interpreters are central to the open architecture concept: these are FPGA configurations that allow the tag reader to change the interface layer that connects to the generation and detector subsystem. Each interpreter is structured as an initialization block that sets the appropriate parameters for the generation subsystem (excitation frequency and amplitude), the detection subsystem (ADC clock frequency, low-pass filter cutoff frequency, synchronous demodulator source input), and the FPGA internal post processing of the output of the detector board. The FPGA then accepts sequencing instructions from the microcontroller that tell it when to perform what operations. The sections below describe the operations performed by each device interpreter, and example Verilog code for one such interpreter is listed in Appendix B.

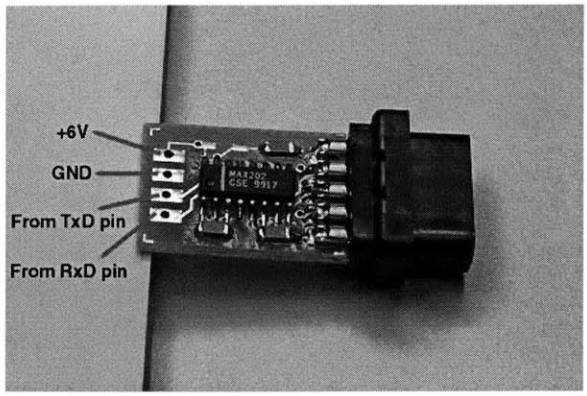


Figure 5-12: TTL to RS-232 level conversion device.

125 kHz Inductive

For the 125 kHz inductive tag, the generation subsystem is programmed to output a full-scale amplitude sinusoidal signal at 125 kHz through the primary DAC of the DDS device. The detection subsystem is programmed to synchronously demodulate using the excitation reference signal from the generation subsystem, lowpass filter the output of the synchronous demodulator with a filter bandwidth of 10 kHz, and sample the input signal at 100 kHz. Within the FPGA, a digital comparator determines the maximum difference between each sample in the absence of a tag and saves this threshold. It also saves the average sample value.

When a tag is introduced into the region of the antenna the loading reduces the average sample value, and this change is used to detect the presence of the tag. The amplitude modulation is detected by measuring the difference between samples and noting when the difference between samples exceeds the threshold value. The cycles are tracked using a counter that is run off the reference signal from the generation subsystem, and this counter is used to detect the bit transitions.

Since the tag starts transmitting immediately, the FPGA starts keeping an internal buffer that stores the values of the bits as they are decoded the moment the tag is detected. The FPGA then places the bytes on the bus to the microcontroller, which then takes the bytes off the bus and searches through the bytes for the start sequence. It then outputs the actual data through the serial port if necessary.

13.56 MHz Inductive

For the 13.56 MHz inductive tag, the generation subsystem is programmed to output a full-scale amplitude sinusoidal signal at 13.56 MHz through the primary DAC of the DDS device. The detection subsystem is programmed to synchronously demodulate using the excitation reference signal from the generation subsystem, lowpass filter the output of the synchronous demodulator with a filter bandwidth of 28 kHz and sample the input signal at 250 kHz. Within the FPGA, a digital comparator determines the maximum difference between each sample in the absence of a tag and saves this threshold. It also saves the average sample value.

When a tag is introduced into the region of the antenna the loading reduces the average sample value, and this change is used to detect the presence of the tag. The amplitude modulation is detected by measuring the difference between samples and noting when the difference between samples exceeds the threshold value. The cycles are tracked using a counter that is run off the reference signal from the generation subsystem.

When the tag is detected, the FPGA transmits the command frame to reset the QUIET bits within the tag (which ensures that the tag will respond to any unselected read command), then sends another command frame to perform an unselected read of the 64-bit serial number from the tag within the antenna (the tag reader does not implement the anti-collision protocol, so multiple tags are not supported). Both these operations are performed by modifying the output level of the AD9852 on the generation subsystem board.

The tag replies with the serial number, and the FPGA takes the bits and places them on the bus to the microcontroller. The microcontroller takes the bytes off the bus, searches through them for the serial number and outputs them from the serial port if necessary.

58.5 kHz Mechanical Magnetic

For the 58.5 kHz mechanical magnetic resonators, the generation subsystem is programmed to output a full-scale amplitude sinusoidal signal at 58.5kHz through the primary DAC of the DDS device. The detection subsystem is programmed to synchronously demodulate using the excitation reference signal from the generation subsystem, lowpass filter the output of the synchronous demodulators with a filter bandwidth of 2 kHz and sample the output at 100 kHz. The FPGA executes the detection strategy outlined below in the absence of any tag and saves the value as a threshold.

For the detection, the FPGA demodulates using the reference signal from the AD9852 to control the switch. A running sum of samples is taken with one sample every 20 microseconds. The FPGA than switches the demodulation reference to a manually generated clock; this clock pulse is generated by observing the reference signal from the AD9852 and generating a demodulation signal that trail the edges of the synchronous reference by one quarter of the period of the excitation signal: the FPGA has a timebase that permits intervals of $8.33ns$ to be distinguished, allowing reasonably accurate generation of a demodulation signal with a phase lag of $\pi/2$. An identical running sum of samples is taken with this demodulation signal. These sums are then used as the in-phase and out-of-phase components of the response, and converted into magnitude and phase values. If any of these values exceed the thresholds, the FPGA outputs all 4 values on the bus to the microcontroller, which then outputs the information on the serial port if necessary.

8 MHz Planar Inductive

For the 8 MHz planar inductive tag, the generation subsystem is programmed to output a full-scale amplitude sinusoidal signal at 8 MHz through the primary DAC of the DDS device. The detection subsystem is programmed to synchronously demodulate using the excitation reference signal from the generation subsystem, lowpass filter the output of the synchronous demodulators with a filter bandwidth of 2 kHz. The FPGA executes a detection strategy identical to that for the 58.5 kHz resonators,

with the only significant difference being the frequency at which the operations are executed.

Chapter 6

Tag Reader Control Interface

The concept of a common control model for all tag readers is targeted towards a single interface for all embedded tag reader control and interface programs. I am attempting to develop a standard set of possible control commands that an external agent would need to be able to control and communicate with a given tag reader. As an example, in all of the tag readers described in [9], there is the ability to scan over a part of the tag reader's excitation frequency range with variable resolution. As a result, a command to set the frequencies at which the scan starts and stops is necessary. Given that all the tag readers I have worked on till now have used microcontroller-based control systems, defaults are set during the power-up cycle of the microcontroller. In the course of the tag reader's use there is typically a need to change these values. In a similar fashion, there is other functionality that requires external control and is shared across all tag readers, and this points towards a standard tag reader interface. The communications and control channel (the means by which external agents interface with the tag reader) and the protocol (the channel-specific format used to transmit data) differ between tag reader implementations and applications. As an example, some tag readers use the Wiegand channel and protocol (for access control applications), while I have used the RS-232 channel and protocol in this system (and in prior systems developed in the same laboratory). A design goal for the interface is a set of tag reader commands that are independent of the channel and protocol. An external agent would use these to control various functions and request changes in the state of the tag reader's control

program. Currently the RS-232 serial protocol is the default channel used by our tag readers, as our microcontrollers come with hardware peripherals that implement that protocol. For applications that require multiple tag readers to interface with control programs that may reside on the same computer, the RS-232 channel fails to scale efficiently as the number of tag readers increases. The advent of cheap Ethernet connectivity has increased the Ethernet communication channel's viability, and Ethernet scales much better than any serial protocol. As larger numbers of tag readers need to be connected to common information and/or data collection systems, such channels become increasingly attractive. The same control commands and interface should be usable irrespective of the channel being used, which will allow changes to the communication channel beyond even Ethernet. A standard software interface simplifies the development of subsequent tag readers by providing a common command set, a subset of which could be implemented in any particular tag reader, depending on the capabilities of its hardware. Separating the design of the tag reader's control structure from the hardware implementation allows us to develop a single robust control program (for a workstation) that would be able to control any tag reader and monitor its data visually (if appropriate). This approach has proven useful as applications have emerged that require multiple tag readers connected to a network without human intervention.

6.1 Control Modes

The interface differentiates between two types of external agents: human and machine. As a bias towards human controllers (and the default control and communications channel, the RS-232 interface) the commands are typically ASCII (American Standard for Communications and Information Interchange) byte sequences and tag reader responses as well as data output are also in ASCII format. For human control, the tag reader inserts visual framing characters (such as carriage return characters for data output) into the tag reader's output data stream. Also, reference information is inserted into the stream (such as text descriptors of returned data and text prompts

for commands with interactive properties). The machine control mode is designed for reliable control by software programs that need to either run specific sequences of commands or do reliable data plotting and collection. Framing bytes are inserted into the data stream between the control program and the tag reader to simplify synchronization. No visual framing characters or reference information about returned data are inserted into the data stream. Data is not returned in ASCII format, but as raw byte values, adjusted to account for certain values reserved for framing and synchronization.

6.2 Output Data Format

One common thread through all our previous tag readers is that, by default, they perform a scan of a section of the RF spectrum and elicit one or more data values regarding the response in the environment of the antenna at that frequency. This implementation is different in that the focus has been on specific single frequencies, but it nonetheless retains the ability to perform similar frequency scans. On the tag reader, an arbitrary amount of post-processing can be performed on the data obtained from the antenna before it is output through the main communications/control channel (arbitrary in the sense that the interface specification does not discuss what post-processing can or can not be performed). The interface provides for standard output formats for the case where no pre-processing is done on the raw data. For the human control mode, the default output format is a sequence of lines, each line representing a single point in the data scan. Each line starts with an asterisk followed by an ASCII representation of the particular frequency point. Next, ASCII representations of the associated data values are output, separated from each other and from the frequency value by a single space. The line is terminated with a carriage return. In general, terminal emulation programs have been used to interface with and control the tag reader, and the use of asterisks and carriage returns as framing characters are a reflection of this. Figure 1 below shows an example of the output of a tag reader in human control mode that takes 2 measurements per frequency value,

where each measurement is a 16-bit value, and the frequency representation is a 32-bit value (for this thesis, 48-bits would be required to capture this information). The values are transmitted in base-16 format (which is a more compact representation than the default decimal format, and as such minimizes the data transmit time), and <LF><CR> represents a line feed, carriage return pair. Figure 6-1 is an example of one output line from such a scanning reader.

*0021FEFC 0124 0234<LF><CR>

Figure 6-1: Sample tag reader output.

For the machine control mode, the default output format is simply a sequence of raw data values. These are arbitrarily sized (for multi-byte values, the MSB (most significant byte) comes first) and run from the data values from the frequency at the start of the scan to the frequency at the end of the scan, inclusive. The intent is that upon startup the control agent will synchronize with the tag reader to discover the start and stop frequencies, as well as the size of the difference between frequency points. If necessary, the program can append these values to the appropriate data points by itself, reducing the bandwidth requirements on the data channel. A discovery command is implemented that will return the number of data values per frequency point and the size in bytes of each value. The data is output in a packet format, with the start of the data packet (and the start of the frequency scan) indicated by a byte value of 0. The end of each packet is also marked with a 0 (for cases where the data from the scan extends over more than one data packet). The control agent uses these markers at the beginning and end of each packet for synchronization, and to accommodate channels that may impose arbitrarily small data packet sizes. The end of each frequency scan is indicated by a byte value of 1. Figure 2 below shows the packet structure for a tag reader in machine control mode that takes 1 measurement per frequency value, where each measurement is an 8-bit value, and the frequency representation is a 48-bit value. The channel used is limited to 6 byte packets, and the entire frequency scan is 6 points.

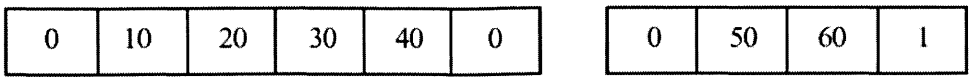


Figure 6-2: Sample packet structure.

6.3 Commands

The commands consist of byte sequences sent by the external control agent. The tag reader implements a passive control structure that is interrogated by the external agent, and some commands elicit a response from the tag reader. Each command begins with a command byte, an arbitrary number of modifier bytes after the command byte and an arbitrary number of data bytes after the modifier bytes. Some commands allow or require interactive responses. The basic structure is shown in figure 3 below. The first byte, 0x61 (in hexadecimal) is the ASCII character 'a', the command byte used for the set start frequency command in tag readers with frequency scanning capability. The command has no modifiers, and is followed by an ASCII representation of the desired start frequency, (in this case, 5 bytes, all ASCII characters, representing the number 60000), which is translated into a numeric value within the tag reader. The command is optionally terminated with the ASCII character '\n', 0x2E. In machine control mode, the tag reader responds to all commands with a data packet. The packet is started with a data value 2 and terminated with a data value 3, and may or not contain any data. This is in place of the 0 and 1 framing bytes outlined in section 3 above. The listing in Appendix C gives a basic grouping of the commands, descriptions of each command and associated special properties. It lists the associated byte sequences for both directions of the data stream (to and from the tag reader) and gives a reference for the data stream for both human control and machine control.

Chapter 7

Results and Conclusion

As of yet, the system is not fully functional. The hardware components all perform as expected, the system tests well in simulation, but several developmental issues emerged during the hardware and software integration, ranging from unexplainable interactions between the clock chip for the FPGA and the microcontroller programmer in the control module, to significant pollution from the RF generation subsystem's reference signal into the detector circuitry through the control bus.

The evolution of the design of this project went from the comparatively simple hardware utilized in the first wide-band tag reader discussed in Chapter 5 through a design in which I attempted to perform baseband sampling at 40 MHz and reconstruct the entire analog signal chain in digital logic within the FPGA. That design worked poorly at best, and evolved further to the current design where the digital logic is no longer being used for arbitrary signal processing, but rather for limited logic functionality, and the objective is to find generalized analog signal chains, rather than arbitrary digital implementations. The cost and complexity associated with re-creation of analog functionality within the digital domain is currently very high. One day, this may change.

The use of the antenna in a bridge configuration to communicate with the silicon tags is a useful approach that when completed could provide additional information (such as relative orientation of the device with respect to the antenna by measuring the sign of the bridge imbalance). The frequency specific rectification technique used

for the synchronous demodulator shows potential to be a very broadband detection technique, and I intend to continue working on it over the next year.

7.1 Future Work

The implementation of the software radio techniques used here requires extremely careful attention to detail to prevent ringing on the synchronous demodulator's switching signal and noise from the switching action from polluting the output of the bridge: the ringing is only on the order of 100 mV, but since the output of the differential amplifier is comparable, this is enough to eliminate the reading. The primary motivation for the synchronous demodulation was its succesful operation at frequencies near DC. A potentially viable alternative is an analog multiplier, which provides similar frequency-selective detection capability without the switching action. In addition, the use of a stacking board structure will be abandonded for a more conventional separate board layout, which should alleviate some of the noise problems caused by the digital chatter on the bus.

Fixed bandwidth low-pass filters may provide a simpler, easier to understand system; further low-pass filtering can be provided using the FPGA, reducing the demands on the analog hardware.

The use of the serial EEPROMs for persistent storage limits the system storage to 2M bits on the same serial bus. With the size of the FPGA used, the configuration datastream is 249,119 bits. This places the practical limit on the number of different FPGA configuration files that can be stored in the system at 8. Other non-volatile memory options such as flash memory would allow a larger number of configurations to be stored, and extend the range of supportable devices.

The control program on the PIC16F876 microcontroller relies on foreknowledge of the device interpreter's sequencing requirements for any tag to be detected: a device interpreter cannot be added to the system without modifications to the microcontroller code. If the microcontroller could reprogram not only the FPGA but itself in real time, that would solve this problem: the device interpreter would come with

both the FPGA configuration data and the microprocessor code. Alternatively, all the sequencing information could be stored in the FPGA and the microcontroller could use a standard communication protocol to talk to the FPGA, but there are a large number of possible configurations and predicting the microcontroller-FPGA communications requirements of all of them is difficult.

External control software would have to rely on foreknowledge of the possible tag readers that could be connected to the system. It would be optimal if a discovery system could be implemented to allow an unknown tag reader to communicate to a compliant control agent the commands it supports in some standardized fashion. In addition, almost all tag detection schemes use specific constant values in their algorithms: a generalized mechanism to support creation, retrieval, modification and deletion of arbitrary constants would simplify the specification of the device interpreters.

Once this platform is stable and well understood, the next logical progression would be a module that would permit this relatively low-frequency system to operate at frequency ranges such as 900 MHz or 2.45 GHz. This module could use a mixer to transform modulation generated by this system to the necessary higher frequencies to communicate with a tag that uses far-field electromagnetic propagation, essentially unifying all the RFID domains of operation.

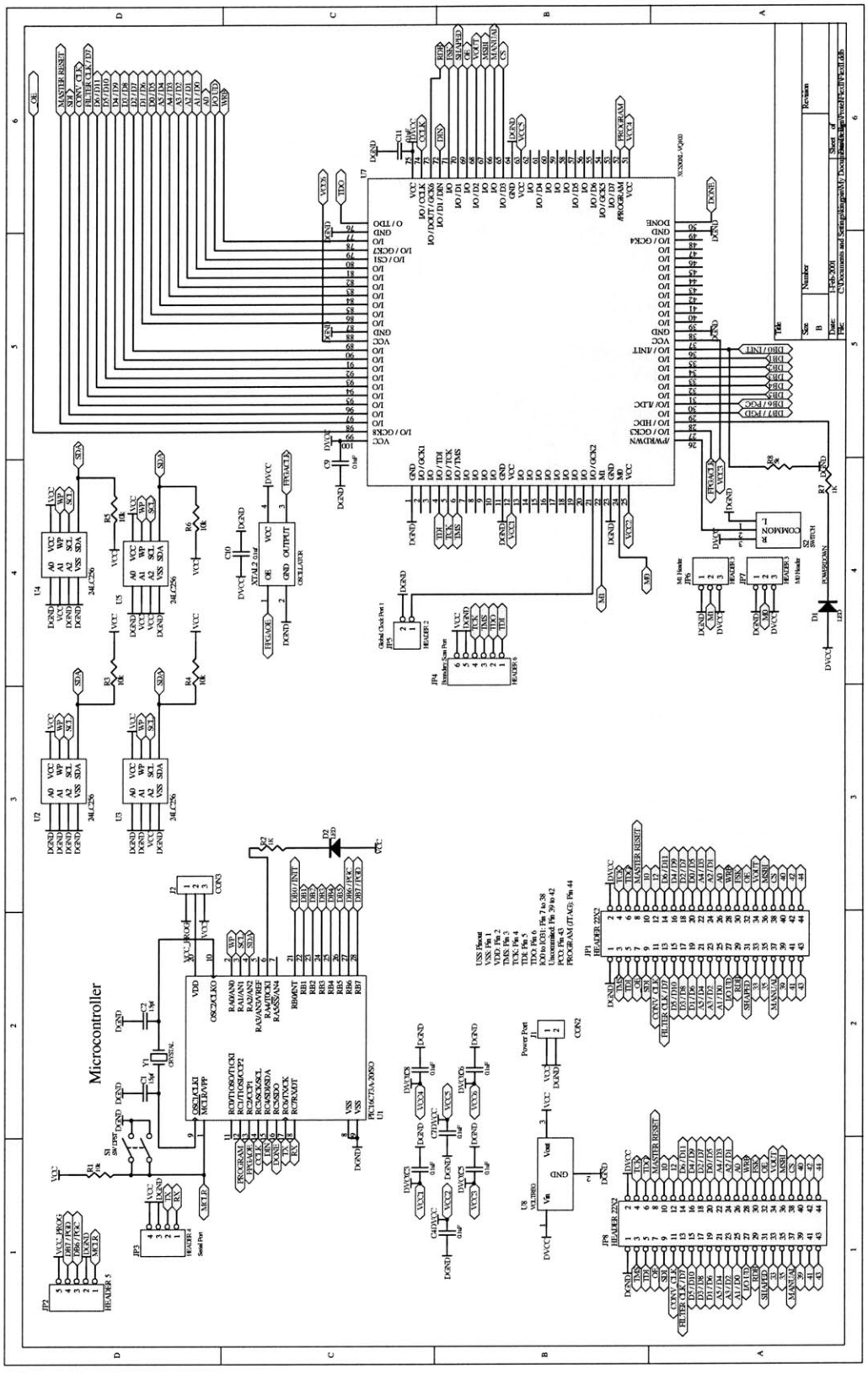
Much further out is the idea of the ultimate open architecture RF system, which would be capable of receiving arbitrary electromagnetic signals and applying arbitrary useful operations on them: the current system's capabilities would be a minimal sub set of this overall system, and this would be the ultimate replacement for every device that currently uses the electromagnetic spectrum.

Thank God I do not have to build it.

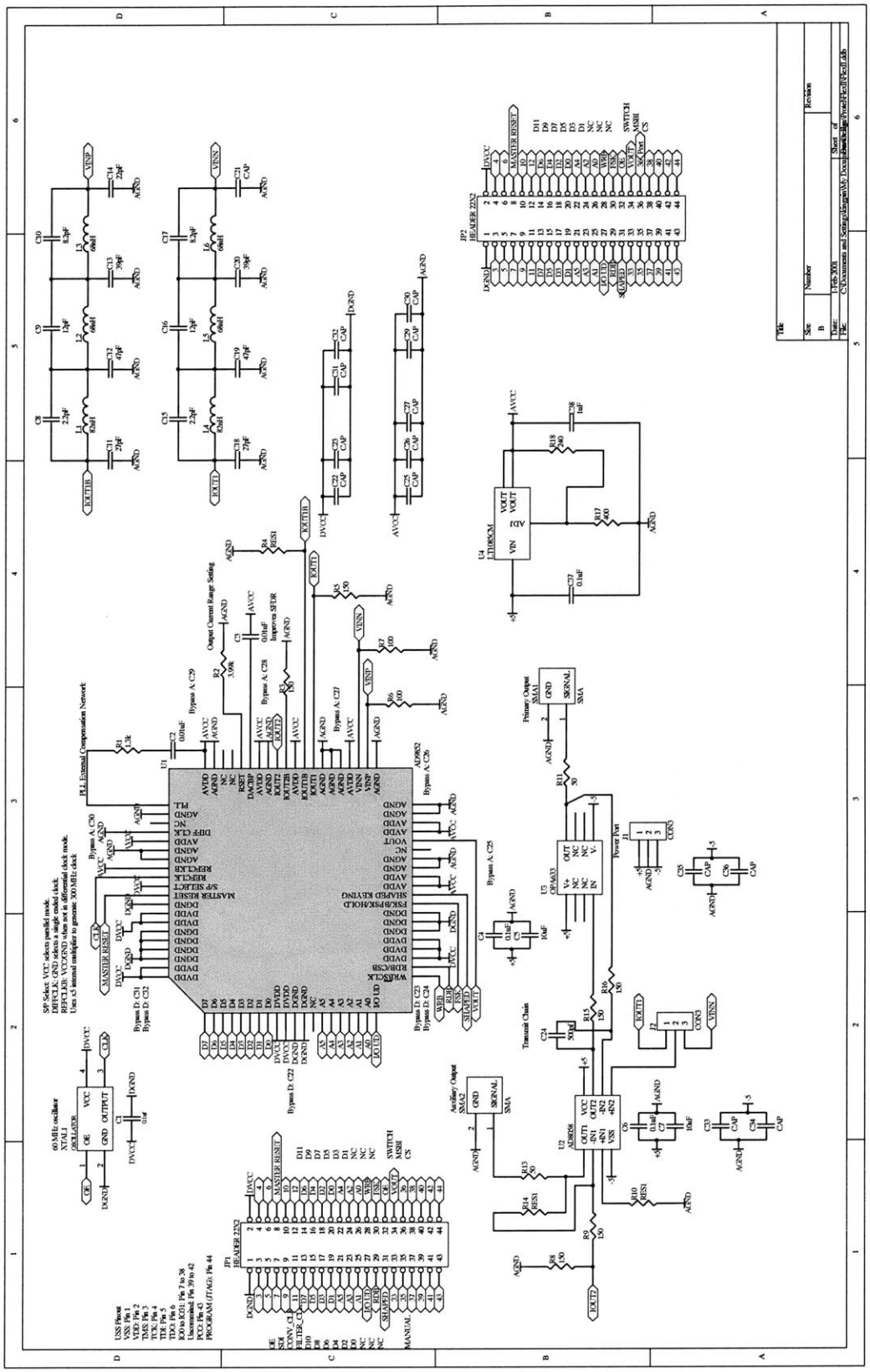
Appendix A

System Schematics

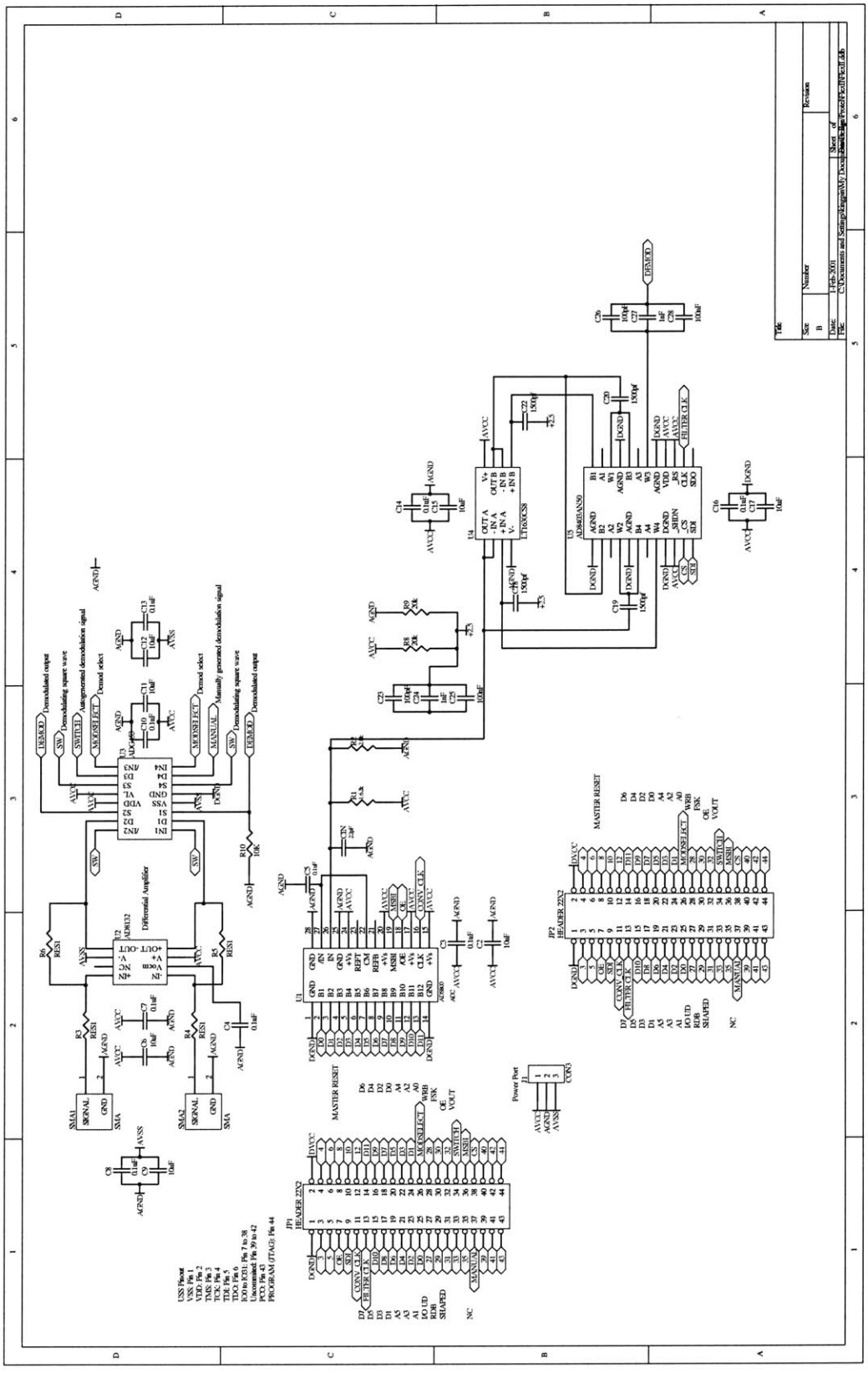
A.1 System Control Subsystem



A.2 RF Generation Subsystem



A.3 RF Detection Subsystem



Appendix B

Device Interpreter

B.1 Example Verilog for a Device Interpreter for an 8 MHz tag

```
module thesis (LED, CLK, DDS_OE, MASTER_RESET,
D, A, WRB, RDB, FSK, VOUT, MSBI,
ADC_OE, CONV_CLK) ;

input CLK ;
input VOUT ;

output LED ;
output DDS_OE ;
output MASTER_RESET ;
output WRB ;
output RDB ;
output FSK ;
output MSBI;
output ADC_OE;
output CONV_CLK;
```

```
inout [7:0] D ;
inout [5:0] A;

// add your declarations here
reg LED, WRB, RDB, FSK, DDS_OE, MASTER_RESET;
reg [5:0] address;
reg address_dir;

reg [7:0] data_bus;
reg bus_dir;

reg io_update;
reg io_ud_dir;

// output for the detector board
reg CONV_CLK, ADC_OE;

// internal counters
reg [7:0] count;

// ADC registers
reg[7:0] locount,// The number of clock periods the ADC clock is low for
hicount,  // The number of clock periods the ADC clock is high for
curcount; // The number of clock period elapsed since the ADC clock's last transit

reg [15:0] compare;
reg lastclk, sampling;

reg voutplus, voutminus;
```

```
reg vouthigh, voutlow;

// registers for detection
reg [15:0] thresh_high, thresh_low;
reg [15:0] sumlow, sumhigh;
reg [11:0] value_high, value_low;

// Using excitation for 8 MHz tag
// At REFCLK = 60 MHz
// REFCLK multiplier engaged, value 5x (00101 in control register 1E)
// Control DAC disabled (Control DAC pwrdown in control register 1D high)
// Cosine DAC enabled
// Inverse SINC bypassed (Bypass Inv Sinc in control register 20 high)
// external update clock (Int Update Clk in control register  high)
// shaped keying off/digital amplitude control off (OSK EN in control register 20
// Single tone mode (the default after a master reset)
//
// The frequency tuning word is 7.505999 * 10\^12, which is 06 D3 A0 6D 3A 06
//
// comparator is on

// this selects the direction of the data bus
assign D[0] = bus_dir ? data_bus[0] : 1'bz;
assign D[1] = bus_dir ? data_bus[1] : 1'bz;
assign D[2] = bus_dir ? data_bus[2] : 1'bz;
assign D[3] = bus_dir ? data_bus[3] : 1'bz;
assign D[4] = bus_dir ? data_bus[4] : 1'bz;
assign D[5] = bus_dir ? data_bus[5] : 1'bz;
assign D[6] = bus_dir ? data_bus[6] : 1'bz;
assign D[7] = data_bus[7];
```

```
// this sets the direction of the io update line
//assign IO_UD = io_ud_dir ? io_update : 1'bz;

//assign A[0] = (address_dir | mod_select) ? address[0] : 1'bz;
assign A[0] = address[0];
assign A[1] = address_dir ? address[1] : 1'bz;
assign A[2] = address_dir ? address[2] : 1'bz;
assign A[3] = address_dir ? address[3] : 1'bz;
assign A[4] = address_dir ? address[4] : 1'bz;
assign A[5] = address_dir ? address[5] : 1'bz;

assign MSBI = 0;

// add your code here
STARTUP U1 (.GSR(RESET)); // startup block

always @ (posedge CLK)
begin
if(RESET) begin
WRB = 1;
RDB = 1;
FSK = 0;
address[5:0] = 6'b000000;
bus_dir = 1;
address_dir = 1;
data_bus[7:0] = 8'h00;
//io_ud_dir = 0;
//io_update = 0;
MASTER_RESET = 1;
```

```
DDS_OE = 1;
count = 0;
ADC_OE = 1;
end else begin
// this does the initialization sequence
DDS_OE = 1;
RDB = 1;
FSK = 0;
count = count + 1;

// write the bytes 06 D3 A0 6D 3A 06
case(count)
8'h0E: MASTER_RESET = 0;   // end the master reset
8'h0F: address = 6'h1D;
8'h10: WRB = 0;
8'h11: data_bus = 8'b00000100; //00010100; // disable the control dac
8'h12: WRB = 1;
8'h13: address = 6'h1E;
8'h14: WRB = 0;
8'h15: data_bus = 8'h06; //8'b01000101;  // set PLL range > 200, disenable the PLI
8'h16: WRB = 1;
8'h17: address = 6'h20;
8'h18: WRB = 0;
8'h19: data_bus = 8'b01000000; // shut off shaped keying, bypass the inverse sinc
8'h1A: WRB = 1;
8'h1B: address = 6'h04;
8'h1C: WRB = 0;
8'h1D: data_bus = 8'h09; //0B; //06;
8'h1E: WRB = 1;
8'h1F: address = 6'h05;
```

```
8'h20: WRB = 0;
8'h21: data_bus = 8'h30; //60; //D3;
8'h22: WRB = 1;
8'h23: address = 6'h06;
8'h24: WRB = 0;
8'h25: data_bus = 8'h03; //B6; //A0;
8'h26: WRB = 1;
8'h27: address = 6'h07;
8'h28: WRB = 0;
8'h29: data_bus = 8'hA4; //0B; //6D;
8'h2A: WRB = 1;
8'h2B: address = 6'h08;
8'h2C: WRB = 0;
8'h2D: data_bus = 8'h11; //60; //3A;
8'h2E: WRB = 1;
  8'h2F: address = 6'h09;
  8'h30: WRB = 0;
8'h31: data_bus = 8'h4B; //B6;
8'h32: WRB = 1;
  8'h36: bus_dir = 0; // receiving on the data line
     8'h37: address_dir = 0; // receiving on the address line as well
     8'h37: ADC_OE = 0;
     8'h38: count = count - 1;
endcase
end
end

always @(posedge CLK) begin
if(RESET) begin
CONV_CLK = 0;
```

```
lastclk = 0;
voutplus = 0;
voutminus = 1;
voutlow = 0;
vouthigh=0;
thresh_high = 0;
thresh_low = 0;
sumlow = 0;
sumhigh = 0;
value_high = 0;
value_low = 0;
compare = 0;
sampling = 0;
LED = 0;

// ADC initialization
locount = 2;   // the default starting sample rate: 500 kHz = 2*10\^-6 period, = 6
hicount = 2;
curcount = 8'h00;
end else begin
if(count >= 8'h37) begin
// This is the ADC timing block
curcount = curcount + 1; // increment the adc counter

if(CONV_CLK == 1) begin
lastclk = 1;

// this is the side of the clock that is skewed long
if(curcount == locount) begin
CONV_CLK = 0;
```

```
curcount = 0;
end
end else begin
lastclk = 0;

// this is one clock cycle
if(curcount == hicount) begin
CONV_CLK = 1;
curcount = 0;
end
end

if(sampling == 1) begin
if(lastclk == 0 && CONV_CLK == 0) begin
if(VOUT == 0) begin
sumlow = sumlow + {0000,D[6:0],A[5:1]};
sampling = 0;
end else begin
sumhigh = sumhigh + {0000, D[6:0], A[5:1]};
end
end
end else begin
compare = sumhigh - sumlow;
sumlow = 0;
sumhigh = 0;
sampling = 1;
end
if(compare > 150) LED = !LED;
end
end
```

```
end


endmodule
```

Appendix C

Tag Control Interface Commands

C.1 General Commands

These commands set general tag reader properties, such as the output mode and format or the tag-operating mode, or initiate internal routines, such as self-calibration.

- Set Data Streaming Mode: this toggles the data-streaming property of the tag reader. When in data-streaming mode, the tag reader continuously outputs the results of its search for tags.
  Command Byte: ASCII 'd'; Hexadecimal 0x64.
  Command Modifiers: None.
  Command Data: None.
  Command Terminator: Not present.

- Set Polling Mode: this toggles the polling property of the tag reader. When in polling mode, the tag reader waits for a trigger signal from the external control program, then performs a single search operation, returns the results of that search, then waits for the next trigger signal.
  Command Byte: ASCII 'e'; Hexadecimal 0x65.
  Command Modifiers: None.
  Command Data: None.

Command Terminator: Not present.

- Poll Tag Reader: for a tag reader with the polling mode property set to true, this is the trigger signal that initiates a single search operation and returns the results. Otherwise, it is ignored.
  Command Byte: ASCII 'z'; Hexadecimal 0x7A.
  Command Modifiers: None.
  Command Data: None.
  Command Terminator: Not present.

- Set Onboard Output Mode: this toggles the onboard output enable property of the tag reader. For tag readers with output channels on the reader itself (such as LED/LCD displays or speakers), when in onboard output mode, these channels are enabled. Otherwise, they are disabled.
  Command Byte: ASCII 'o'; Hexadecimal 0x6F.
  Command Modifiers: None.
  Command Data: None.
  Command Terminator: Not present.

- Set Output Data Format: this command switches between multiple output formats. For tag readers that support multiple formats, the command modifiers are used to signify which mode.
  Command Byte: ASCII 'h'; Hexadecimal 0x68.
  Command Modifiers: An optional ASCII representation of a number, starting at 0. When not present, changes output format to default. When present, is tag-reader dependent.
  Command Data: None.
  Command Terminator: Present.

- Set Power Saving Mode: this command toggles the power saving mode of the tag reader. For suitably equipped tag readers, in power saving mode the signal output chain is disabled.
  Command Byte: ASCII 'v'; Hexadecimal 0x76.
  Command Modifiers: None.
  Command Data: None.
  Command Terminator: Not present.

- Pause Tag Reader: this command toggles the active state of the tag reader. When paused, the tag reader skips all software functions related to tag reading. It may or may not power down the tag reading signal chain. It however responds to external commands, and does not output any data.
  Command Byte: ASCII 'x'; Hexadecimal 0x78.
  Command Modifiers: None.
  Command Data: None.
  Command Terminator: Not present.

- Set Tag Reader Controller Mode: this command toggles the controller state of the tag reader. The tag reader may be in human control mode, for control by a human operator, or in machine control mode, for control by a software program. These states are as described in Section 2 above.
  Command Byte: ASCII 'M'; Hexadecimal 0x4D.
  Command Modifiers: None.
  Command Data: None.
  Command Terminator: Not present.

- Switch to Machine Control Mode and Pause: this command was added to allow software controllers that are connecting to a tag reader place it in a deterministic state. Upon receiving this command, the tag reader pauses and places itself

in machine control mode, then awaits further instructions.

Command Byte: ASCII 'P'; Hexadecimal 0x50.

Command Modifiers: None.

Command Data: None.

Command Terminator: Not present.

- Set Identifier String: this sets the identifier kept by each tag reader. The identifier may or may not persist through power cycles, and is at least 32-bits long. This identifier may be assigned by a control program to enable it distinguish between multiple tag readers that may share the same data channel.

  Command Byte: ASCII 'u'; Hexadecimal 0x75.

  Command Modifiers: None.

  Command Data: 4 or more bytes, depending on the size of the identifier space within the reader. The reader will either truncate the data to fit the available space, or zero pad the data if the space is more than the available space. The value sent is literal data (i.e. not an ASCII representation, but the actual numeric value. No translation is done).

  Command Terminator: Present.

- Get Identifier String: this retrieves the current value stored in the identifier space of the tag reader.

  Command Byte: ASCII 'n'; Hexadecimal 0x6E.

  Command Modifiers: None.

  Command Data: None.

  Command Terminator: Not present.

- Initiate Internal Calibration Routines: this runs any internal calibration routines the tag reader has. It may or may not result in an interactive prompt.

  Command Byte: ASCII 'p'; Hexadecimal 0x70.

Command Modifiers: Optional (tag reader dependent).

Command Data: None.

Command Terminator: Present.

- Enable Internal Post-Processing Routines: this toggles the internal post-processing property of the tag reader. On some tag readers, there will be the capability to run some internal processing routines on the raw data obtained from the antenna measurements before output. This may or may not modify the format of the output data.

  Command Byte: ASCII 'q'; Hexadecimal 0x71.

  Command Modifiers: Optional (tag reader dependent).

  Command Data: Optional (tag reader dependent).

  Command Terminator: Present.

- Get Internal Post-Processing Data: this streams out the current state associated with the tag reader's internal post-processing routines through the main communications/control channel in a tag reader dependent format.

  Command Byte: ASCII 'r'; Hexadecimal 0x72.

  Command Modifiers: None.

  Command Data: None.

  Command Terminator: Not present.

- Adjust Internal Post-Processing Data: this initiates the internal routines to adjust the data associated with the internal post processing routines. This is typically a series of interactive prompts for information.

  Command Byte: ASCII 'S'; Hexadecimal 0x53.

  Command Modifiers: None.

  Command Data: None.

  Command Terminator: Not present.

- Get Tag Reader State: this streams out the current state of the tag reader's properties through the main communications/control channel in a tag reader dependent format.
  Command Byte: ASCII 's'; Hexadecimal 0x73.
  Command Modifiers: None.
  Command Data: None.
  Command Terminator: Not present.

- Adjust Internal Thresholds: this adjusts the internal threshold variables on the tag reader. The effect is tag reader dependent.
  Command Byte: ASCII 't'; Hexadecimal 0x74.
  Command Modifiers: None.
  Command Data: At least one argument, each argument an ASCII representation of a base 10 number, with each argument separated by ASCII ';' (hexadecimal 0x3B). The order and significance of the arguments are tag reader dependent.
  Command Terminator: Present.

- Set Target Tag Mode: this command selects the target tag to search for (for example, a tag reader may be capable of searching for both silicon RFID tags and magnetic EAS tags).
  Command Byte: ASCII 'm'; Hexadecimal 0x6D.
  Command Modifiers: An ASCII representation of a number greater than or equal to zero. Currently assigned values are:
  0 - Resonant mode tags (such as magnetic EAS tags).
  1 - Harmonic mode tags (such as magnetic domain wall tags).
  Other values may be assigned in a tag reader dependent fashion.
  Command Data: None.

Command Terminator: Not present.

- Reset All Constants to Default: this command resets all internal constants to their value immediately after a power-on reset. It may or may not implement a remote hardware reset.
  Command Byte: ASCII 'y'; Hexadecimal 0x79.
  Command Modifiers: None.
  Command Data: None.
  Command Terminator: Not present.

- Discover Current Output Format: this command returns a byte sequence that details the default output format for the system. The sequence is at least 4 bytes long, and increases in multiples of 2. The first byte in the sequence is the size of the entire sequence (including the size byte). The second byte is the number of data values returned by the tag reader for each frequency point. For each of the values that may be returned there is a 2-byte number that indicates the data value's size, MSB first. The sizes are listed in the order that the data values will be returned.
  Command Byte: ASCII 'D'; Hexadecimal 0x44.
  Command Modifiers: None.
  Command Data: None.
  Command Terminator: Not present.

C.2 Scanning Commands

These commands are those that set whether or not the tag reader does a frequency scan and set the related frequency parameters.

- Set Scanning Mode: this toggles the scanning property of the tag reader. When

in scanning mode, the tag reader performs a search for tags between the current scan start and stop frequencies, in frequency intervals set by the scan step frequency. Otherwise the tag reader searches for a tag at a single frequency.
Command Byte: ASCII 'w'; Hexadecimal 0x77.
Command Modifiers: None.
Command Data: None.
Command Terminator: Not present.

- Restart Frequency Scan: if a scan is in progress, this command restarts the scan from the current scan start frequency. Otherwise, it is ignored.
  Command Byte: ASCII 'g'; Hexadecimal 0x67.
  Command Modifiers: None.
  Command Data: None.
  Command Terminator: Not present.

- Set Start Frequency: this sets the frequency at which the scan starts.
  Command Byte: ASCII 'a'; Hexadecimal 0x61.
  Command Modifiers: None.
  Command Data: An ASCII representation of the frequency value to start the scan at. The number must be greater than 0. The tag reader determines the range of allowable values.
  Command Terminator: Present.

- Set Stop Frequency: this sets the frequency at which the scan stops.
  Command Byte: ASCII 'b'; Hexadecimal 0x62.
  Command Modifiers: None.
  Command Data: An ASCII representation of the frequency value to start the scan at. The number must be greater than 0. The tag reader determines the range of allowable values.

Command Terminator: Present.

- Set Step Frequency: this sets the frequency difference between each point in the scan.
  Command Byte: ASCII 'c'; Hexadecimal 0x63.
  Command Modifiers: None.
  Command Data: An ASCII representation of the value of the difference between each frequency point in the scan. The number must be greater than 0. The tag reader determines the range of allowable values.
  Command Terminator: Present.

- Set Single Frequency: this sets the frequency at which the tag reader searches for tags when not in scanning mode.
  Command Byte: ASCII 'f'; Hexadecimal 0x66.
  Command Modifiers: None.
  Command Data: An ASCII representation of the frequency value at which the tag reader performs the search for a tag. The number must be greater than 0. The tag reader determines the range of allowable values.
  Command Terminator: Present.

- Set Harmonic Base Frequency: this sets the base frequency at which the tag reader transmits (for tag readers with harmonic detection capabilities, where the tag reader transmits at a certain base frequency and searches for harmonics of that frequency in the response of the tag).
  Command Byte: ASCII 'B'; Hexadecimal 0x42.
  Command Modifiers: None.
  Command Data: An ASCII representation of the frequency value at which the tag reader transmits when in harmonic mode. The number must be greater than 0. The tag reader determines the range of allowable values.

Command Terminator: Present.

C.3 Legacy Commands

These commands are included to deal with current implementations of the interface. They will be eliminated as soon as an appropriate format can be implemented to support an arbitrary number of constants for special purposes.

- Set Transmit Pulse Period: when implemented, this allows the modification of the length of time of the radio frequency pulse the tag reader transmits while performing a search. The length is a multiple of 10ms.
  Command Byte: ASCII 'j'; Hexadecimal 0x6A.
  Command Modifiers: None.
  Command Data: An ASCII representation of the length of time (in multiples of 10ms) that the tag reader should transmit for. The number must be greater than 0. The tag reader determines the range of allowable values.
  Command Terminator: Present.

- Set Transient Delay Period: when implemented, this allows the modification of the length of time after the end of the transmit pulse that the tag reader waits for either transient energy in the transmit coil to subside, or the frequency generator to stabilize. This delay is of use when the same antenna is used for the RF transmission and tag response detection.
  Command Byte: ASCII 'k'; Hexadecimal 0x6B.
  Command Modifiers: None.
  Command Data: An ASCII representation of the length of time (in multiples of 10ms) that the tag reader should wait after the end of the transmit pulse before measuring the response from the tag. The number must be greater than 0. The tag reader determines the range of allowable values.

Command Terminator: Present.

- Set Measurement Period: when implemented, this allows the modification of the length of time that the measurement of the tag response is taken. This delay is of use when a time-dependent measurement technique is in use (such as an integrator).

  Command Byte: ASCII 'l'; Hexadecimal 0x6C.

  Command Modifiers: None.

  Command Data: An ASCII representation of the length of time (in multiples of 10ms) that the tag reader should take the measurement. The number must be greater than 0. The tag reader determines the range of allowable values.

  Command Terminator: Present.

Bibliography

[1] Philips Semiconductor. *ICODE1 Label ICs Protocol Air Interface*, 1999.

[2] www.infotec.org/history.htm. *Infotec*, 1999.

[3] Richard Fletcher, Jeremy Levitan, Joel Rosenberg, and Neil Gershenfeld. Application of Smart Materials to Wireless ID Tags and Remote Sensors. *Proceedings of the Materials Research Society Fall Meeting*, 1996.

[4] Richard Fletcher. Force Transduction Materials for Human-Technology Interfaces. *IBM Systems Journal*, 35(3):630 – 639, July 1996.

[5] Theodore Van Duzer Simon Ramo, John R. Winnery. *Fields and Waves in Communications Electronics*, chapter 2, pages 68–106. John Wiley & Sons, second edition, 1984.

[6] International Standards Organization/International Electrotechnical Commission. *Identification cards - Contactless integrated circuit(s) cards - Vicinity cards - Air interface and initialization*, first edition, 2000.

[7] Constantine I. Balanis. *Antenna Theory: Analysis and Design.* John Wiley & Sons, 1996.

[8] Federal Communications Commission Office of Science and Technology. *FCC methods of measurements of radio noise emissions from industrial, scientific and medical equipment*, 1986.

[9] Richard Fletcher, Olufemi Omojola, Edward Boyden III, and Neil Gershenfeld. Reconfigurable Agile Tag Reader

Technologies for Combined EAS and RFID Capability. *Proceedings of the 2nd IEEE Workshop on Automatic Identification Advanced Technologies*, 1(1), September 1999.

[10] Olufemi Omojola et al. An installation of interactive furniture. *IBM Systems Journal*, 39(3 & 4), 2000.