Multi-Disciplinary Engineering Design Conference
Kate Gleason College of Engineering
Rochester Institute of Technology
Rochester, New York 14623

Project Number: 06509

RADIO FREQUENCY IDENTIFICATION (RFID) GARAGE DOOR ENTRY SYSTEM

Kenneth Williams (EEEE)
Thomas Cervino (EEEE)
Michael Cummins (EEEC)
Michael Flannery (EEEC)

Abstract - The RFID Garage Door Entry System team is a project team which seeks to create an automation solution using a relatively un-harnessed technology called Radio Frequency Identification (RFID). Using RFID technology, the team seeks to combine the functionality and convenience of automated remote transmission with an existing garage door opener system. The intent of this project was to build a system that allowed a garage door to open wirelessly with no interaction from the user.

Index Terms – Radio Frequency Identification (RFID), Reader, Tag, Security

I. INTRODUCTION

The RFID Garage Door Entry System team created a product which will automate the operation of a typical garage door using RFID technology. With the technology used in garage door control, a simple idea is explored: How to make a garage door open automatically upon arrival, without the push of a button. The RFID garage door opener system will consist of two major components: a reader and a tag both of which will communicate wirelessly with each other. The stationary reader will be located in the garage and will initiate all communication sequences. When a tag is in range it will then respond to the reader. The tag will validate the reader, and the reader will validate the tag. The tag will be located within the car but will not be physically embedded. This is to allow versatility of the product, such as switching a tag between automobiles, and also due to the goal of this product to be easily installable. The desire to utilize a new technology in a familiar situation is a motivating factor for this project. RFID is a relatively untapped technology that has perfect applications in secure home automation. A few of the product requirements include the following:

1) The system shall have a range of no less than 30 feet
2) The system shall be able to store at least one tag in internal memory
3) The system shall not interfere with the existing garage door apparatus
4) The system shall utilize a standard 120V (Single Phase) residential connection for power purposes

II. NOMENCLATURE

ASK – Amplitude Shift Keying
Carry Current – The maximum allowed current through the common pole of the relay
FSK – Frequency Shift Keying
IC – Integrated Circuit
LED – Light Emitting Diode
mAh – milliamp hours (unit of power)
MHz – Megahertz
RAM – Random Access Memory
Reader – the stationary device (located in the garage)
RFID – Radio Frequency Identification
Security Function – A series of operations performed on the Security Key to obtain the Security Password
Security Key – A pseudo random number used to generate a Security Password
Security Password – Generated based on the Security Key and a predefined algorithm
Tag – the mobile device (located in the car)
λ – Wavelength (m)
c – Speed of light ($3.0*10^8$ m/sec)
Te – one clock period

III. DESIGN

A. GARAGE DOOR INTERFACE

Typical garage door systems are controlled in several ways. The push button on the wall is the primary means of opening and closing the door. The control from either an

© 2005 Rochester Institute of Technology

external keypad or push button remote serves the same purpose only wirelessly. This project seeks to reduce the amount of user feedback into the system through the use of RFID and will interface with the existing system through the wired pushbutton. This will allow the RFID system to interface with the existing system seamlessly. RFID will provide a secure wireless method of controlling the garage door. As per product requirements the RFID garage door opener must appear transparent to all existing control systems.

The first step in integrating the RFID system requires relocation of wires. The push button wall controls are typically two-wire active-low devices which source and sink on the garage door opener. The push button on the wall is a momentary switch which closes the connection. A sample diagram is shown in Fig. 1.

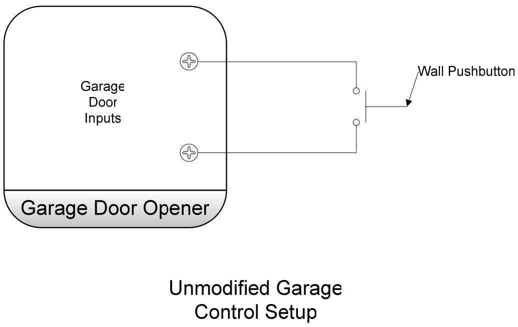

Figure 1 – Existing Garage Door Control

As a non-intrusive way of interfacing with the push button, these wires will be lifted from the door opener during installation and re-terminated to the reader, which will provide two input connections for the wires. Within the reader these connections will allow for a signal to be sent to the PIC16F676 as well as the existing garage door opener. The common pole on the relay will be connected to one of the now empty terminals on the garage door opener. The relay's normally open throw will be connected to the other empty terminal. The PIC16F676 is programmed as a state machine. Upon seeing that the button has been depressed it will act accordingly and register the change in the condition of the garage door. This pin will be connected to the base of an NPN bipolar-junction transistor, and when it receives an active signal (+3 to 5VDC) it will drive the coil of the relay. A detailed schematic of this operation is given in Fig. 2.

The relay was necessary in the design to imitate the pushbutton that was originally in the garage door setup. The push button, as stated earlier, acts as a momentary switch; the relay will be an electromechanical version of the pushbutton. When the pushbutton is depressed, the microcontroller will record the state of the garage door and since the push button is pulled high to interrupt the microcontroller, its 5V signal will drive the transistor into saturation.

Figure 2 has been slightly modified to allow for an input to the BJT of as low as 3V. Using a 10kΩ resistor instead of the larger one in our original design allows more current to flow through the Base of the BJT at 3V. The coil in the relay needs approximately 30mA flowing through it for it to throw the switch therefore the collector current in our BJT driven relay must be around 30mA.

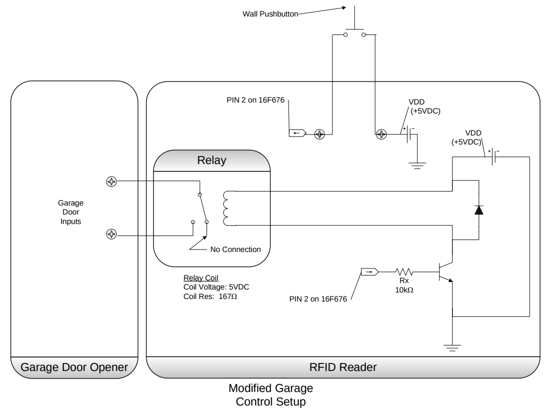

Figure 2 – Modified Garage Control

A decision was made to use a NPN bipolar junction transistor. At the desired IC (30mA), the chosen transistor has the parameters VBE=0.7V, β=205. Using simple current equations, a rated coil resistance of 167Ω, and the BJT current law in Equation 1, it was determined that IB would be equal to 146.3μA.

$$I_C = \beta * I_B \qquad (1)$$

I_C: collector current
I_B: base current
β: current gain

Since the turn on voltage of the transistor is 0.7V, and the active signal is connected to pin 2 on the 16F676, which has a minimum bias of 3VDC, the resistor must drop 2.3V to produce a current of 146.3μA. Using Ohm's Law, it was determined that the required resistance Rx to be a maximum of 10kΩ. The BJT will accept voltages of 3 or higher to throw the switch in the relay with this design.

The relay that is used in this circuit is an OMRON G5V-1 low signal relay and it was chosen due to its small size and very low voltage and current requirements. The relay needs 5V supplied to it for it to operate and its carry current (the max allowable current is 2A. Another important aspect of this relay is that its maximum switching time is 5ms; this effectively is no delay from when the signal from the microcontroller is sent to when it switches the pole on the relay.

B. HARDWARE

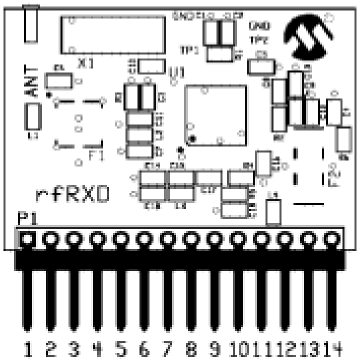

Figure 3 – Receiver Module

Pin	Description
1-10	No Connection
11	Receive Data In
12	No Connection
13	Power: 2.5-5.5 VDC
14	Ground
ANT	Antenna Connection

Table 1 – Receiver Module Pin Assignment

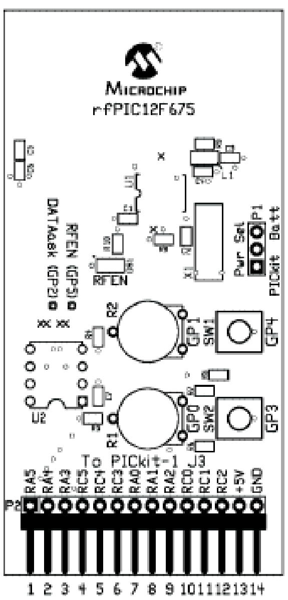

Figure 4 – Transmitter Module

Pin	Description
1	GP5
2	GP4
3	GP3
4, 5, 6	No Connection
7	GP0
8	GP1
9	GP2
10, 11, 12	No Connection
13	Power: 2.0-5.5 VDC
14	Ground

Table 2 – Transmitter Module Pin Assignment

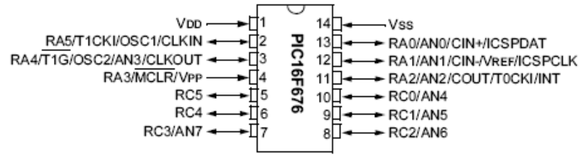

Figure 5 – 16F676 Pin Assignment

The initial design called for the use of a Microchip transmitter module based off of the PIC12F675F (Figure 4) chip and a receiver module based off of the rfRXD0420 (Figure 3). This design used the PIC12F675 for the entire program. In order to accommodate the complexity of the software design, a third chip was introduced, the PIC16F676 (Figure 5). The PIC16F676 acts as the control center for the system, controlling when transmission occurs and dealing with all inputs to the system Additionally several LED's and pushbuttons were added to the layout to facilitate a more friendly user interface. Figure 13 shows the PCB layout which gives the interaction between the hardware components (Tables 1, 2 and Figure 5 show the pin assignments for the three major devices). A NAND gate is required between the 16F676 and the transmitter module due to the transmitter module requiring an active low signal to initiate a transmission. However, when in production, this could be removed after modification to the transmitter module layout.

C. COMMUNICATIONS

The original design called for a communications protocol that consisted of a form of handshaking. During the course of building the prototype it became apparent that this was not optimal. A slightly modified version of this was implemented. The new protocol still utilized a Security Key, Security Password and a predefined Security Function. The new communication sequence is as follows:

1) The *reader* periodically sends out a signal that includes the *Reader ID*.
2) The *tag* receives a signal and checks the *Reader ID* value received with that in memory.
3) Upon a match the tag then transmits the *Tag ID*, *Security Key* and *Security Password*
4) The *reader* receives the *Security Key*, *Security Password* and *Tag ID*.
5) The *reader* first checks for a valid *Tag ID*. If the ID is valid it continues the verification process.
6) The *reader* then takes the *Security Key* and generates a local copy of the *Security Password*.
7) The *reader* compares the two *Security Passwords*, if a match occurs then a valid *tag* has been found. It then signals the garage door to open and temporarily disables polling.

Copyright © 2005 by Rochester Institute of Technology

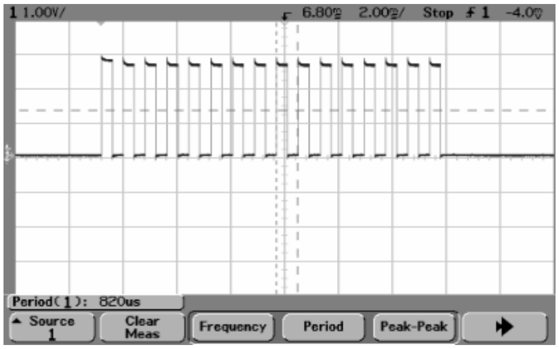

Figure 6 – The Preamble

The transmission consists of a 72 bit data stream, a Preamble, a Header and a Guard Time. The Preamble is a series of 16 pulses that initiates the stream. (*See Fig.6 above*) The Header is then checked to see a high pulse before 6 ms. The Guard Time indicates the end of the transmission and is held low for 8 ms. The transmission structure (Figure 7) consists of the Preamble, followed by the Header, then the data stream followed by the guard time. During the development of the communication protocol an error occurred when trying to record the 72 bits of the data stream received. Due to this, the last 8 bits are ignored.

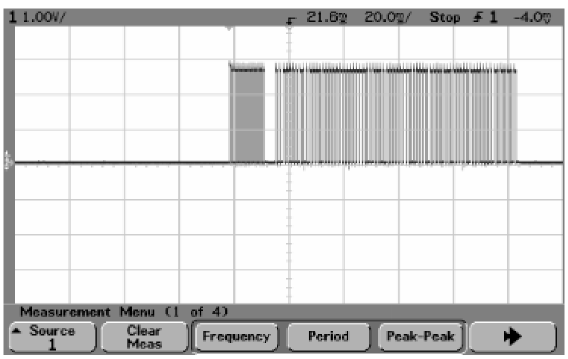

Figure 7 – Full Data Transmission

In order to transmit all the values a form of encoding is necessary. For this application the following encoding was used. Every data bit occurs over a period of *3Te*. If a value of 0 is to be transmitted the signal is held high for the first *2Te* and low for the final *Te*. For a value of 1 the signal is high for the first *Te* and low for the last *2Te*.

Currently the data stream is broken down as follows. The first 8 bits of the stream are a generic serial number. For a market product this could be equivalent to the model number. This would be helpful to ensure compatibility between tags and readers and also as the first from of security. Since the system has the capability to LEARN the ID's of the reader and the tag, it is necessary to differentiate between an actual transmission and the setup transmissions. This is accomplished with another 8 bits of the data stream. For the reader it transmits a 32 bit ID. For the tag the 32bits is split up to a 16 bit ID, an 8 bit Security Password and 8 bit Security Key. Finally there are 24 bits of junk data and data that is ignored. It is possible that this data may be used to increase the security encoding or tag ID value. However, at this time the junk data in itself is seen as a security feature because it is not published as to where this invalid data occurs. Some of this data is static (the same in every transmission) and some of the data alters from transmission to transmission. At this time it is believed that this may help to make the system more secure.

D. SOFTWARE

The software to operate the system was written using assembly and file templates provided in the Microchip Development kit. The first stage of the design process focused around achieving transmission between the receiver and transmitter module. Since both the reader and the tag contain a transmitter and receiver module 4 main program files were necessary. The transmitter module program in the reader must communicate with the reader module program in the tag and so forth. The initial stage also provided a single output to signify that the receiver had received a signal. The basic concepts for the software flow may be seen in the Software Flow diagrams in Figures 8, 9 and 10.

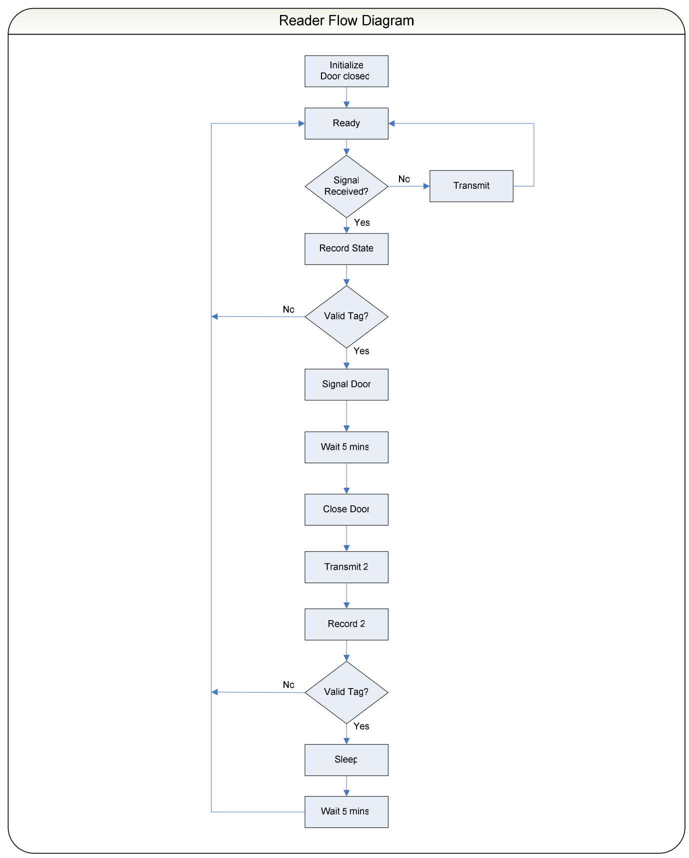

Figure 8 - Reader Flow Diagram

The next stage of software development focused around securing the transmissions. This required coding the signals to follow the procedure outlined in section C. COMMUNICATIONS. The validation coding was simply written through the use of an XOR command and a conditional branch. It also required a subroutine to read the EPROM data.

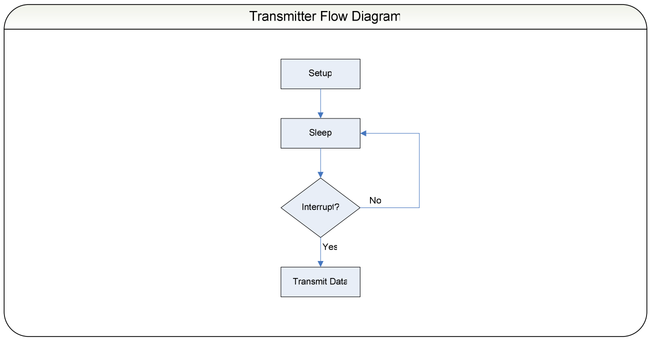

Figure 9 - Transmitter Module Flow Diagram

The final stage of the software development centered on the I/O controls. The interaction between the two modules, the 16F676 is fairly simple but requires multiple connections. This phase of the design also required consideration of the PCB layout. For the interaction with the garage door system, a simple solution was found. Unless the 16F676 is sending a signal to the garage door, the output pin controlling the garage door will act as an input. This will allow the garage door pushbutton to always work. The only time this pin will act as an output is when the system is actually attempting to signal the garage door. The drawback to this solution is that it requires rewriting the I/O register which decreases the response time. However, for this application it will not noticeably impact the system

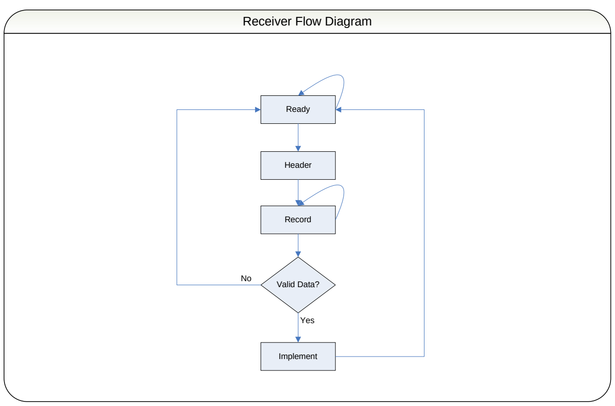

Figure 10 - Receiver Module Flow Diagram

An additional feature was then added which would allow for the end user to manually program the reader and tag. In order to accomplish this, two momentary pushbuttons were added to each device. One pushbutton was attached to an input for the 16F676 and one pushbutton was attached to the transmitter module. When the pushbutton attached to the transmitter module forces a transmission to occur. When the pushbutton attached to the 16F676 is activated it causes the device to go into a LEARN mode where it records the ID of the signal it receives. This slightly complicated the coding, requiring the forced transmission to be discernable from a normal transmission.

IV. TESTING

To test the functionality of the system it was built on a breadboard with all the components hardwired together (Figure 12). This setup allowed the system to be tested for its ability to learn the transmitter ID's and distinguish between the two RF transmissions from the tag. Within the laboratory a range of approximately 75ft was achieved, which exceeds the required range for the system. One should note that this range was achieved inside a building with more interference than one would have in a standard garage. This range will almost certainly increase when moved to a garage setting.

After completing the testing of the system a layout was designed and sent for manufacturing (Figure 11). This allows for a more finished product.

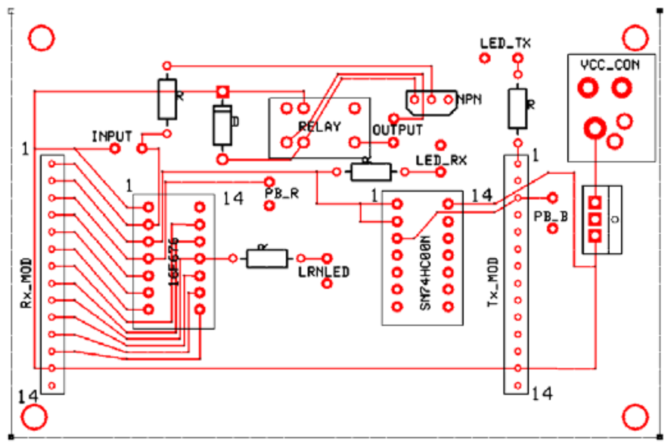

Figure 11 - PCB Layout

Another change that was made to the original design was the addition of a voltage regulator. The original design uses a 5VDC transformer that only drops to 5V when there is a current draw of at least 500mA. The reader never reaches a 500mA current draw so the transformer was outputting approximately 9V instead of 5V. This phenomenon required the use of a 5V DC voltage regulator. The regulator being used is the LM340T5 and it is able to handle loads up to 1A. This is well over what is needed in the reader.

Copyright © 2005 by Rochester Institute of Technology

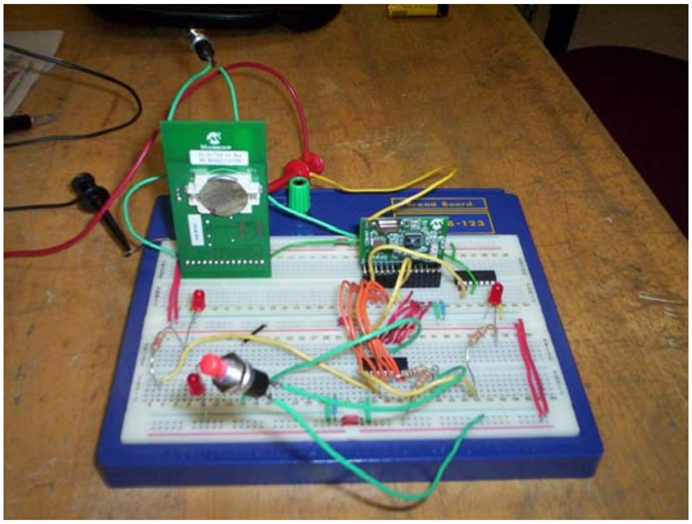

Figure 12 - Test Setup

It was also necessary to test the estimated battery life. In order to due this the current draw was measured under several different conditions. Table 3 shows the current draw of each device. By utilizing Equation 2 it was found that this resulted in a 76,546 mAh power consumption for 1 year of operation. The batteries for the tag supply 6600 mAh (2200 mAh per AA battery). This clearly does not meet the 1 year desired outcome. This can be attributed to several factors that were not initially foreseen. One of the main factors is the mode of operation for the receiver IC chip. This is due to a limitation in the receiver module design. This issue would be solved in one of two manners. On way would be to provide a method of recharging the batteries. A simpler way is to expose the AA battery insert to allow the batteries to be changed out. Based on the current draw seen, the batteries would need to be replaced approximately every month. This option would also require the addition of a low power indicating LED.

	Idle	Transmission
16F676	1.1 mA	2 mA
Rx Module	7.1 mA	7.61 mA
Tx Module	.54 mA	8 mA

Table 3 – Current Draw by Device

$$t_{idle} * (\frac{1}{60}) * I_{idle} + t_{Tx} * (\frac{1}{60}) * I_{Tx} = P(mAh) \quad (2)$$

t_{idle} = 109 minutes
t_{Tx} = 525491 minutes
I_{idle} = 8.74 mA
I_{Tx} = 17.61 mA
P=76546 mAh

The most intensive and crucial testing was to test the security and communications protocol. In order to test the system three different tags were needed. Due to monetary concerns, the prototype tag was built to allow the programming to be updated in order to simulate three different tags at different times. The three tags that were to be simulated were broken down into two categories, a valid tag and two invalid tags. To test the systems functionality an indicator was connected to the reader instead of the garage door system. Upon the reader communicating with a valid tag, the indicator LED becomes active.

The first of the two invalid tags utilized the same tag id as the valid tag. However, instead of a valid Security Password and Security Key, pseudo random values were transmitted. This ensures that the system does not just test the tag id. The second invalid tag utilized the valid security protocol, but was an invalid id code. By utilizing these three tags it is possible to test the functionality of the communication protocol and security implementation. However, this does not test how vulnerable the system would be to intrusion.

V. CONCLUSION

The main goal of this project was to create an RFID system and apply it to an application of opening a garage door. The final results show the successful design of an RFID system with a working interface to the garage door system. The prototype provides for basic operation however, before becoming a market product there are several things that should be implemented. The devices used allow for a crude type of distance sensing based upon signal strength. In order to determine when to close the garage door could be modified to be based off of distance rather then a time period.

Also, modifying the code to allow for multiple tags, and an interface (USB) that would allow for the user to add or remove tags. The battery consumption may have been further reduced by further modifying layout of the rfRXD0420 module. This part failed to meet the specified 100 nA standby current draw because the module does not allow for the chip to be placed in standby mode. If the device were able to be placed into standby, a battery life of greater than 1 year would be achieved. On a final note, if the tag enclosure were to be modified, in order to allow it to be rechargeable by being placed in a cradle would be of great benefit to this project. For a prototype the overall product meets the general requirements set forth at the onset of the project.

ACKNOWLEDGEMENTS

The RFID team would lack to thank the Professor Slack for his time and energies in heading up the Senior Design course. Additionally a most sincere thank you to Professor Phillips, who helped impart both technical knowledge as well as professional knowledge upon all of his students.

REFERENCES

[1] “rfPIC12F675K/675F/675H 20-Pin FLASH Based 8-Bit CMOS Microcontroller with UHF ASK/FSK Transmitter”, Microchip Datasheet [Online], http://ww1.microchip.com/downloads/en/DeviceDoc/70091a.pdf

[2] “PIC17F630/676 14-Pin FLASH Based 8-Bit CMOS Microcontroller”, Microchip Datasheet [Online],

http://ww1.microchip.com/downloads/en/DeviceDoc/41191D.p
df
[3] “rfRXD0420/0920 UHF ASK/FSK/FM Receiver”, Microchip Datasheet [Online], http://ww1.microchip.com/downloads/en/DeviceDoc/70090a.pdf
[4] “MC7800, MC7800A, LM340, LM340A Three-Terminal Positive Voltage Regulators,” Motorola Datasheet [Online], http://pdf1.alldatasheet.com/datasheet-pdf/view/4447/MOTOROLA/MC7800.html
[5] “SN54HC00, SN74HC00 Quadruple 2-Input Positive NAND Gates,” Texas Instruments Datasheet [Online], http://pdf1.alldatasheet.com/datasheet-pdf/view/27870/TI/SN54HC00.html
[6] “G5V-1 Low Signal Relay,” Omron Datasheet [Online], http://oeiwcs.omron.com/webapp/commerce/command/ProductDisplay?prrfnbr=550&prmenbr=316

Copyright © 2005 by Rochester Institute of Technology