

**RADIO FREQUENCY IDENTIFICATION OF PERSONNEL IN PLANT  
DURING EMERGENCY CONDITIONS**

By

**MUHAMMAD FARID BIN MD DAUD**

**FINAL PROJECT REPORT**

Submitted to the Electrical & Electronics Engineering Programme  
in Partial Fulfillment of the Requirements  
for the Degree  
Bachelor of Engineering (Hons)  
(Electrical & Electronics Engineering)

JUNE 2007

**CERTIFICATION OF APPROVAL**

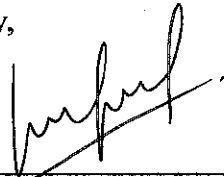
**Radio Frequency Identification of Personnel  
in Plant during Emergency Condition**

by

**Muhammad Farid Bin Md Daud**

A project dissertation submitted to the  
Electrical & Electronics Engineering Programme  
Universiti Teknologi PETRONAS  
in partial fulfilment of the requirement for the  
**BACHELOR OF ENGINEERING (Hons)**  
**(ELECTRICAL & ELECTRONICS ENGINEERING)**

Approved by,



**(DR. MOHAMAD NAUFAL B. MOHAMAD SAAD)**

**UNIVERSITI TEKNOLOGI PETRONAS**

**TRONOH, PERAK**

**June 2007**

## **CERTIFICATION OF ORIGINALITY**

This is to certify that I am responsible for the work submitted in this project, that the original work is my own except as specified in the references and acknowledgements, and that the original work contained herein have not been undertaken or done by unspecified sources or persons.

  
\_\_\_\_\_  
MUHAMMAD FARID BIN MD DAUD

## **ABSTRACT**

Nowadays, nearly every industrial plant throughout the nation are taking concern on the emerging safety issues that is seemed to be more apparent – compared to just taking serious attention to the production line. It's been said that if you think safety is expensive, try an accident. Safety of each personnel is deeply linked on the psychological part that contributes to the well being of an industrial plant and therefore the workers are part of the valuable assets to the company. Parallel to the development of industrial competency and complexity, the safety issues have becoming more technologically related. RFID (Radio Frequency Identification), already known for its agility and reliability in supply chain management, has now being diverging in areas regarding safety. RFID is not just a label that tags for certain equipments / goods, but now able to detect location of moving object, especially human, in an enclosed area. From simulation up to practical application, RFID had shown significant improvement for a faster and precise detection of personnel compared to other traditional barcode detection or manual head count to ensure safety evacuation of all personnel during emergency.

# TABLE OF CONTENTS

<b>ABSTRACT</b> .....	iii
<b>ACKNOWLEDGEMENT</b> .....	iv
<b>LIST OF FIGURES</b> .....	vii
<b>LIST OF ABBREVIATIONS</b> .....	viii
<b>CHAPTER 1: INTRODUCTION</b> .....	1
1.1 Background of study .....	1
1.2 Problem Statement.....	2
1.3 Objective and Scope of Study.....	4
<b>CHAPTER 2: MODELING THEORY</b> .....	5
2.1 Model of Transmitter .....	7
2.1.1 Coding .....	8
2.1.2 Raised Cosine Filter .....	9
2.1.3 Hilbert Transform .....	10
2.1.4 SSB Transmission .....	11
2.1.5 Quantization.....	11
2.1.6 Up-Converter .....	11
2.1.7 Power Amplifier .....	12
2.1.8 Output Band Pass Filter .....	12
2.2 Model of Tags .....	12
2.3.1 Tag Received Power .....	12
2.3.2 Tag Reflection Model .....	13
2.3 Model of Receiver .....	14
2.3.1 Antenna.....	14
2.3.2 Low Noise Amplifier (LNA) .....	14
2.3.3 Direct Conversion .....	15
2.3.4 Filter .....	15
2.3.5 Base-Band DSP.....	15

<b>CHAPTER 3: LITERATURE REVIEW .....</b>	<b>16</b>
3.1 Current Security and Safety System .....	16
3.2 Existing Model of RFID Implementation .....	16
3.2.1 Watcher-ATS System .....	16
<b>CHAPTER 4: METHODOLOGY.....</b>	<b>20</b>
4.1 Active RFID Localisation Techniques.....	20
4.2 Choice of Best Frequency .....	21
4.3 Wireless Personnel Safety System (Wi-PerS) .....	21
4.4 Active RFID Receiver-Transmitter.....	22
4.4.1 RFID Receiver Module.....	23
4.4.2 RFID Receiver Circuitry.....	24
4.4.3 RSSI Curve .....	25
4.4.4 RFID Transmitter Module .....	28
4.4.5 RFID Transmitter Circuitry .....	29
4.4.6 Receiver Multiplexing .....	32
4.4.6.1 Multiplexer Schematic .....	33
4.4.6.2 Multiplexer Control Commands .....	34
4.4.7 Hardware Setup.....	35
<b>CHAPTER 5: ANALYSIS AND RESULTS.....</b>	<b>36</b>
5.1 Hardware Results ... ..	36
5.2 Application using ActiveX .....	38
<b>CHAPTER 6: DISCUSSION.. ..</b>	<b>39</b>
<b>CHAPTER 7: CONCLUSION.....</b>	<b>40</b>
<b>REFERENCES.....</b>	<b>41</b>
<b>APPENDICES.....</b>	<b>42</b>

## LIST OF FIGURES

Figure 1: RFID System Operation .....	2
Figure 2: Forward Link Simulation .....	6
Figure 3: Return Link Simulation .....	7
Figure 4: Configuration for SSB, DSB and unmodulated return link .....	8
Figure 5: Manchester Coding Scheme .....	8
Figure 6: Raised Cosine Filter ... ..	9
Figure 7: Manchester coding after raised cosine filter.....	9
Figure 8: Hilbert Transform Wave .....	10
Figure 9: Hilbert Transform of Manchester Coding .....	10
Figure 10: Tag received power versus distance .....	13
Figure 11: Tag being defined by zone .....	17
Figure 12: Overview on the peripheral interconnection .....	18
Figure 13: The physical main module of RFID receiver (RF8315R).....	23
Figure 14: Receiver core module PCR3A .....	24
Figure 15: Block diagram of RX3400 integrated circuit .....	25
Figure 16: RSSI curve for 433MHz and 315MHz receiver .....	26
Figure 17: Typical design and connection for RX3400 receiver module .....	27
Figure 18: Transmitter main module of RF40315T.....	28
Figure 19: Transmitter circuit diagram .....	29
Figure 20: Transmitter core module FS1000A .....	29
Figure 21a: Low power transmitter application.....	30
Figure 21b: Equivalent LC Model for matching circuit .....	30
Figure 22: Determining transmitter frequency using spectrum analyzer.....	31
Figure 23: RS232 Multiplexer... ..	32
Figure 24: RS232 Multiplexer Schematics .....	33
Figure 25: Hardware setup for RFID triangulation.....	35
Figure 26: HyperTerminal configuration of RFID System.....	36
Figure 27: COM1 configuration.....	37
Figure 28: Nine unique IDs with 4 alphanumeric characters being read .....	37
Figure 29: Application using ActiveX.....	38

## **LIST OF ABBREVIATIONS**



## **ACKNOWLEDGEMENT**

First of all, I would like to express a lot of thank to Allah s.w.t to make my project run as required for the entire final year. I also would like to express my gratitude to the supervisor, Dr. Mohamad Naufal for her guidance and encouragement to assist me in the project. Great thanks to other lecturers of Electrical & Electronics Engineering. Big thanks also go to all lab technicians, especially to Mrs Siti Hawa for great support and helpful assistance.

I would like also like to express a special thank to my family for their priceless supports, encouragements, constant love, valuable advices and their understanding of me. And also bunch of thanks to all my colleagues for the supports to this project.

Finally, million thanks to all parties who had contributed directly or indirectly in completing this project.

Thank You.

**MUHAMMAD FARID MD DAUD**  
Electrical and Electronics engineering  
Universiti Teknologi PETRONAS

# CHAPTER 1

## INTRODUCTION

### 1.1 Background of Study

RFID (Radio Frequency Identification) is a mean of storing and retrieving data through electromagnetic transmission (usually in wireless communication) to an RF compatible integrated circuit.

RFID systems have several basic components or technical characteristics that define them. These comprise of a reader / interrogator (receiver), including an antenna (the device that is used to read and/or write data to RFID tags), a tag / transponder (A device that transmits to a reader the data, known also as RFID transmitter) and the communication between them. RFID uses a defined radio frequency and protocol to transmit and receive data from tags. A range of devices and associated systems are available to satisfy an even broader range of applications. Despite this diversity, the principles upon which they are based are quite straight forward, even though the technology and technicalities concerning the way in which they operate can be quite sophisticated.

RFID tags can be segregated into two major classifications according to their power source:

- **Passive tags**

Passive tags can be either battery or non-battery operated, depending on the intended application. Passive tags reflect the RF signal transmitted to them from a reader or transceiver and add information by modulating the reflected signal. A passive tag does not use a battery to boost the energy of the reflected signal. It may use a battery to maintain memory in the tag or power the electronic parts that will enable the tag to modulate the reflected signal.

• **Active tags**

Active tags contain both a radio transmitter and battery to power the transmitter. Active tags have an onboard radio and therefore have substantially more range (~300 feet/100m) than passive or “active/passive tags.” Active tags are also more expensive compared to passive tags and, as with any battery-powered product; the batteries must be replaced after a certain time.

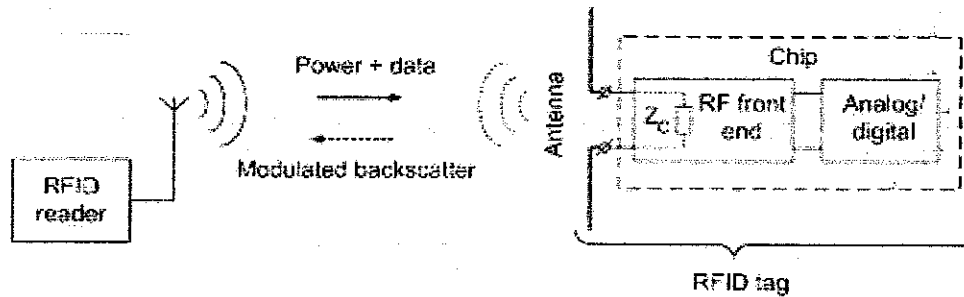


Figure 1: RFID system operation. The backscattered signal is modulated by changes in chip impedance  $Z_c$ .

The use of active RFID technology is expanding rapidly. Active RFID uses an internal power source (battery) within the tag to continuously power the tag and its RF communication circuitry. Many resources within the RFID research and development community have been focusing on hardware and firmware components, including active and passive RFID tags, tag readers, embedded software, error reduction and storage in electronic databases, while the application of such RFID tags are limited with sensing of indoor or small areas. Only few resources focusing on exploiting the RFID applications are made viable and cost effective for large covered areas. Therefore, more emphasis should be treated on the RFID research in long-range detection.

## **1.2 Problem Statement**

Traditionally, the normal procedures in emergency safety and evacuation are not totally reliable. There are in some cases where although the regular safety precaution is implemented, the rate of emergency cases reported still at high stake. There are several factors that lead to the ineffectiveness of current safety standard of procedures, but usually the main reasons are 1) lack of awareness / discipline of personnel and 2) lack of potentially faster detection and improper supervision / communication of personnel during emergency cases. Usually the first factor can be improved but for the second factor, there is a need for a more reliable system to overcome the problem.

Take for an example of a large plant where there involves so many workers and the risk of accident to occur is high. Frequent shift of workers can lead to uncertainty whether or not all the members of the old shift made out of the plant and whether or not the all members of new shift arrived. Although the personnel are heavily trained in safety procedures, but in a case where at a certain time, unexpected calamity such as fire, smoke / fog, hazardous gas release, and explosion might occur and the possibility for them to be trapped in such a chaotic condition is high, therefore for a normal procedure it is almost impossible to ensure that each personnel are safely detected and evacuated in a short period. It may become even worse when the detection is done lately and small injuries might already evolved into severe burns and in some outcomes can lead to the death of the personnel.

Therefore, there is a need to come out with an RFID system that can facilitate in proper detection during those stated condition. The proposed RFID system has to be able to detect the presence and mobility tracking (in/out) of personnel inside the plant, thus reducing time taken in the event of evacuation whereas the information of personnel's whereabouts is important, besides ensuring that access control to the specific controlled area is strictly limited to authorised personnel by the mean of geo-fencing and access control.

### **1.3 Objective and Scope of Study**

The objective of our research is to develop an outdoor location-sensing system for plant emergency condition. Our goal is to implement a prototype outdoor location-sensing system using low cost wireless devices based on existing infrastructures without burdening cost of developing a new one. At present, there are several types of location-sensing systems, each of them having their own strengths as well as limitations. Infrared, 802.11, ultrasonic, optical, cellular, magnetic and RFID are some examples of these systems.

In the project, we are focused in using commodity off-the-shelf products. This should somehow decrease the time consumed for preliminary design of the devices and can have more concentration at the systemic stage. From preliminary research done to compare several wireless technologies, there have been found that RFID have greater advantages over other technology with respect to the application. The no contact and non-line-of-sight (Non-LoS) nature of this technology are significant advantages and common among all types of RFID systems. All RF tags can be read despite extreme environmental factors, such as rain, fog, ice, paint, and other visually and environmentally challenging conditions. They can also work at remarkable speeds. In some cases, tags can be read in less than 100 milliseconds. The other advantages are their promising transmission range and cost effectiveness.

## **CHAPTER 2**

### **MODELING THEORY**

In order to have a technical comprehension on the RFID subject, nevertheless the system has to be firstly simulated and evaluated. A system simulation environment in Simulink is constructed where special attention is emphasized on the analog/RF circuit [1]. There are several additive parameters that have to be taken into account for simulating RFID in real situation, such as phase noise of local oscillator, TX-RX coupling, reflection of the environment, Additive White Gaussian Noise (AWGN), DC offset, I/Q mismatch, and others. The whole performance of the system can be evaluated by changing the method of coding, varying parameters of designated blocks, and estimation of operation distance.

To limit the simulation for a simpler analysis, a single reader and a single tag bi-directional communication can be investigated to simulate the physical parameters. The communication link is half duplex, means that the communication between reader to tag occurs first and then tag to reader (“reader talks first”). In forward link, reader sends a modulated carrier to tags and powers up the tags while in return link, reader sends a continuous wave carrier, tag receives the carrier for power supply and backscatters by changing the reflection coefficients of antenna. In such a way, data is sent to reader from tag. This method of sending/receiving of data is called backscatter method.

Readers should be designed in compliance with the local frequency regulatory in transmitter. To detect the backscatter signals from tag, a relative high sensitivity is chosen at a given bit error rate.

Figure 2 shows the simulation of transmitter in Simulink. In forward link, it is critical to see whether the transmitting signal is under the frequency mask of the local regulation. Therefore raised cosine filter, Hilbert transform, DAC (quantization error) and filter, PLL, mixer and high power amplifier are added to accurately get the required frequency. The transmission types can be SSB (single side band), DSB (double side band) or continuous wave carrier by switching the manual switches in Figure 2.

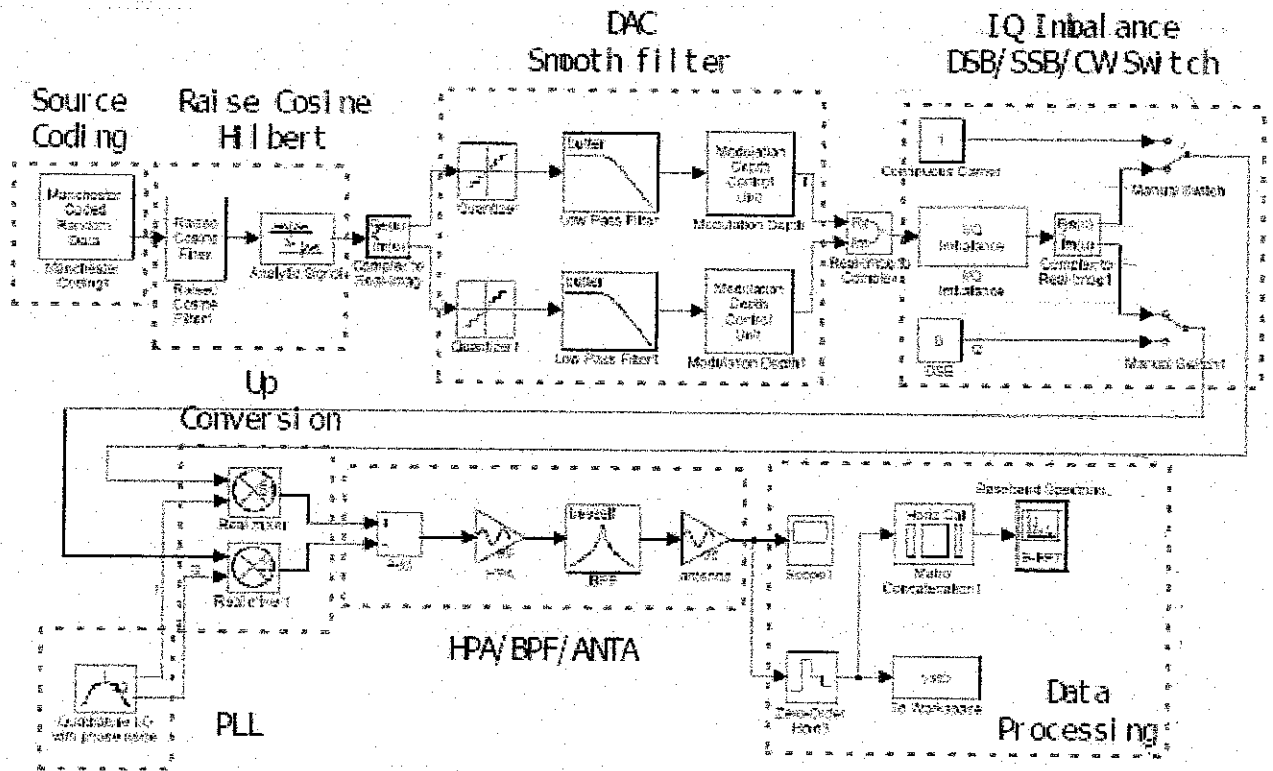


Figure 2: Forward link simulation

Figure 3 is the simulation of return link. The free space is modeled by a pass loss with changing phase due to distance between reader and tag. The transmitter sends a continuous carrier to power up tag. AWGN channel is used to model the sources of noise from space. Another source of receiving power during the return link is the direct coupling from TX to RX, modeled by introducing a gain and phase delay.

The receiver includes band pass filter, LNA, Mixer, AC coupling, channel select filter and the variable gain stages. Meanwhile, the tag is modeled by coding method of variable antenna gain and percent of reflection. Comparison of the received and down converted signal with the data tag backscattered will give the bit-error rate performance.

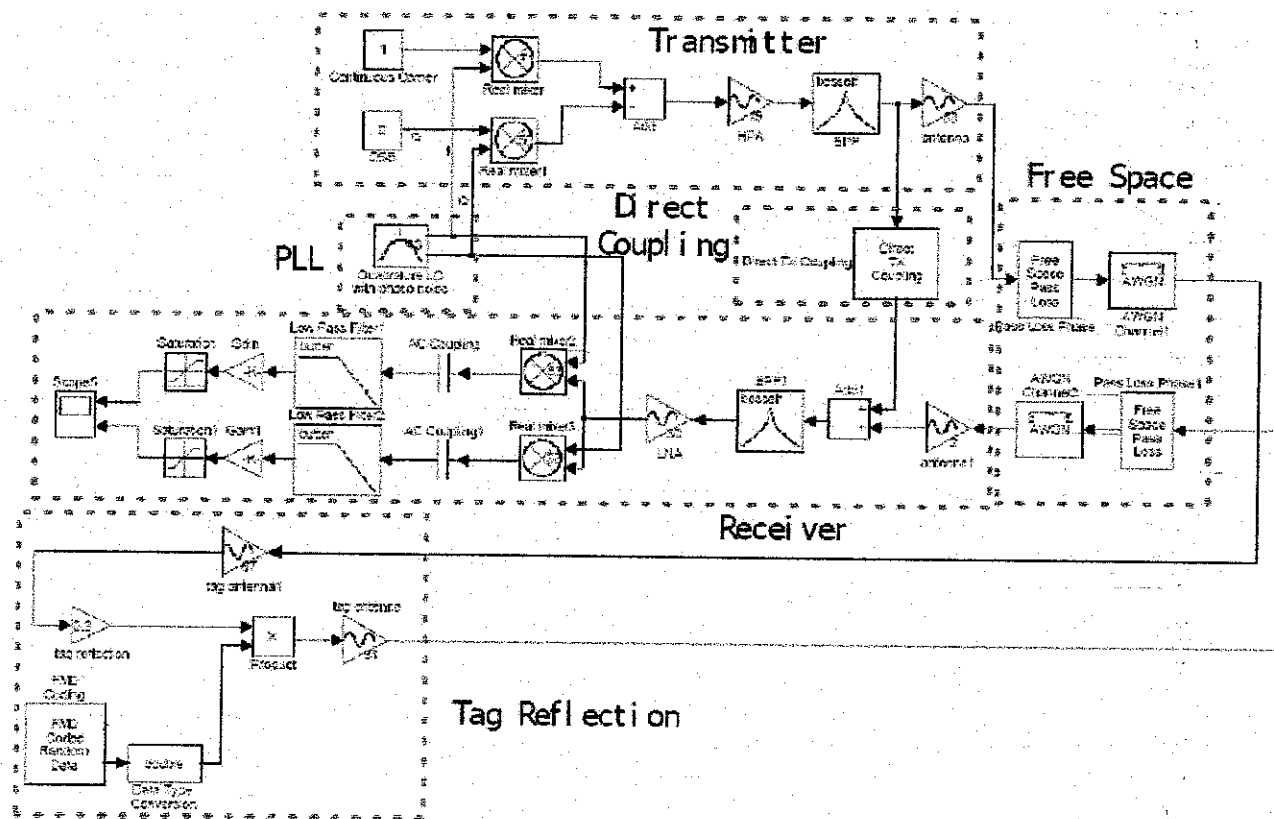


Figure 3: Return link simulation

## 2.1 Model of Transmitter

The transmitter architecture has been chosen to be I/Q-branches due to the SSB transmission and different digital modulation techniques such as ASK or PSK. The coding for forward link is Manchester coding. The transmitter should fulfill the protocol and support the DSB or SSB transmitting for forward link, and send an unmodulated carrier for return link. Figure 4 gives the configurations of transmitter for SSB and DSB modulations and the return link unmodulated carrier.



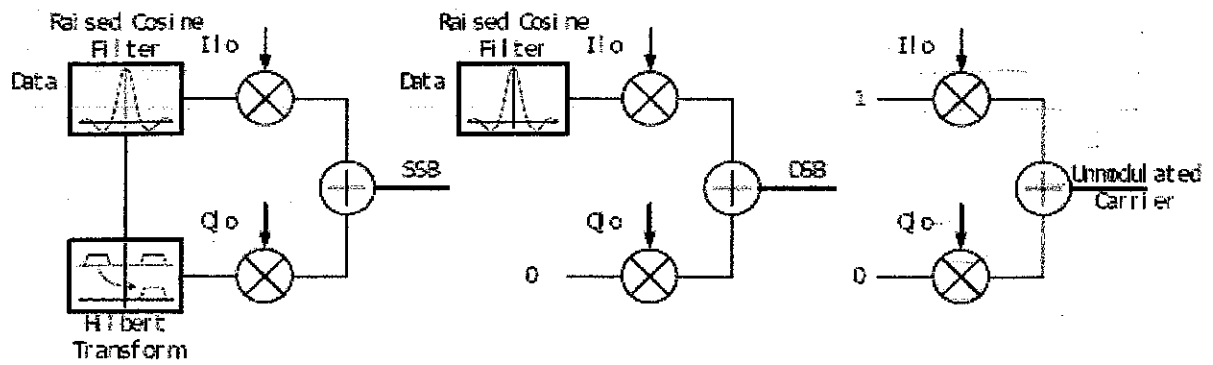


Figure 4: Configuration for SSB, DSB and unmodulated return link

### 2.1.1 Coding

The protocol is based on Manchester coding for forward link, whereas FMO and Manchester sub-carrier coding are for return link [1]. The power spectral density of Manchester sub-carrier is different with original Manchester code because additional DC component is added by the asymmetric probability of two levels.

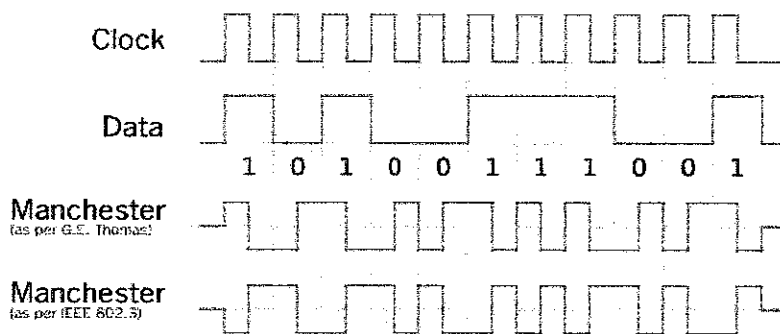


Figure 5: Manchester coding scheme

BER (Bit error rate) is introduced to evaluate the performance of RFID in digital communication system. In forward link, the CNR (carrier-to-noise ratio) emitted is large enough for a tag to demodulate data by envelope detector and the tag will reflect the incident power.

### 2.1.2 Raised Cosine Filter

The raised-cosine filter is a particular electronic filter, frequently appearing in telecommunications systems due to its ability to minimise *inter-symbol interference* (ISI). A band-limited signal, which has no ISI should satisfy Nyquist criterion [2]. It is so called due to the non-zero portion of the frequency spectrum of its simplest form ( $\beta = 1$ ) being a cosine function, 'raised' up to sit above the  $f$  (horizontal) axis.

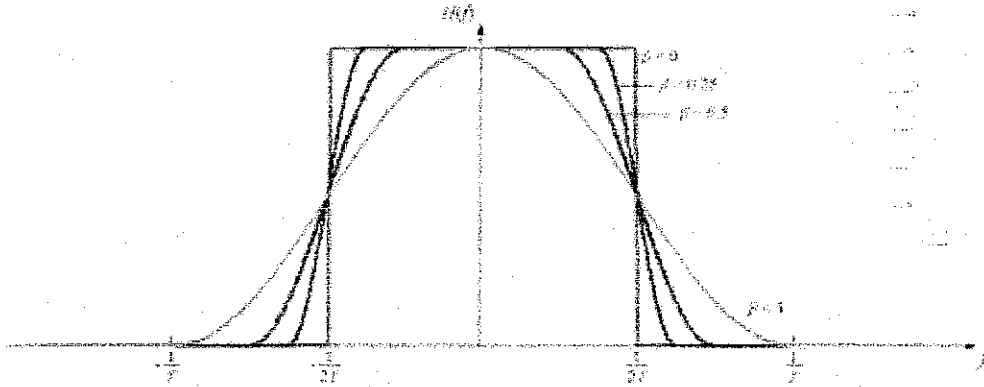


Figure 6 is the simulation result of Manchester coding with roll off factor 0.1, 0.5 and 1, the oversampling ratio 32, and data rate 80kbps. To meet the stringent waveform bound less than 5% of the modulated signal; the roll off factor  $\beta$  must chosen to be 1.

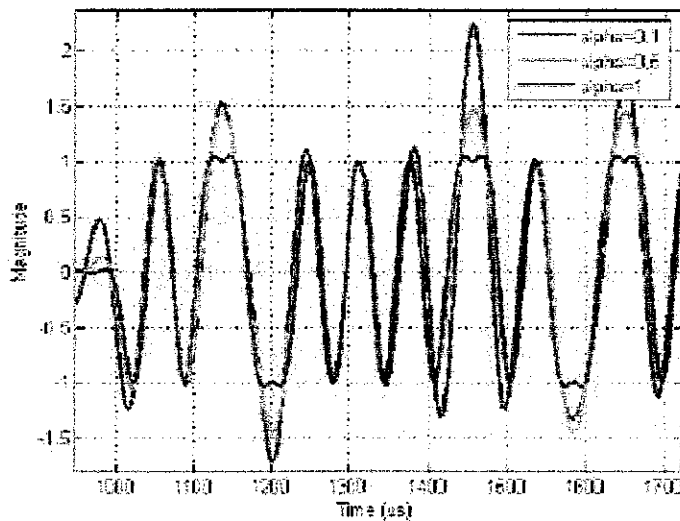


Figure 7: Manchester coding after raised cosine filter

### 2.1.3 Hilbert Transform

The Hilbert transform, here denoted  $H$ , of a real-valued function,  $s(t)$ , is obtained by convolving signal  $s(t)$  with  $1/\pi$  to obtain  $\hat{s}(t)$ . Therefore, the Hilbert transform  $\hat{s}(t)$  can be interpreted as the output of a linear time invariant (LTI) system with input  $s(t)$ , and a system impulse response given as  $1/\pi$ . It is a useful mathematical tool to describe the complex envelope of a real-valued carrier modulated signal.

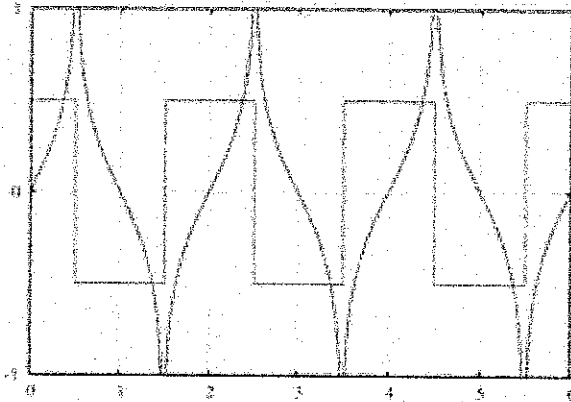


Figure 8: The Hilbert transform, in red, of a square wave, in blue

Figure 9 shows the Hilbert transform of Manchester coding with data rate 80kbps.

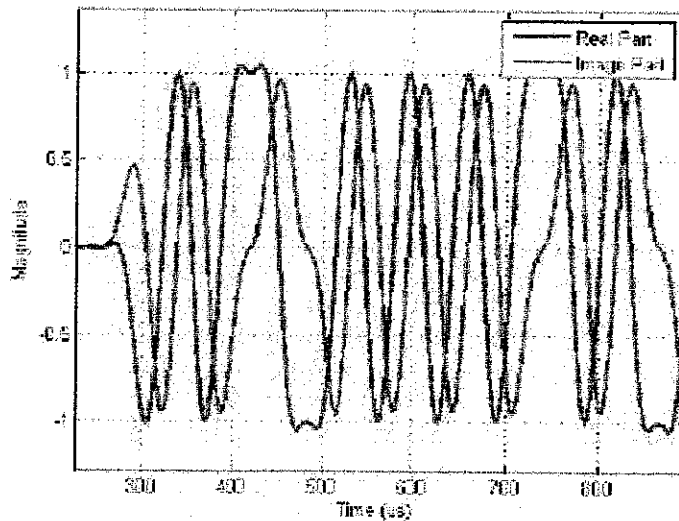


Figure 9: Hilbert Transform of Manchester coding

#### 2.1.4 SSB transmission

SSB-AM is derived by removing one of the sidebands of DSB-AM, and occupies one half bandwidth of DSB-AM [2]. The signal power of SSB is half of the DSB. The noise power in the bandwidth is also half of the DSB due to the half bandwidth. Therefore, the SNR (signal-to noise ratio) of SSB and DSB are the same.

When the signals are up-converted and mixed, the SSB-AM is produced. I/Q mismatch is one of the problems both in I/Q transmitter and in receiver. In transmitter, the phase and gain mismatch of I/Q-branches will degrade the suppression of SSB transmission since the DSB transmission only occupies the I-branch. In practice, it is desirable to maintain the amplitude mismatch less than 1dB and phase error below 5° [3].

#### 2.1.5 Quantization

The signal is over sampled by FIR filter such as raised filter and Hilbert transform. After digital signal processing, the digitized signal is send into analog part. In practical, a DAC will convert digital signals into analog, which yields quantization error. The clock of DAC is usually higher than the signal. In an oversampling circuit, the maximum sinusoidal power to the quantization noise is [4]:

$$SNR_{max} = 6.02N + 1.76 + 10\log(OSR)$$

N is number of the quantization bits, OSR is the oversampling rate. The first term (6.02N) is the SNR due to the N-bit quantizer while the OSR term is the SNR enhancement obtained from over sampling. This can model the noise power induced by the DAC. The low pass filter after DAC is to smooth out the resulted waveform.

#### 2.1.6 Up-converter

The transmitter architecture of Figure 3 suffers from LO (Local Oscillator) pulling. The output power of PA is a modulated waveform with high power and a spectrum centered around the LO frequency. Despite of various shielding techniques employed to isolate the VCO (Voltage Controlled Oscillator), the “noisy” output of the PA (Power Amplifier) still corrupts the oscillator spectrum through “injection pulling” or “injection locking”. The problem worsens if the PA is turned on and off periodically to save power.

Therefore, the VCO must be followed by a buffer stage with high reverse isolation between the VCO and the PA.

### 2.1.7 Power Amplifier

The power amplifier is modeled with nonlinearities, IIP2 and IIP3 for different types of power amplifiers. The AM/PM effect of amplifier is not included since tags are not sensitive to the phase of the carrier. The power amplifier is to give a proper power gain and the gain range of the power amplifier should cover the regulatory of CEPT, FCC, etc.

### 2.1.8 Output Band Pass Filter

The output band pass filter is to remove the out of band spurious spectrum. A fourth order Bessel filter is selected with the bandwidth range from 860MHz to 960MHz. The maximum input power of the filter is about 1W and it can be implemented by passive elements (R, L and C).

## 2.2 Model of Tags

### 2.2.1 Tag Received Power

In forward link, the output power is

$$P_{EIRP} = P_{PA} G_{TX}$$

The Effective Isotropic Radiated Power (EIRP) of the reader is  $P_{EIRP}$ . The typical maximum output power is 500mW, 2W (ERP, CEPT) and 4W (EIRP, FCC). Converted to dBm, the permitted maximum limits are about 29dBm (500mW ERP, 825mW EIRP), 35dBm (2W ERP, 3.3W EIRP) and 36dBm (4W EIRP).  $G_{TX}$  is the gain of the transmitter antenna. The typical value is assumed to be 6dBi. Therefore, the maximum output power from power amplifier should be 23dBm, 29dBm and 30dBm, respectively. The power transmitted from reader to tag can be expressed as

$$P_{rec} = P_{PA} G_{TX} G_{tag} \left( \frac{\lambda}{4\pi d} \right)^2 = P_{EIRP} G_{tag} \left( \frac{\lambda}{4\pi d} \right)^2$$

$\lambda$  is the wavelength of the carrier.  $d$  is the distance from reader to tag. The tag available power versus distance can be seen in Figure 10. From the industrial experience, RF input power of 10uW (-20dBm) to 50uW (-13dBm) is required to power on tag.

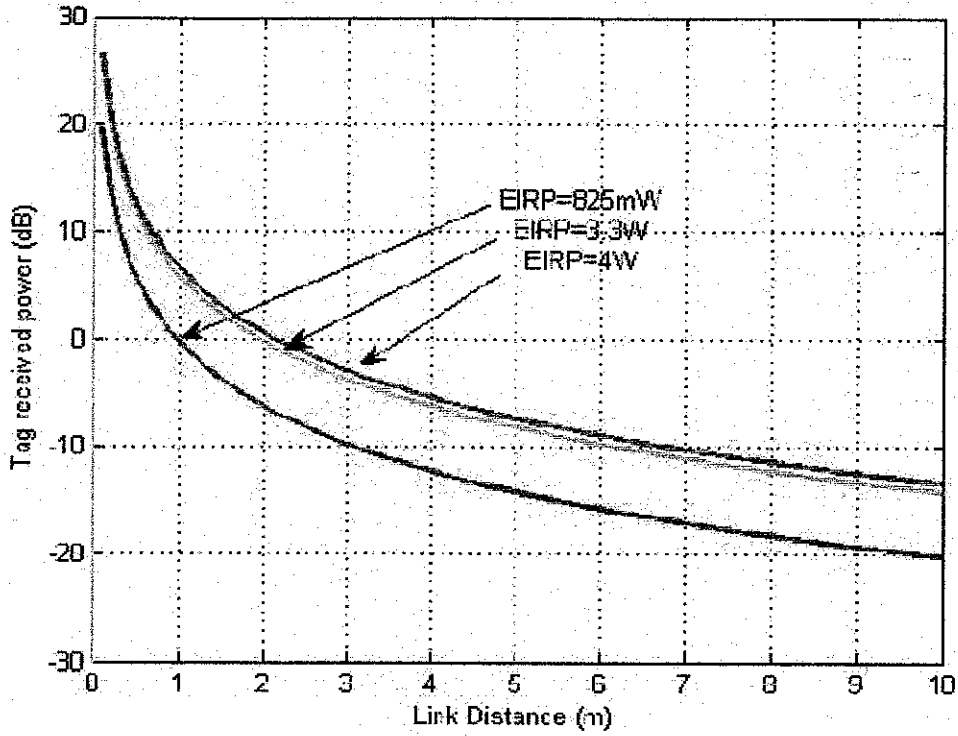


Figure 10: Tag received power versus distance

### 2.2.2 Tag Reflection Model

As we know, tag received power includes two parts, the reflected power and the available power can be used by the chip. The distribution of these two parts is very critical for a maximum distance. The available power from antenna can be used by the rectifier is

$$\begin{aligned}
 P_{RF,m} &= p_1 P_{RF,m,1} + p_2 P_{RF,m,2} \\
 &= \frac{v_0^2}{8R_{ant}} \left[ p_1 (1 - |\rho_1|^2) + p_2 (1 - |\rho_2|^2) \right]
 \end{aligned}$$

The reflection power is

$$P_{bs} = \frac{1}{8} |i_1 - i_2|^2 R_{rad}$$

$v_o$  is the peak source voltage that would be observed if the antenna were not loaded by the IC. In time domain, the probabilities that chip in state 1 and state 2 are  $\rho_1$  and  $\rho_2$ .  $\rho_{1,2}$  are the reflection coefficients.  $R_{ant}$  is the real part of the antenna impedance.  $i_{1,2}$  are the current flow through the impedance.  $R_{rad}$  is radiation impedance of antenna.

## 2.3 Model of Receiver

### 2.3.1 Antenna

The antenna can be configured in two types, two antennas or one antenna with a circulator. In return link, the receiver of reader listens to the response of tag while the transmitter sends a continuous wave to power up the tag. It is very critical to have a high isolation between TX and RX for a high performance reader.

The direct coupling from TX to RX with one antenna is larger than two antennas because of low isolation performance of circulator. Assume the transmitting power is 36dBm (FCC), the isolation of a circulator is about 35dB (Commercial circulator can hardly exceed 40dB). Therefore, the power seen in the receiver is about 0dBm. In this case, the receiver circuit should have a large dynamic range to handle the relative large signal and detect the weak signal backscattered from tag. The direct coupling signal is much larger than the reflection from the environment and the environment can be ignored.

### 2.3.2 Low Noise Amplifiers (LNA)

The LNA is optional for different antenna configurations. If it is configured with two antennas, the isolation is relative high. In this case, LNA is used to get a proper gain and better NF (noise factor) of receiver.

The gain range is from  $-10$  to  $10$  dB. If a circulator is used, the isolation is very poor and the power into the receiver is very large. In this case, a power splitter is used instead of LNA because of its capability of handling large signal.

### *2.3.3 Direct Conversion*

The architecture of receiver is direct conversion receiver suitable for multi-protocol operation. The DC offsets are very large due to low isolation between the TX and RX. The receiver will have a multi-stage gain to amplifier the weak signal. Since the DC offset is much larger than the signal, the offset may saturate the amplifier if it is not removed. An AC coupling stage is inserted after the mixer filtering out the DC component.

The I/Q mismatch of the receiver is different with the transmitter. In receiver, the I/Q mismatch will corrupt the down-converted signal constellation such as QPSK. In RFID system, the modulation used in return link is AM and PSK. It has less influence in the receiver with amplitude modulation.

### *2.3.4 Filter*

A high order channel select filter is applied to get a sufficient out of band suppression. The filter type in the receiver is a 5-order Butterworth filter due to its flatness in the passband and suitable for amplitude modulation.

### *2.3.5 Base-band DSP*

The base-band DSP is to decode the signal from ADC. The DSP should combine the signal power of I/Q branch for maximizing the signal power to get the best BER performance. In addition, some filtering must be made to suppress the out of band interference in further.



## **CHAPTER 3**

### **LITERATURE REVIEW**

#### **3.1 Current Security and Safety Systems**

An RFID system using active tags is a versatile tool in situations involving restriction of access, movement monitoring, communication between operators and a control system, and locating colleagues in an emergency. In an active RFID system, access control is an inherent feature. Safety and security is the new dimension that open up to RFID implementation.

#### **3.2 Existing Model of RFID implementation**

Active RFID systems have been improving considerably, and they present a versatile tool for safety, access control, and security. However, to make such a system the extended arm, it must be set up well and have a simple user and maintenance interface. The option of connecting an RFID system to the administrative and process control network multiplies the possibilities and potential payback of such an investment. One of the systems that have been proven work in long-range detection using active RFID is the Watcher-ATS system.

##### *3.2.1 Watcher-ATS System*

Watcher is a software application that is at the heart of the Watcher-ATS system. It is installed on a server. PC clients that connect to the server are defined and the RFID equipment in the software is configured. There is also choice of integration of additional systems, such as video surveillance and fire alarms. Watcher system is presented here for a study comparison purpose to the intended output of this project. Therefore we can design an appropriate RFID system that functions alike to the Watcher-ATS but with lower cost and possible to implement.

Initially, a tag sends its unique ID to the RFID interrogator (reader). Watcher receives this info, updates tag position in real time, and notes the time of the previous reading. All data, reports, and statistics are handled in the Watcher database. The communication interface is open, so units can exchange data using TCP/IP, RS-232, RS-422, UHF, and VHF.

Watcher-ATS allows the administrator to define and adjust zones while the system is operating. Zones may be overlapping, but field strength measurement still locates the tag (see Figure 11).

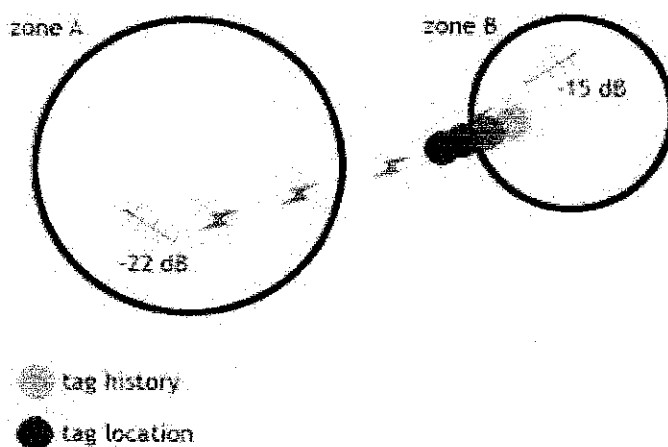


Figure 11: Tags being defined by zone.

Two zones (A and B) each have one antenna. A tag (the red dot) is located between the zones. The tag "belongs" to zone B until the field strength registered by zone A's antenna is greater. Each antenna's signal strength received from the tag is indicated beneath the antenna. Zone B's antenna has a field strength reading of -15 dB, compared to -22 dB for zone A's antenna, so the tag is closer to zone B than zone A. The history of the tag (previous readings, indicated by the tinted red dots) indicates that the tag belongs to zone B, because this was the last zone it was in. This history information is especially useful in cases where the field strength measurements are equal or where sudden jumps in the field strengths occur.

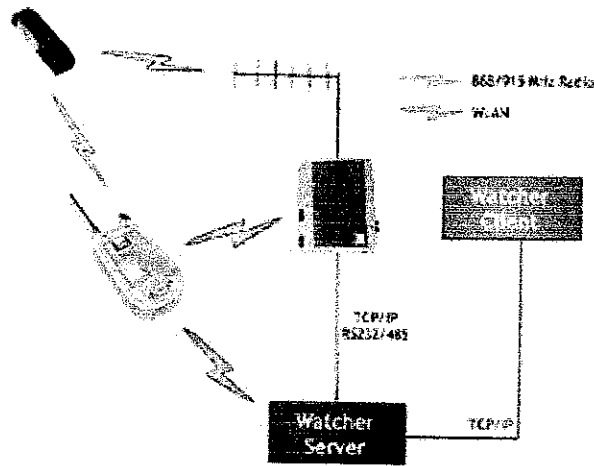


Figure 12: Overview on the peripheral interconnection.

Shown above is an overview of the communication flow in a typical Watcher-ATS system. The interrogator uses its antennas to communicate with the tags over 868/915 MHz radio frequency. The Carrier also communicates with the tags and uses a wireless local area network (WLAN) to communicate with the interrogator and Watcher server. Either TCP/IP or RS-232/-485 link the interrogator and the Watcher server; Watcher clients use traditional TCP/IP to connect with the server.

This interrogator is both a transceiver and a decoder; when it transmits a signal through the antenna, the tag answers or reflects the information embedded in it. The advantage over bar-code systems is that the interrogator does not have to "see" the tag or code visually. a system such as Watcher-ATS can accurately read the tags of an entire busload of workers passing at 40 km/h (25 mph). To achieve this, care has to be taken when tuning the equipment and Watcher software to the application.

The antenna scans its surroundings with signals that will wake up an active tag to reply with its embedded ID or the tag "reports" to the interrogator by itself. The tag identification rate may be adjusted, but has a typical maximum of 100 tags per second. A passive tag has no power source; it uses the power of the antenna signal to respond. An active tag contains its own power source and transmitter.

The server with the Watcher installed is connected to all the interrogators. There may be several clients where system maintenance or configuration is done.

Field strength measurement is used to assess the distance between tag and antenna. To locate a tag, up to four antennas per interrogator may be used. A zone is defined with one or more interrogators, depending on equipment, walls, and other obstacles.

In order to locate tags, the designer has to define a geographical zone and locate a minimum of one antenna in the zone. Using several antennas enables more accurate tag positioning using signal strength measurement. There are reflections from walls and equipment to take into account, and in buildings or process industry facilities involving multiple vertical levels, there exist challenge to locate the tags on the correct level. In addition, software algorithms must work together with the right equipment to avoid several antennas simultaneously reading a tag or, for a tag within range of several antennas, by allocating the tag to one zone.

## CHAPTER 4

### METHODOLOGY

Here we discuss existing RFID systems, along with applications of RFID onto plant for rescue and access control.

#### 4.1 Active RFID localisation techniques

There have couple of research and software that is commercialized to support location tracking for 802.11 wireless RFID tags. Most of these tags are limited with few hundred meters of range. Examples are Aeroscout, WhereNet and Ekahau. Somehow, these system are already established RTLS system that hybridize RFID with complex and expensive Wi-Fi system. Our goal however to have pure RFID used in real-time location system and considerably low cost implementation.

Usually the above mentioned location systems is an active RFID that includes Wi-Fi asset tags and also software necessary for asset tracking over a wireless LAN that ranging about few hundred meters at most. Previous algorithm for location detection has been proposed:

The nearest neighbour search techniques for RTLS is to take sample radio signals and correlate them to a known physical location. Once the samples were taken and stored, all recorded samples were performed with a linear search in real time and the closest signal match determined the personnel's location.

The triangulation techniques can present much more accurate location by means of averaging the three closest locations found during the search. Means of determining location via formulating the radio signal propagation models are performed but proven to be less accurate.

The probabilistic techniques that are applied for RTLS is to find location that is based upon which location in the stored radio map which has the maximum probability given the received signal strength vector. Usually this type of implementation of such wireless location determination must be done step by step and involves complexity of calculation even though the superiority of probabilistic approaches.

The choice between these techniques may justify how the tags / transmitter location is detected. However, it does not necessarily stick to just one technique, wherever either combination of the techniques may prove better result.

#### **4.2 Choice of the best frequency**

There is no specific frequency for RFID usage. Usually, the general frequency that are currently used for typical RFID systems are 125kHz, 13.56 MHz, 433 MHz, 900 MHz (UHF), 2.4 GHz (Microwave) and 6.1 GHz (Ultra Wideband). By default, the frequency that is approved for commercial use of RFID in Malaysia as stated by MCMC (Malaysian Communications and Multimedia Commission) are 125kHz, 13.56 MHz, 433 MHz and 900 MHz. For active RFID system utilized in this project, the frequency of 433 MHz is used due to its low cost implementation, less known interference, long-range detection (up to 40 meters) and the system implement backscatter method compared to inductive coupling.

#### **4.3 Wireless Personnel Rescue System (WiPeRS)**

In wake of recent issues in safety of working persons, there have been suggested an extension of a wireless real time location technology using RFID tags. By attaching RFID tag to the equipment and personnel, by using wireless access, they can easily be detected. It offers instant tracking of personnel, equipment and assets for improved safety and efficiency.

Conditions in plant to consider deployment of RFID system such as telecommunication cables, water, oil and gas, surface irrespective of soil conditions in terms of the presence of metal, water, concrete also battery life hours that powers the RFID tags. Other consideration might be poor signal penetration, high implementation cost and the inability to control the tag's RF signal in case of battery-powered tags.

Ideally, each personnel are given battery powered tag that transmits signals periodically informing the precise location to a remote server outside of the plant. Then using wireless computers, outside staff are able to access location information on internal Web pages by pointing their Web browsers to an intranet page. The last known location of personnel will be mapped, in the event the wireless network collapsed.

With all these in place, the location of personnel, as well as other valuable equipment can be continuously tracked and viewed in real-time from any web browser to ensure safety and higher probation.

Before the implementation of the project, it is advised to adhere with the requirement and approval from regulatory body for the choice of frequency. It is also noted that each plant requires a customized solution that caters to the individual requirement of the plant environment and to avoid interference with other plant control and monitoring systems. Therefore, area of coverage is an important planning aspect.

#### **4.4 Active RFID Receiver and transmitter**

The RFID unit used in the project itself consists of receiver (in formal word: reader) and transmitter (to simulate tags). The transmitter emits signal to be read by receiver. The transmitter and reader have to use similar frequency to allow communication between them. The frequency used is 433MHz. The readers (receivers) communicate to the main PC through RS232 DB9 serial port.

#### 4.4.1 RFID Receiver Module

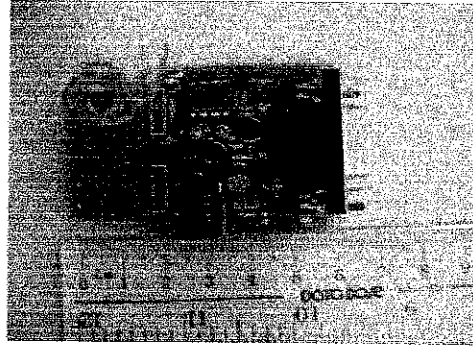


Figure 13: The physical main module of RFID Receiver (RF8315R)

The RF8315R active RFID receiver module receives data sent from RF40315T modules. This receiver module requires no external power supply (some PC or notebook may require external 9V power input). Data received will be sent to RS232 COM port. Standard communication and data acquisition software such as HyperTerminal can read the data. Custom program can read data from COM port for system integration or application development. An included ActiveX control makes the application integration to the hardware simpler and faster.

The device is plug-and-play based. Therefore, there should not necessary to send command to control the receiver. It can read data within 40 meters with build in RF40315T antenna. No additional power input is required for most desktop PC because the power supplied throughout the RS232 cable is sufficient. The device is of superheterodyne design which is for maximum stability. Superheterodyne design is the most stable but expensive design. This is particular suitable for challenging working conditions such as strong wind, serious raining and fast moving objects. Anti-collision algorithm is employed where RF8315R can handle 160 transmitters at the same time.

Although this design has so many advantages, it cannot receive short distance signal (within 1 meter). As a result this receiver cannot report the ID send by RF40315T within 1 meter. Below is the characteristic and specification of the receiver module:



Supply Voltage	9VDC via wall adaptor if necessary
Supply Current	4mA Typical
Operating Temperature	0 - 50°C
Operating Frequency	433 MHz
Data Output	ID sent by RF40315T (4 characters) plus 1 space
Capacity	160 ID at the same time
Build-in Watchdog	Yes. 2.3 seconds
<b>SERIAL PORT ( RS232)</b>	
Type	RS232, 9600 Baud, 8 bit words, 1 stop bit, 1 start bit, no parity

#### 4.4.2 RFID Receiver Circuitry

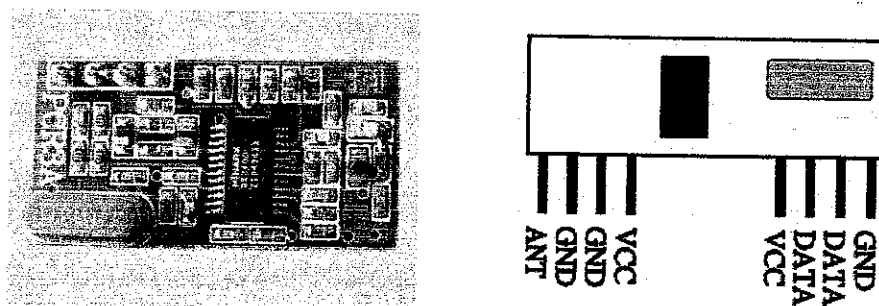


Figure 14: Receiver core module PCR3A

The receiver main unit is connected to the receiver core module PCR3A (as shown above). In the core module resides the ASK receiver IC, RX3400 which is suitably used in extremely low power radio applications and used in constructing RFID receiver circuits. The receiver IC incorporates an LNA; mixer; PLL-based local oscillator including VCO, fixed divider (divide by 64), reference crystal oscillator, phase-frequency detector (PFD), and charge pump; IF filter; logarithmic amplifier; data filter; peak detector; and 1-bit comparator and is capable of demodulating ASK input signals. The block diagram of this IC is illustrated in the diagram on the next page.



#### 4.4.3 RSSI Curve

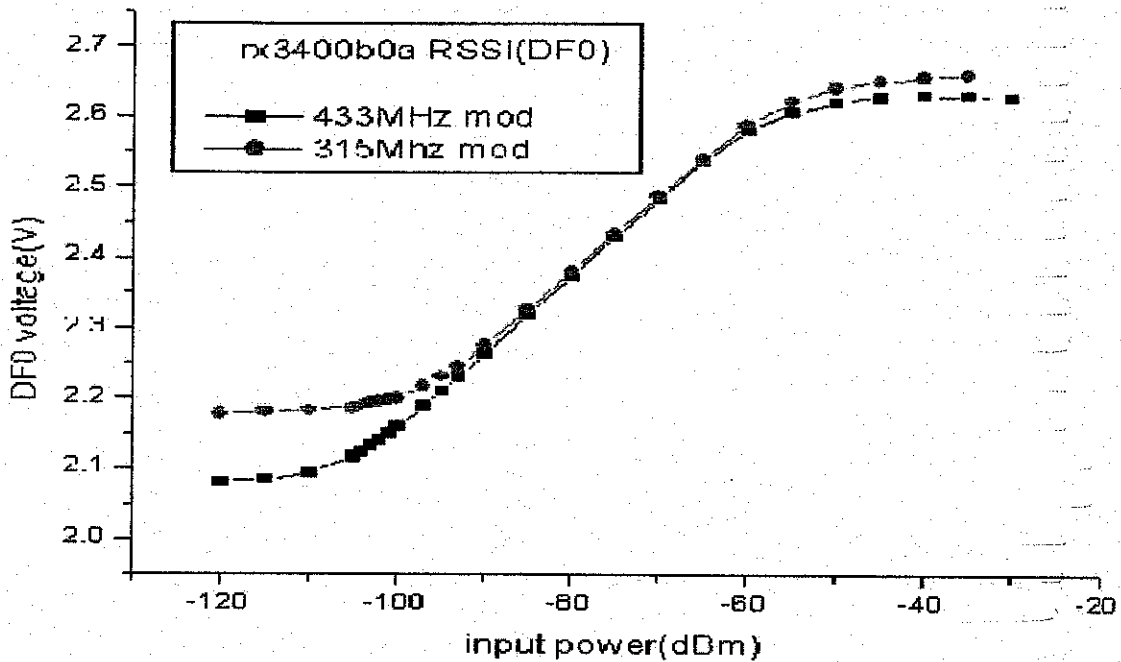


Figure 16: RSSI curve for 433MHz and 315 MHz receiver

One special feature of the RX3400 is that it provides an RSSI (Reduced Signal Strength Indicator) output. This characteristic is very important since we can ideally measure the distance between receiver and transmitter by looking at the signal strength (usually measured in dB). By looking at the characteristic of RSSI curve above, we can see the nonlinearity connection between the voltage measured at DF0 point (in the receiver IC RX3400) and input power from transmitter. Therefore, the receiver has to process the information and translated it into a comprehended function to be sent to computer.

The integrated 1-bit comparator make use of this RSSI by operating as a data slicer and “square up” the data filtered RSSI output from the logarithmic amplifier. The decision threshold voltage level for the 1-bit comparator is stored on an external capacitor connected to ASKREF pin (pin 10).

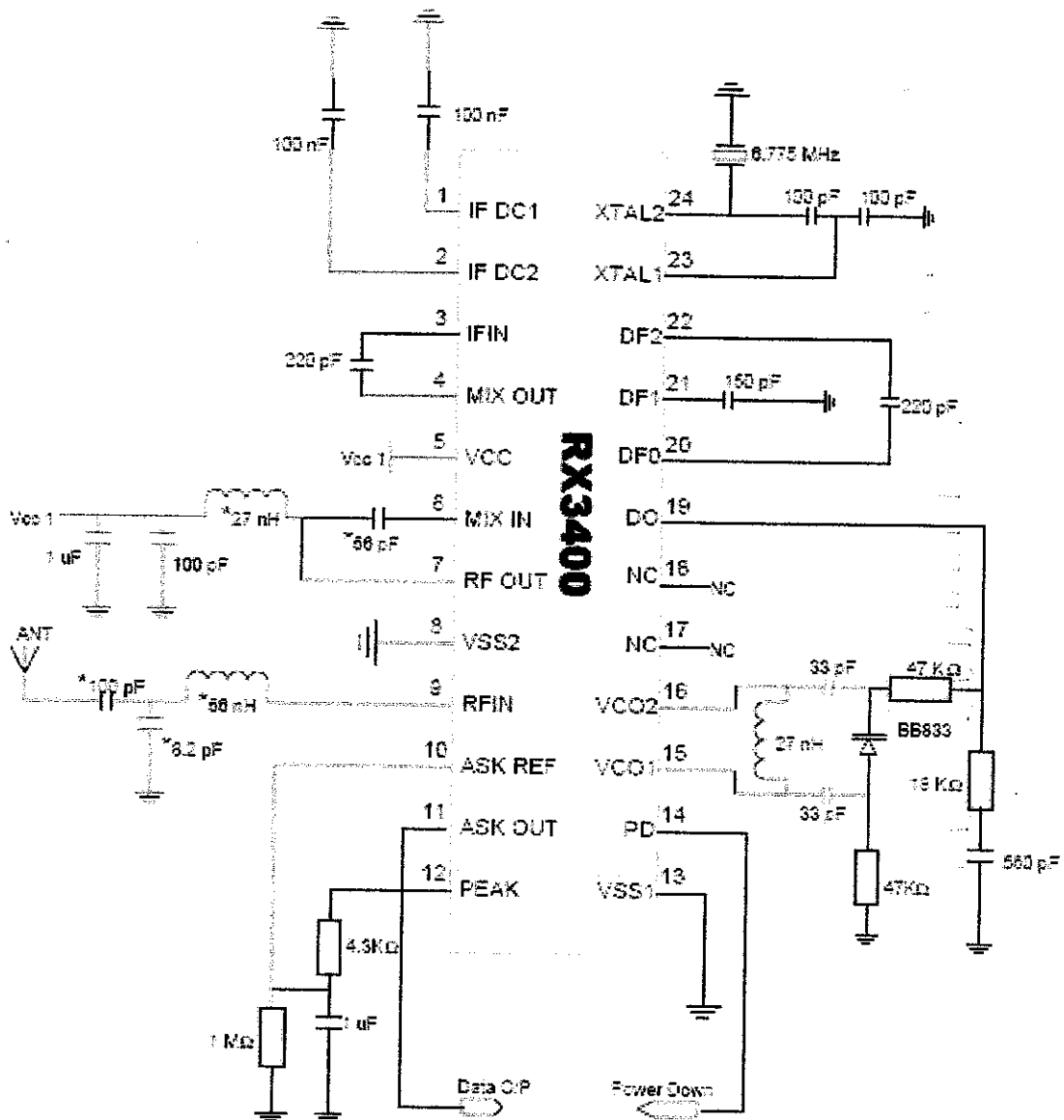


Figure 17: Typical Design and connection for RX3400 receiver module.

#### 4.4.4 RFID Transmitter Module

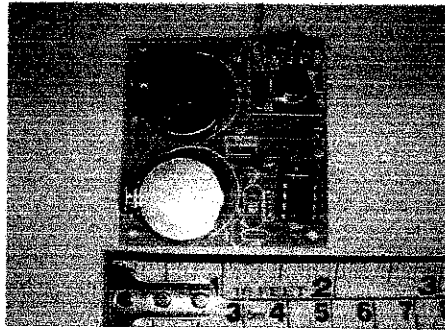


Figure 18: Transmitter main module RF40315T

A unique 4 alphanumeric characters (A-Z, a-z, 0-9) will be sent out on every 2.5 seconds plus/minus 0.5 second. The matching receiver RF8315R can receive the ID within 40 meters although the RF power emitted from the transmitter is very low. The transmitter will only turn on when ID is transmitting ( $< 0.01$  second), as a result it will not cause data jam to other devices that are using the same frequency band. Besides, it has low power consumption for long life time (4,000 hours for 2 x CR2032 batteries. Each CR2032 supply 3V). Preliminary testing shows that it can achieve detection range up to 40 meters and up to 100 meters if working environment is excellent.

Power Supply	2 X CR2032
Power Consumption	6mA when transmitting, 12uA when idle
Operating Temperature	0 - 50°C
Operating Frequency	433 MHz
Data Output	4 characters (A-Z, a-z, 0-9). All transmitters carry unique ID
Effective Radius	40 meters
RF output power	$< 15\text{mW}$

#### 4.4.5 RFID Transmitter Circuitry

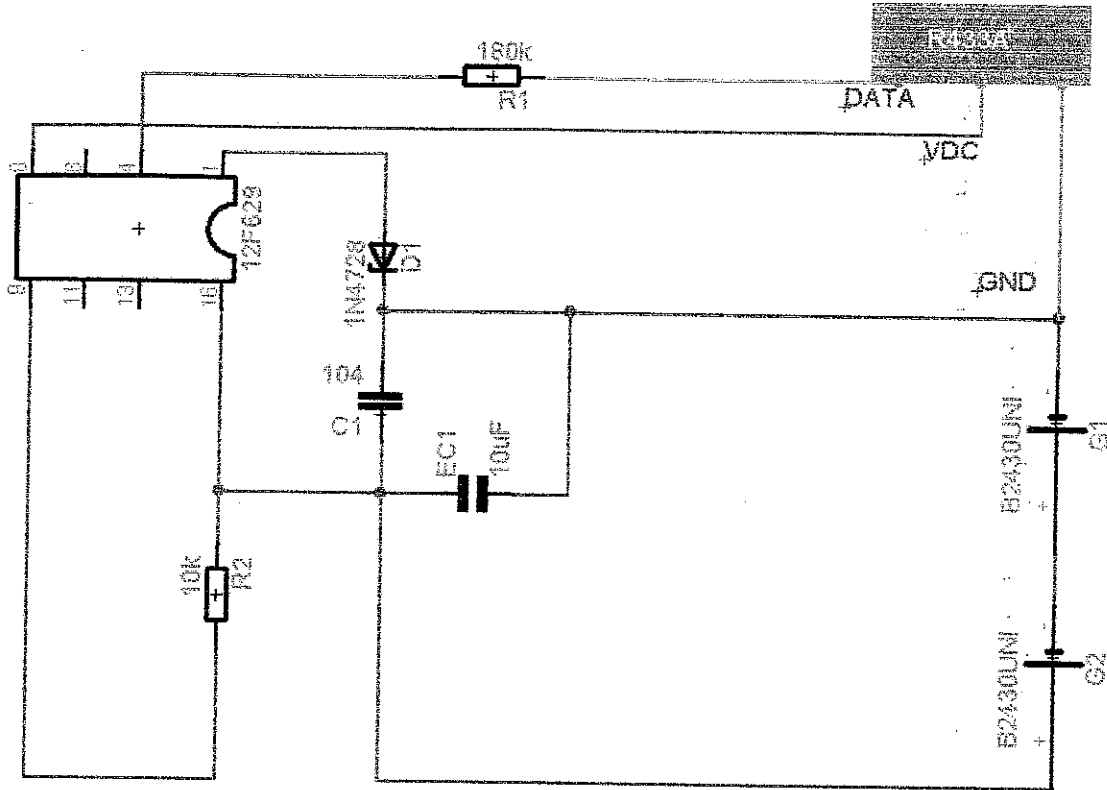


Figure 19: Transmitter Circuit Diagram

The main circuitry of RFID transmitting circuit consists of FS1000A transmitter core module and associated microcontroller circuit using Microchip 12F629. The configuration is simple, consists of only several components and powered by serially connected 3 volt batteries (summing up to 6V).

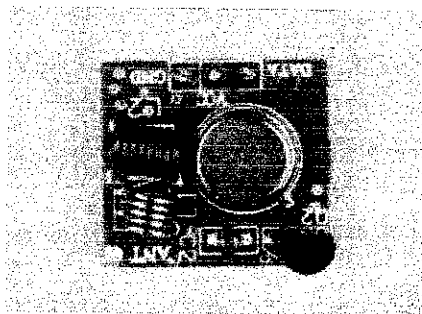
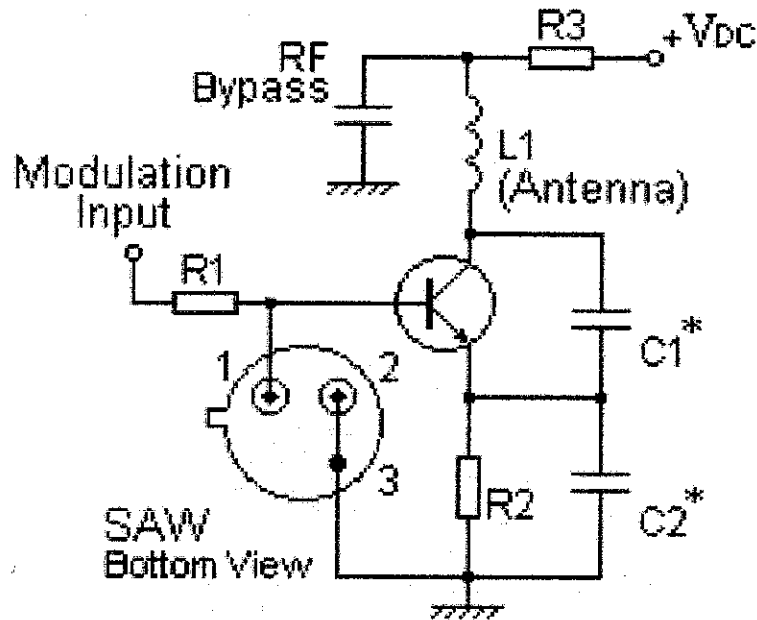


Figure 20: Transmitter core module FS1000A

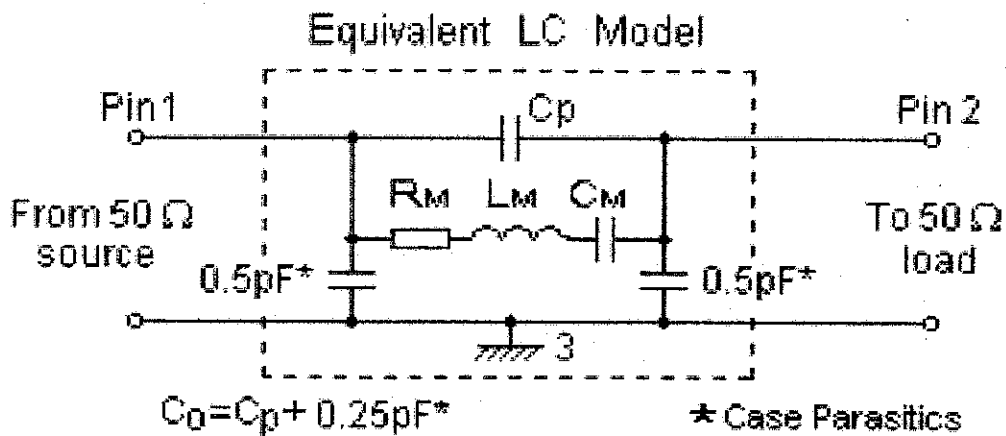
The transmitter core module, FS1000A consists of a local oscillator unit as shown above. The ACTR433.92 (also known as R433A) is a true one-port, surface acoustic-wave resonator in a low profile metal TO-39 case (one with silver caps shown above).

It provides reliable, fundamental-mode, quartz frequency stabilization i.e. in transmitters or local oscillators operating at 433.92MHz. The single core wire is attached to the ANT terminal to serve as the antenna of the transmitter.

The circuit to fully illustrate the application of low power transmitter in RFID transmitter is shown below. Shown also below is the equivalent RLC model/S parameter for 50  $\Omega$  impedance source-load matching circuit.



(a)



(b)

Figure 21a: Low power transmitter application.  
Figure 21b: Equivalent LC Model for matching circuit

The frequency response graph below shows transmission (measured in M Log) versus frequency (MHz) of the resonator/local oscillator. This graph shows the performance and precision of the resonator, using spectrum analyzer. The typical frequency response of this type of transmitter is centered on 433.92 MHz. This means that the output frequency in which the transmitter can optimally operate is in the said frequency.

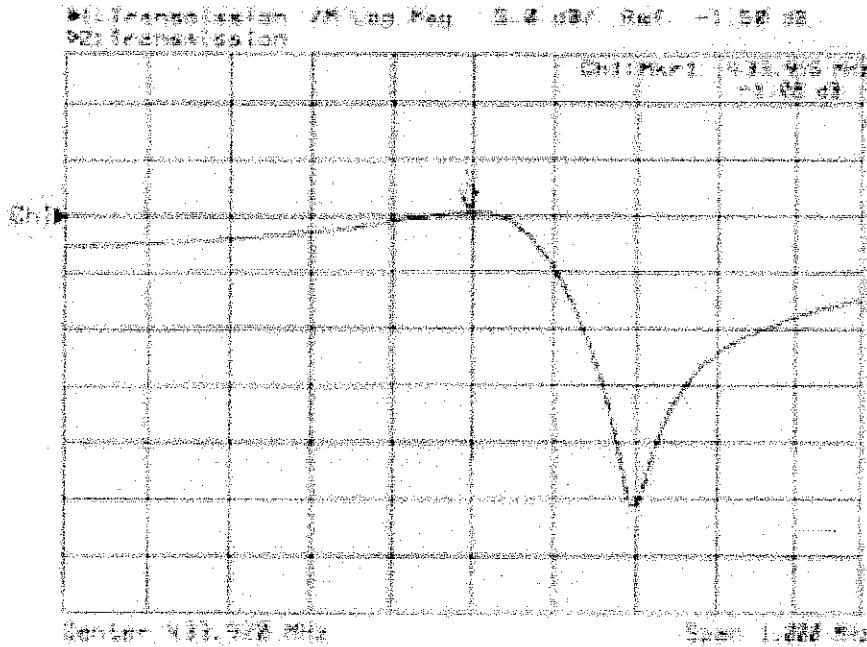


Figure 22: Determining transmitter frequency using spectrum analyzer



#### 4.4.6 Receiver Multiplexing

From the approach and techniques discussed in chapter 3 Section 1, the most suitable detection technique is the triangulation technique due to its higher accuracy and less complexity approach. But, it is impossible for us to depend on just one receiver and one transmitter to appropriately demonstrate and simulate the localisation of personnel in triangulation technique. Therefore, we need to multiplex at least three receivers altogether to demonstrate the triangulation technique effectively.

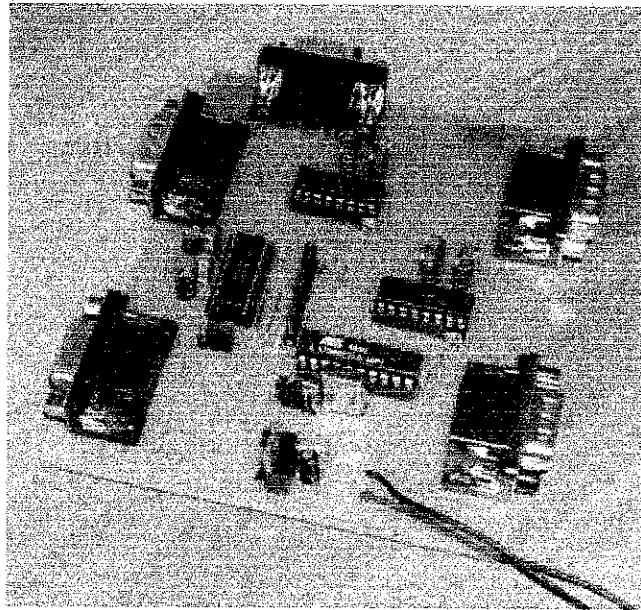


Figure 23: RS232 Multiplexer

This multiplexer allows up to 4 devices to be connected to one single RS232 port and can also be stacked for port expansion. Via stacked multiplexers, even an arbitrary number of devices can be controlled with one single port. But in this project, we are restricted to just single multiplexer because we only need just three receivers to adequately perform triangulation.

It has one master port and 4 slave ports and works like a switch connecting the master port to one of the slave ports. The multiplexer works at a fixed data rate of 9600 baud (no parity, 1 stop bit). The multiplexer supports line based communication and fixed data rate of 9600 baud (no parity, 8 data bits, 1 stop bit), where each line must be terminated by a

carriage return (0x13). The core operation of the circuit lies in the microcontroller, which is the ATMEL AVR AT90S2313-10. The hardware tuning is easy and is very low in cost. It has operating voltage of 9VDC (although can operate as minimal as 7VDC and up to 24VDC max). The multiplexer can also works as a programmer board for the microcontroller. The ATMEL AVR is programmed by using special software called *AVR Loader* which fully supported in Windows environment.

#### 4.4.6.1 Multiplexer Schematic

##### Master Port

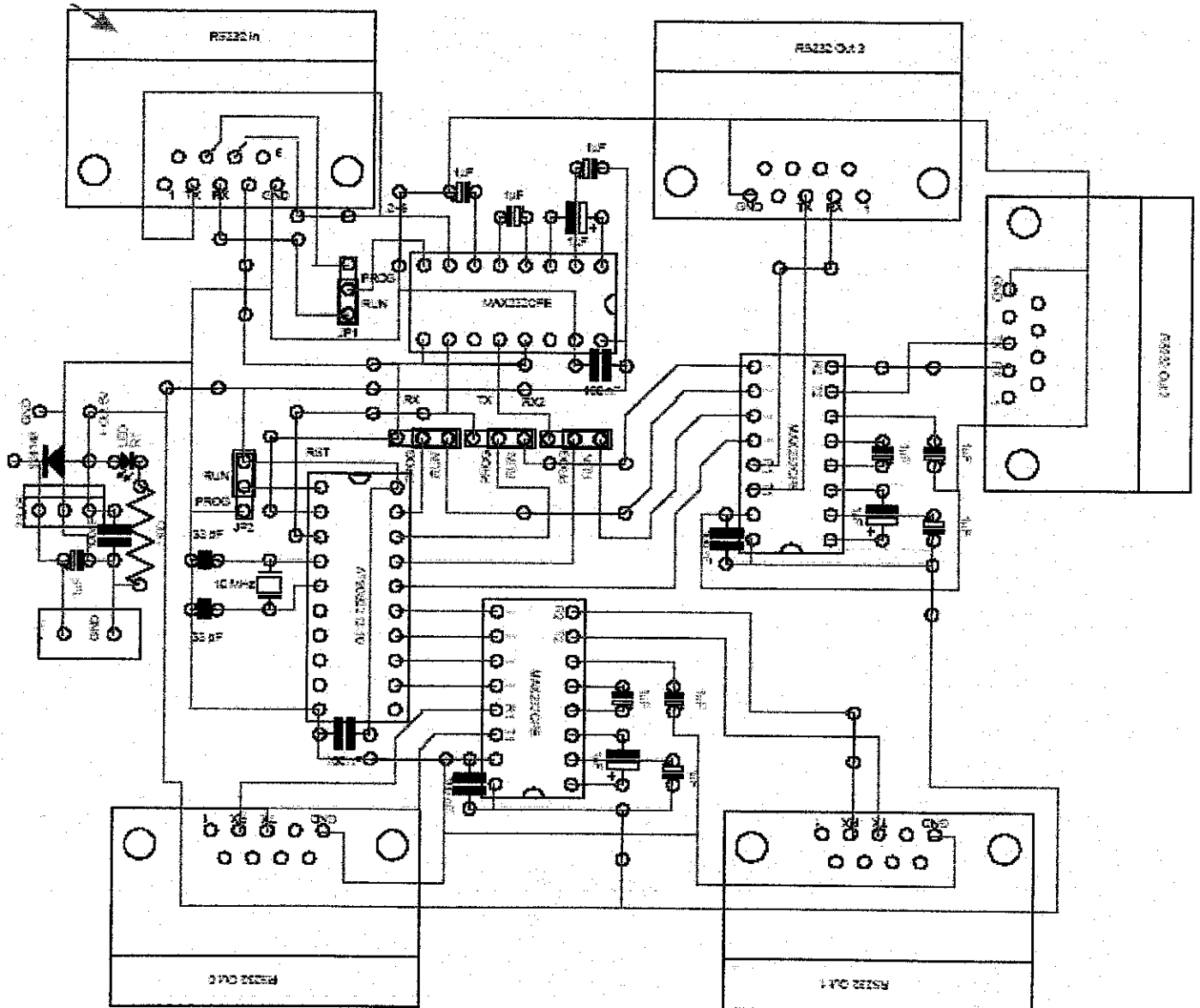


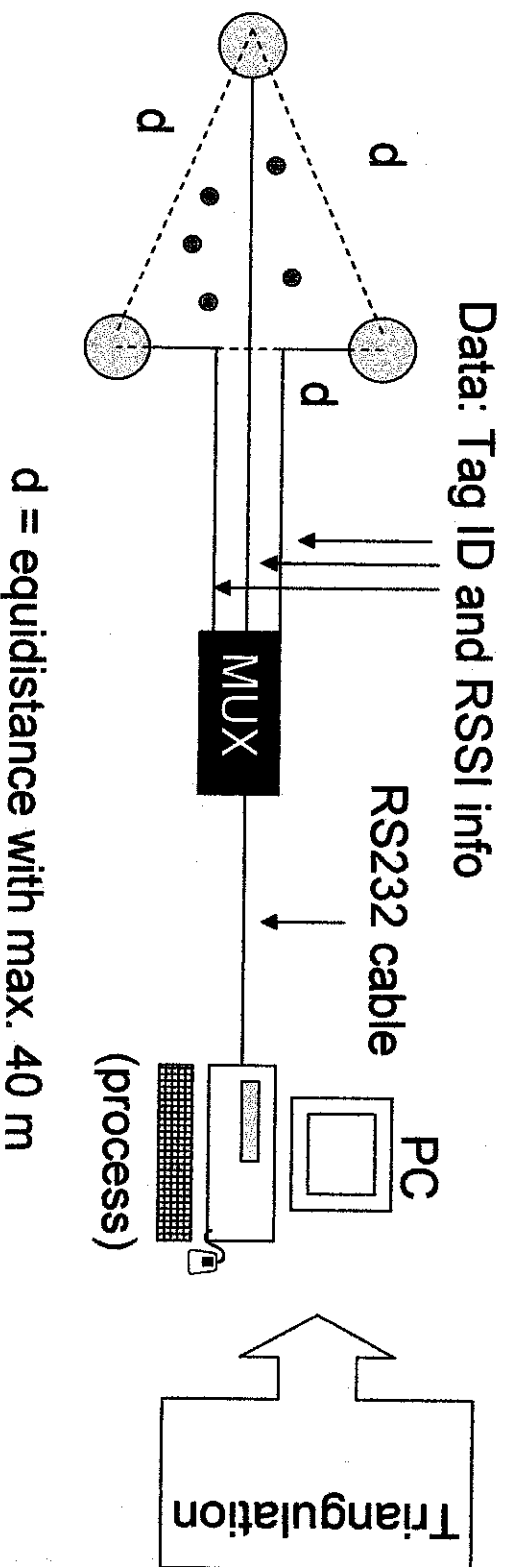
Figure 24: RS232 Multiplexer Schematics

#### 4.4.6.2 Multiplexer Control commands

By programming the microcontroller, the RS232 multiplexer works more like an electronic switch. Data received by the master port is transferred directly by the currently active slave port. Data received by the currently active slave port is forwarded unbuffered by the master port.

Control commands perform the switching between different ports as well as requesting status information. Control commands differ from normal data lines by their starting '\$' sign. This '\$' must be the first character of a line (i.e. it must be immediately transmitted after a 0x13 character). Control commands are only detected at the master port. To allow transmission of data lines starting with a '\$' sign or allow stacking of multiplexers, a '\$\$' at a line start is transmitted as a single '\$' followed by the normal data. As description of the control commands follows:

Command	Functions
<b>\$?</b>	Requests version identification string. The controller responds with something like 'RS232 Multiplexer Rev. 1.0'
<b>\$s</b>	Requests status information. The controller returns an 8-digit string; each digit is 1 or 0, respectively. The first 4 digit indicate framing errors. The first digit is 1 if a framing error has occurred at slave port 0, The second digit indicates a framing error on port 1 and so on. The last 4 digits indicate an overflow error and are always 0. Overflow means that a character was received on a slave port before a previously received line could be fully transmitted by the master port. The 5th digit indicates an overflow error on slave port 0, the 6th digit on port 1 and so on.
<b>\$n</b>	Makes port n the actual port. n is a digit from 0 to 3. Afterwards all data received at the master port is forwarded to slave port n. This also activates data reception on slave port n.



- Legend**
- RFID Receiver (reader)
  - RFID transmitter (tags)

Figure 25: Hardware setup for RFID triangulation

## CHAPTER 5

### ANALYSIS AND RESULTS

#### 5.1 Hardware results

In order to demonstrate the functionality of the radio frequency identification detection system, the hardware simulation is carried out. The identification is then detected by software using HyperTerminal software. The receiver is first connected to COM port 1 which is the dedicated serial port in a PC, and then the RFID tags are detected.

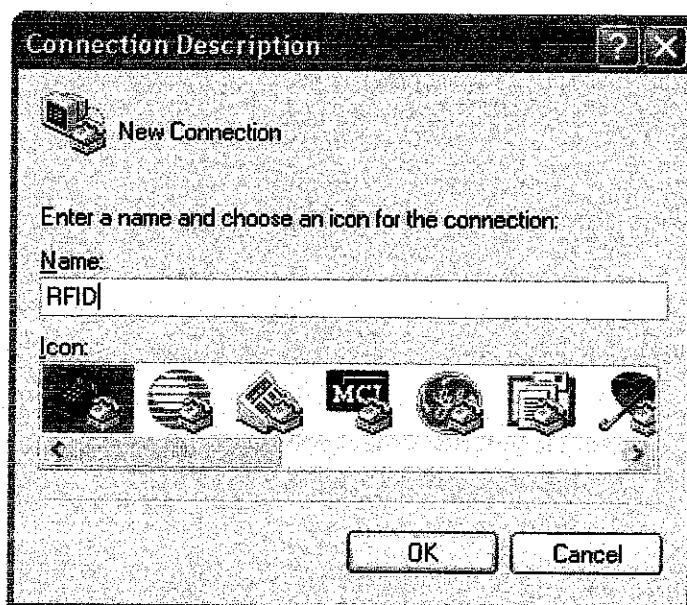


Figure 26: HyperTerminal configuration of RFID system

After the connection has been defined, the port is then set up. By using COM1 port, the bits per second is set to 9600 bps, with data bits of 8, parity set to none and stop bits are set to 1. Then, the RFID unit(s) will be detected. The transmitter will emit 4 alphanumeric characters to the receiver and the receiver will supply the information together with RSSI data to the PC in multiplexed manner.

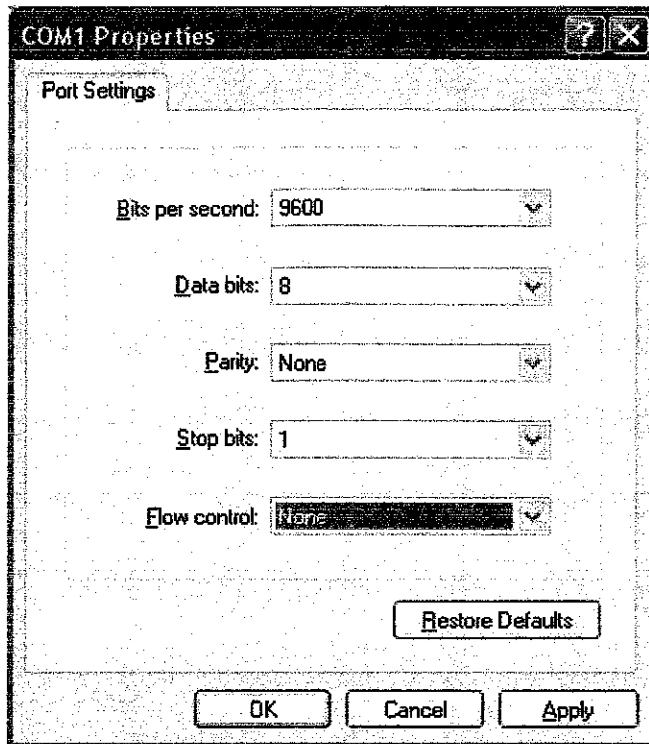


Figure 27: COM1 configuration

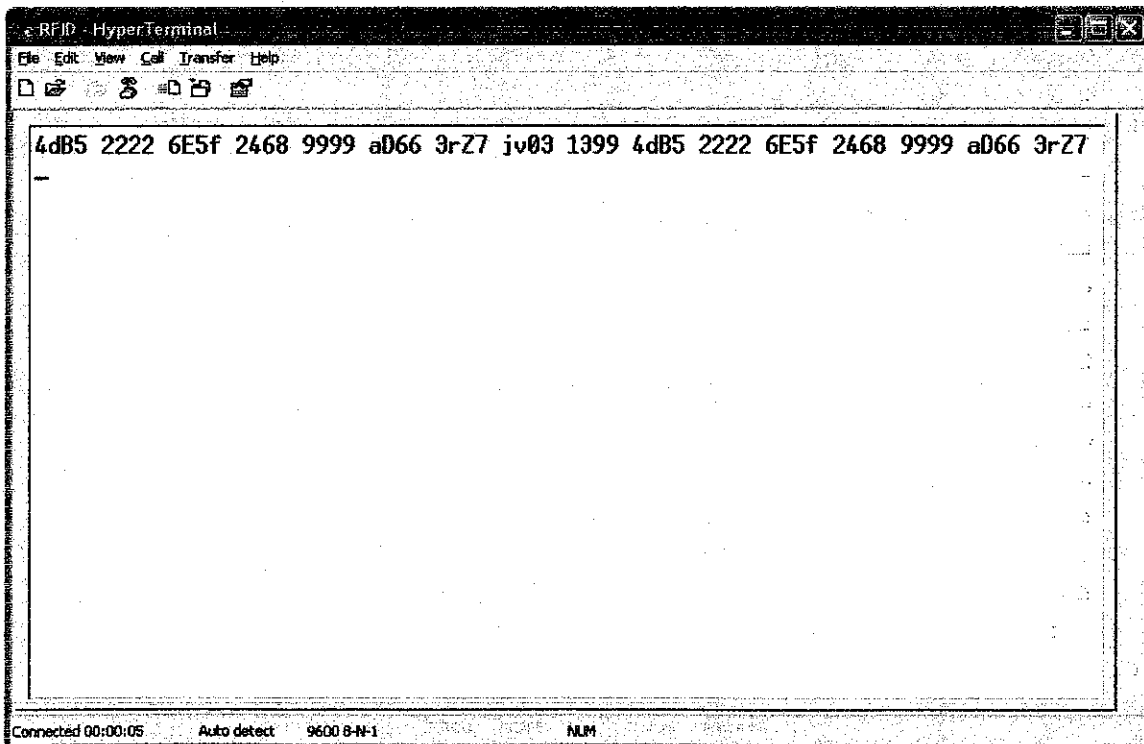


Figure 28 : Nine unique IDs with 4 alphanumeric characters being read simultaneously by RFID reader

## 5.2 Application using activeX

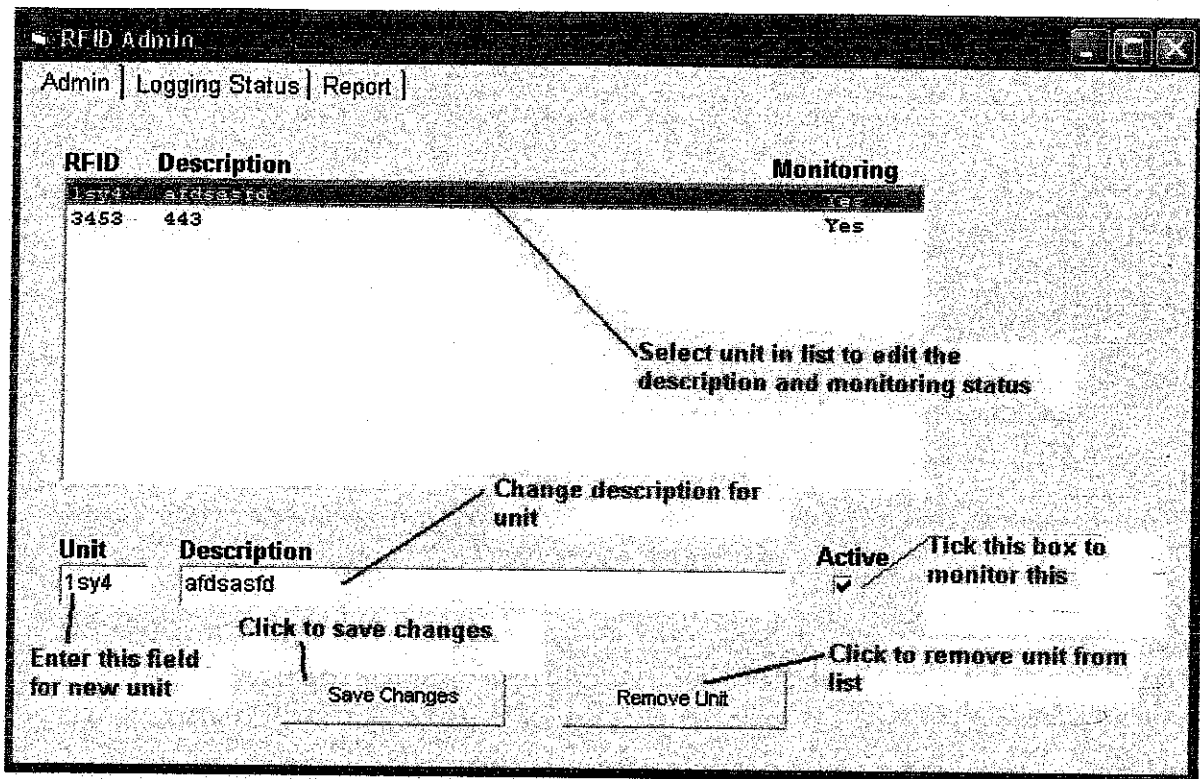


Figure 29: Application using activeX

The figure above shows how the transmitter is detected and logged into a program. The program (which custom built using Visual Basic and ActiveX control) manipulate the raw data presented in HyperTerminal to a friendlier interface using Visual Basic GUI (Graphic User Interface). Therefore, the user can easily detect the transmitter and display it for personnel's tracking management, and in emergency condition, the monitoring of personnel is not only easier to view but also manageable to track the personnel although he/she is in dangerous situation. The transmitter, although has designated ID in alphanumeric characters (e.g. GZ4J, etc.), with the help of the GUI, the designated unique code can be labelled with meaningful information such as the name of the personnel for easy tracking.

## **CHAPTER 6**

### **DISCUSSION**

During project implementation, there are several technical difficulty faced especially when doing hardware prototyping. The RFID system of transmitter (tag) and receiver (reader) manage to demonstrate the detection part of the project, but being unsuccessful in manipulating the parameters and circuitry ability to perform location sensing.

Internally, the factor came up when the reader itself claimed to be equipped with RSSI output. This means that the reader can be used to perform location sensing through the method discussed earlier in the previous chapter (i.e. by recognising input power level emitted by transmitter). Somehow, the user had put tremendous effort in searching ways to manipulate the RSSI featured in the receiver, but to no avail due to lack of knowledge and also scarce information found regarding the hardware / electronic devices and parts used in the project, besides the practical design architecture of the circuit itself in which it cannot perform the intended purpose despite of lack of space for modification.

Besides, the RSSI approach used in this text is insufficient to accurately locate a person / personnel because the measurement is greatly mislead by a noisy environment. For an example, although the distance between a transmitter and receiver is detected to be 6 meters, if anything comes to distract the signal strength, it might be read to be just 2 meters. Therefore, the reliability of using the concept is in doubt.

Furthermore, the design approach also put limitation to the objective. The design is simple and yet does not support much on expansion. Therefore, major modifications have to be carried out to put the design inline with the prescribed objective. Usually a more complex design requires a lot of cost and sometimes the design is patented and intended not to be released for development purpose. Therefore, cost has indirectly put the limitation to the success of the objective. In other word, the project indeed requires full concentration intensively in developing the RFID system.



## **CHAPTER 7**

### **CONCLUSION AND RECOMMENDATION**

Radio frequency identification (RFID) is a method where a radio frequency device is detected. In this project, the main objective / main task to be completed is that to bring out a system that not only able to deliver the detection capability of an RFID system, but also the ability to perform advanced feature or extension to it, that is to sense and locate the distance of the personnel in real-time.

Hence, the task is not as easy as ever perceived. Firstly, the user has to make a careful study on the most suitable RFID system and method of identification. The results have been aggregated from many sources in order to come up with the system which has as near-as-possible solution for the given problem, besides remaining the cost / budget properly managed. Secondly, the localisation method needed to be carefully selected so that it will not give a backfire effect to the later development of the project, so it will run smoothly and efficiently.

In technical / engineering point of view, the project has been developed to the extent that the user can really use and learn from it. Throughout the project, the user has faced many obstacle and hurdle in order to come with a good system. Although the final overcome is not as good as the early planned result, but at least most of the project phase has been conducted in proper manner and each of the successful milestones somehow contributed to the betterment of the system itself. It is hoped that the system will be improved better as the research and development progress. The technological advancement in RFID can lead to many useful applications that can help harmonise human interconnection with engineering especially in wireless communications.

## REFERENCES

- [1]. EPC Radio-Frequency Identity Protocols Generation 2 Identity Tag (Class 1): Protocol for Communications at 860MHz-960MHz. EPC Global Hardware Action Group (HAG), EPC Identity Tag (Class 1) Generation 2, Last-Call Working Draft Version 1.0.2, 2003-11-24
- [2]. John G. Proakis, "Digital Communications (Fourth Edition)", McGraw-Hill Companies, Inc, 2001
- [3]. Behzad Razavi, "RF Microelectronics", Prentice Hall, Inc. 1998
- [4]. David Johns, Ken Martin, "Analog Integrated Circuit Design", John Wiley & Sons, Inc, 1997

## **APPENDICES**

## MICROCONTROLLER SOURCE CODE

### File: 2313def.inc (Register Definitions for AT90S2313)

```
*****
; APPLICATION NOTE FOR THE AVR FAMILY
;*
;* Number :AVR000
;* File Name : "2313def.inc"
;* Title : Register/Bit Definitions for the AT90S2313
;* Date : 97.12.11
;* Version : 1.20
;* Support telephone : +47 72 88 87 20 (ATMEL Norway)
;* Support fax : +47 72 88 87 18 (ATMEL Norway)
;* Support E-Mail : avr@atmel.com
;* Target MCU : AT90S2313
;*
;* DESCRIPTION
;* When including this file in the assembly program file, all I/O register
;* names and I/O register bit names appearing in the data book can be used.
;*
;* The Register names are represented by their hexadecimal addresses.
;*
;* The Register Bit names are represented by their bit number (0-7).
;*
;* Please observe the difference in using the bit names with instructions
;* such as "sbr"/"cbr" (set/clear bit in register) and "sbrs"/"sbrc"
;* (skip if bit in register set/cleared). The following example illustrates
;* this:
;*
;* in r16,PORTB ;read PORTB latch
;* sbr r16,(1<<PB6)+(1<<PB5) ;set PB6 and PB5 (use masks, not bit#)
;* out PORTB,r16 ;output to PORTB
;*
;* in r16,TIFR ;read the Timer Interrupt Flag Register
;* sbrc r16,TOV0 ;test the overflow flag (use bit#)
;* rjmp TOV0_is_set ;jump if set
;* ... ;otherwise do something else
*****

;**** Specify Device
.device AT90S2313

;**** I/O Register Definitions
.equ SREG = $3f
.equ SPL = $3d
.equ GIMSK = $3b
.equ GIFR = $3a
.equ TIMSK = $39
.equ TIFR = $38
.equ MCUCR = $35
.equ MCUSR = $34
.equ TCCR0 = $33
.equ TCNT0 = $32
.equ TCCR1A = $2f
.equ TCCR1B = $2e
.equ TCNT1H = $2d
.equ TCNT1L = $2c
.equ OCR1AH = $2b
.equ OCR1AL = $2a
.equ ICR1H = $25
.equ ICR1L = $24
.equ WDTCSR = $21
```

```

.equ    EEAR          = $1e
.equ    EEARL         = $1e
.equ    EEDR          = $1d
.equ    EECR          = $1c
.equ    PORTB         = $18
.equ    DDRB          = $17
.equ    PINB          = $16
.equ    PORTD         = $12
.equ    DDRD          = $11
.equ    PIND          = $10
.equ    UDR           = $0c
.equ    USR           = $0b
.equ    UCR           = $0a
.equ    UBRR          = $09
.equ    ACSR          = $08

```

\*\*\*\*\* Bit Definitions

```

.equ    SP7           = 7
.equ    SP6           = 6
.equ    SP5           = 5
.equ    SP4           = 4
.equ    SP3           = 3
.equ    SP2           = 2
.equ    SP1           = 1
.equ    SP0           = 0

.equ    INT1          = 7
.equ    INT0          = 6

.equ    INTF1         = 7
.equ    INTF0         = 6

.equ    TOIE1         = 7
.equ    OCIE1A        = 6
.equ    TICIE         = 3
.equ    TOIE0         = 1

.equ    TOV1          = 7
.equ    OCF1A         = 6
.equ    ICF1          = 3
.equ    TOV0          = 1

.equ    SE            = 5
.equ    SM            = 4
.equ    ISC11         = 3
.equ    ISC10         = 2
.equ    ISC01         = 1
.equ    ISC00         = 0

.equ    EXTRF         = 1
.equ    PORF         = 0

.equ    CS02          = 2
.equ    CS01          = 1
.equ    CS00          = 0

.equ    COM1A1        = 7
.equ    COM1A0        = 6
.equ    PWM11         = 1
.equ    PWM10         = 0

.equ    ICNC1         = 7

```

```
.equ ICES1 =6
.equ CTC1 =3
.equ CS12 =2
.equ CS11 =1
.equ CS10 =0

.equ WDTOE =4
.equ WDE =3
.equ WDP2 =2
.equ WDP1 =1
.equ WDP0 =0

.equ EEMWE =2
.equ EEWE =1
.equ EERE =0

.equ PB7 =7
.equ PB6 =6
.equ PB5 =5
.equ PB4 =4
.equ PB3 =3
.equ PB2 =2
.equ PB1 =1
.equ PB0 =0

.equ DDB7 =7
.equ DDB6 =6
.equ DDB5 =5
.equ DDB4 =4
.equ DDB3 =3
.equ DDB2 =2
.equ DDB1 =1
.equ DDB0 =0

.equ PINB7 =7
.equ PINB6 =6
.equ PINB5 =5
.equ PINB4 =4
.equ PINB3 =3
.equ PINB2 =2
.equ PINB1 =1
.equ PINB0 =0

.equ PD6 =6
.equ PD5 =5
.equ PD4 =4
.equ PD3 =3
.equ PD2 =2
.equ PD1 =1
.equ PD0 =0

.equ DDD6 =6
.equ DDD5 =5
.equ DDD4 =4
.equ DDD3 =3
.equ DDD2 =2
.equ DDD1 =1
.equ DDD0 =0

.equ PIND6 =6
.equ PIND5 =5
.equ PIND4 =4
```

```

.equ    PIND3      =3
.equ    PIND2      =2
.equ    PIND1      =1
.equ    PIND0      =0

.equ    RXC        =7
.equ    TXC        =6
.equ    UDRE       =5
.equ    FE         =4
.equ    OR         =3

.equ    RXCIE      =7
.equ    TXCIE      =6
.equ    UDRIE      =5
.equ    RXEN       =4
.equ    TXEN       =3
.equ    CHR9       =2
.equ    RXB8       =1
.equ    TXB8       =0

.equ    ACD        =7
.equ    ACO        =5
.equ    ACI        =4
.equ    ACIE       =3
.equ    ACIC       =2
.equ    ACIS1      =1
.equ    ACIS0      =0

.def    XL         =r26
.def    XH         =r27
.def    YL         =r28
.def    YH         =r29
.def    ZL         =r30
.def    ZH         =r31

.equ    RAMEND     = $df ;Last On-Chip SRAM Location

.equ    INT0addr   = $001 ;External Interrupt0 Vector Address
.equ    INT1addr   = $002 ;External Interrupt1 Vector Address
.equ    ICPladdr   = $003 ;Input Capture1 Interrupt Vector Address
.equ    OC1addr    = $004 ;Output Compare1 Interrupt Vector Address
.equ    OVFladdr   = $005 ;Overflow1 Interrupt Vector Address
.equ    OVFOaddr   = $006 ;Overflow0 Interrupt Vector Address
.equ    URXCaddr   = $007 ;UART Receive Complete Interrupt Vector Address
.equ    UDREaddr   = $008 ;UART Data Register Empty Interrupt Vector Address
.equ    UTXCaddr   = $009 ;UART Transmit Complete Interrupt Vector Address
.equ    ACIaddr    = $00a ;Analog Comparator Interrupt Vector Address

```

## File: dbfmulti2.asm (core program for RS232 multiplexer)

```
*****
;Author: Frank F. Hitzel, Braunschweig, Germany (2004)
;This software is distributed under the terms of the GNU GPL
;Multiplexer, S version
;Framing Error bug correction by Adolf Schwarz
;*****

.include "2313def.inc"

.MACRO showMessage
    ldi Z1,low(@0 << 1)           ;show error message

INFO_LOOP:
    sbic USR,UDRE
    rjmp DO_SEND
    rjmp INFO_LOOP

DO_SEND:
    lpm
        inc ZL
        mov temp,r0
        out UDR,temp
        cpi temp,$0d
        brne INFO_LOOP

.ENDMACRO

.LISTMAC

rjmp RESET ; Reset Handler

.org $004
rjmp TIM_COMP

.org $007
rjmp UART_RXC

.equ frequency =1000000
;.equ frequency =3690000
.equ baud =9600
.equ freq_divi = (frequency / (baud*8))-1

.equ out0 =1
.equ out1 =2
.equ out2 =5
.equ out3 =7

.equ in0 =0
.equ in1 =3
.equ in2 =4
.equ in3 =6

.equ rxbuffers =15
;***** RAM
.dseg

.org $60 ;ramstart

rxchar0: .BYTE 1
```



```

rxcursor0: .BYTE 1

;***** Code
.cseg

.def rxreg0    =r1

.def txreg     =r5
.def status_save =r6      ; status save register for interrupt routines
.def txchar    =r8      ; contains next char to be sent

.def rxcnt0    =r9

.def txcnt     =r13
.def infofunc  =r14

.def temp      =r16
.def temp2     =r17
.def rxwait0   =r18
.def active_output =r19 ; contains active output as bit of the
                        ; corresponding output pin
.def active_input  =r20 ; contains active output as bit of the
                        ; corresponding output pin

.def txwait    =r22

.def rxstat =r23 ; low 4 bits full status of buffers, high 4 bits are
                ; receive_active_flags
.def status =r24 ; bit0 = sending; bit1=0: last was 0d; bit2=0: last
                ; was control; bit3=1: start send;
                ; high 4 bits are data there bits

.def errstat = r25 ; higher bits are framing errors, lower bits are
                ; overflow

.def tim_temp =r26
.def tim_temp2 =r27

OUTPUT_TAB:
.db out0,out1,out2,out3 ;must be within lowest 256 bytes

MSG_INFO:
.db "DoubleFox MultiplexerS Rev. 1.0a",13,0,0
MSG_ERROR:
.db "error",13,0,0

;*****
;
;                                UART RX
;*****

UART_RXC:      in    status_save,SREG
                in    tim_temp,UDR
                sbic  USR,FE      ;skip next if no framing error
                rjmp  IGNORE_RX
                sbrc  status,2
                rjmp  check_control
                sbrs  status,1
                rjmp  check_first
;
                in    tim_temp,UDR
                cpi   tim_temp,$0d
                brne  NO_LINEEND
                cbr   status,(1<<1) ;clear bit -> 0d detected

```

```

NO_LINEEND:    mov  txchar,tim_temp
               sbr  status,(1<<3)      ;start send

IGNORE_RX:    out  SREG,status_save
               reti

CHECK_FIRST:
;
               sbr  status,(1<<1)
               in   tim_temp,UDR
               cpi  tim_temp,'$'
               breq IS_CONTROL
               mov  txchar,tim_temp
               sbr  status,(1<<3)      ;start send
               out  SREG,status_save
               reti

IS_CONTROL:   sbr  status,(1<<2)      ;last was control
               out  SREG,status_save
               reti

CHECK_CONTROL:
;
               cbr  status,(1<<2)
               in   tim_temp,UDR
               cpi  tim_temp,'$'
               brne SWITCH_DESTPORT
               mov  txchar,tim_temp
               sbr  status,(1<<3)      ;start send
               out  SREG,status_save
               reti

SWITCH_DESTPORT:
               cbr  status,(1<<1)      ;last was 0d
               cpi  tim_temp,'0'
               breq SWITCH_ZERO
               cpi  tim_temp,'1'
               breq SWITCH_ONE
               cpi  tim_temp,'2'
               breq SWITCH_TWO
               cpi  tim_temp,'3'
               breq SWITCH_THREE
               cpi  tim_temp,'?'
               breq SET_INFO
               cpi  tim_temp,'s'
               breq SET_INFO
               out  SREG,status_save
               reti

SET_INFO:     mov  infofunc,tim_temp
               out  SREG,status_save
               reti

SWITCH_ZERO:  ldi  active_output,(1 << out0)
               ldi  active_input,(1 << in0)
               out  SREG,status_save
               reti

SWITCH_ONE:   ldi  active_output,(1 << out1)
               ldi  active_input,(1 << in1)
               out  SREG,status_save
               reti

```

SWITCH\_TWO:

```
ldi active_output, (1 << out2)
ldi active_input, (1 << in2)
out SREG, status_save
reti
```

SWITCH\_THREE:

```
ldi active_output, (1 << out3)
ldi active_input, (1 << in3)
out SREG, status_save
reti
```

```
;*****
;
;                      TIMER
;*****
```

```
TIM_COMP:  in status_save, SREG
           sbrc status, 0
           rjmp TIM_SENDING
           sbrc status, 3
           rjmp TIM_START_SEND
           rjmp TIM_RECEIVE
```

TIM\_SENDING:

```
dec txwait
brne TIM_RECEIVE
tst txcnt
brne TIM_SEND_BIT

cbr status, 1 ;stop bit sent, clear 'sending' bit
rjmp TIM_RECEIVE
```

TIM\_SEND\_BIT:

```
dec txcnt
lsr txreg ;move actual bit into carry flag
in tim_temp, PORTB
brcs TIM_SEND_ZERO
or tim_temp, active_output
out PORTB, tim_temp ;send one
ldi txwait, 8
rjmp TIM_RECEIVE
```

TIM\_SEND\_ZERO:

```
com active_output
and tim_temp, active_output
com active_output
out PORTB, tim_temp
ldi txwait, 8
rjmp TIM_RECEIVE
```

TIM\_START\_SEND:

```
;*****starting send
cbr status, (1<<3) ; clear start send flag
sbr status, (1<<0) ; sending flag
mov txreg, txchar
com txreg
ldi txwait, 9
mov txcnt, txwait
ldi txwait, 8
in tim_temp, PORTB
com active_output
and tim_temp, active_output
```

```

        com active_output
        out PORTB,tim_temp ; send start bit (logical 0)

;*****receive
TIM_RECEIVE:
        in tim_temp,PINB
        and tim_temp,active_input
        sbrc rxstat,0x0 ; are we receiving?
        rjmp tim_rec
        tst tim_temp ;start bit detected (zero)?
        breq tim_start ;jump to start receive
        rjmp tim_ret

TIM_STOP:
        tst tim_temp ;check stop bit
        brne tim_rec_ok
        cbr rxstat,1
        or errstat,active_input ;indicate error
        rjmp tim_ret

TIM_REC_OK:
        cbr rxstat,1
        sbr status,1

TIM_OUT_WAIT:
        sbis USR,UDRE ; normally should be empty, only for
        ; security...
        rjmp TIM_OUT_WAIT
        out UDR,rxreg0
        rjmp tim_ret

TIM_START:
        sbr rxstat,1 ;set receive bit
        ldi tim_temp2,9 ;9 incl. stop bit
        mov rxcnt0,tim_temp2
        ldi rxwait0,10
        rjmp tim_ret

TIM_REC:
        subi rxwait0,1
        brne tim_ret
        dec rxcnt0
        breq tim_stop
        com tim_temp
        subi tim_temp,$ff ;generate carry if bit was set
        ror rxreg0
        ldi rxwait0,8 ;wait 8 cycles

TIM_RET:
        out SREG,status_save
        reti

;*****
; RESET / Initialization
;*****
RESET:
        ldi temp,low(RAMEND)
        out SPL,temp ;init Stack Pointer

;***** Init PORTB
        ldi temp,0b10100110 ;(1 = output)
        out DDRB,temp
        ser temp ;start bit is zero, so go to one
        out PORTB,temp

```

```

;***** Init UART
    ldi temp, (1 << TXEN) | (1 << RXEN) | (1 << RXCIE)
    out UCR, temp
    ldi temp, (frequency / (16*baud)) - 1
    out UBRR, temp

;***** Init Timer
    clr temp
    out TCCR1A, temp          ; disconnect OCl and no PWM
    ldi temp, 0b01001        ; select CK/1 and clear counter on match
    out TCCR1B, temp
    clr temp
    out OCR1AH, temp
    ldi temp, freq_divi      ; RS232 sample frequency
    out OCR1AL, temp
    ldi temp, (1 << OCIE1A)
    out TIMSK, temp          ; enable compare match interrupt

;***** Select output
    ldi active_output, (1 << out0)
    ldi active_input, (1 << in0)

;***** Clear stati (for debugging, otherwise should be zero)
    clr infofunc
    clr status
    clr rxstat
    clr status_save
    clr errstat
    clr txcnt                ; 'not sending' indicator
    dec txcnt                ; txcnt = 0xFF

;*****
;                               RESET / Main
;*****

    clr ZH                   ; always leave ZH zero
    clr YH                   ; always leave YH zero
    sei

MAIN:
    tst infofunc
    brne SHOW_INFO
    rjmp MAIN

SHOW_INFO:
    mov temp, infofunc
    cpi temp, '?'
    breq show_version
    cpi temp, 's'
    breq show_status
    showMessage MSG_ERROR
    clr infofunc
    rjmp MAIN

SHOW_VERSION:
    showMessage MSG_INFO
    clr infofunc
    rjmp MAIN

```

```
SHOW_STATUS:
    ldi  yh,8
    mov  yl,errstat
STATUS_LOOP:
    sbic USR,UDRE
    rjmp SEND_STAT
    rjmp STATUS_LOOP

SEND_STAT:
    lsl  yl
    brcc STAT_0
    ldi  temp,'1'
    rjmp STAT_SHOW

STAT_0:
    ldi  temp,'0'

STAT_SHOW:
    out  UDR,temp
    dec  yh
    brne STATUS_LOOP
    clr  infofunc
    clr  errstat

STATUS_LOOP2:
    sbic USR,UDRE
    rjmp SEND_RET
    rjmp STATUS_LOOP2
SEND_RET:
    ldi  temp,$0d
    out  UDR,temp          ;send 0D

    rjmp MAIN
```

---