DEVELOPMENT OF A WIRELESS TRANSMISSION MODULE FOR MODBUS APPLICATIONS

A THESIS SUBMITTED TO

THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

OF

ATILIM UNIVERSITY

BY

OSMAN TÜRKKAN

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR

THE DEGREE OF MASTER OF SCIENCE

IN

THE DEPARTMENT OF ELECTRICAL AND ELECTRONICS ENGINEERING

MARCH 2008

GCRIS

Approval of the Graduate School of Natural and Applied Science of Atılım University

Prof. Dr. Abdurrahim ÖZGENOĞLU

Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science/Arts.

Asst. Prof. Dr. Ali KARA

Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science/Arts.

Asst. Prof. Dr. Ali KARA

Supervisor

Examining Committee Members

Asst. Prof. Dr. Ali KARA ______________________

Asst. Prof. Dr. Mehmet Efe ÖZBEK ______________________

Assoc. Prof. Dr. Veysel GAZİ ______________________

GCRIS

ABSTRACT

DEVELOPMENT OF A WIRELESS TRANSMISSION MODULE FOR MODBUS APPLICATIONS

Türkkan, Osman

M.S., Electrical and Electronics Engineering Department

Supervisor: Asst. Prof. Dr. Ali Kara

March 2008, 66 pages

RF Modules find many applications areas in industrial control systems. This thesis aims to analyze design and implementation of an RF module. This study presents the system architecture, the design of the RF module, the communication performance and the estimated cost in detail. Simplicity and low-cost design are the main objectives. The challenges and problems in the design and implementation phases are described and solutions are proposed. Various RF module design examples and comparisons are outlined.

There are two scenarios for testing of the system. These are implemented on a two-point network and their performance is measured in field trials. The test results which are also included in this thesis reveal the system overall performance.

Keywords: Wireless Data Communication, Modbus Protocol, RSSI, RF Module

ÖZ

MODBUS UYGULAMALARI İÇİN KABLOSUZ MODÜL GELİŞTİRİLMESİ

Türkkan, Osman

Yüksek Lisans, Elektrik - Elektronik Mühendisliği Bölümü

Tez Yöneticisi: Yrd. Doç. Dr. Ali Kara

Mart 2008, 66 sayfa

RF modülleri endüstriyel kontrol sistemlerinde pek çok uygulama alanları bulmaktadır. Bu tez çalışmasında RF modül tasarımı ve uygulaması analiz edilerek gerçeklenmiştir. Bu calışma sistem mimarisi, RF modülünün tasarımı, haberleşme performansı ve maliyeti hakkında bilgi vermektedir. Tasarım aşamasında basitlik ve düşük maliyet göz önünde tutulmuştur. Uygulama problemleri açıklanarak çüzümleri sunulmuştur. Çeşitli RF modul tasarımları örneklenmiş ve karşılaştırılmıştır.

Sistemin denenmesi için iki senaryo uygulanmıştır. Bunlar iki noktalı ağ topolojisinde denenmiş ve performansları saha testleriyle ölçülmüştür. Bu tez çalışmasının içeriğinde de olan test sonuçları sistemin toplam performansını ortaya çıkarmıştır.

Anahtar Kelimeler: Kablosuz Bilgi Aktarımı, Modbus Protokolü, RSSI, RF Modül

ACKNOWLEDGMENTS

I wish to express my gratitude to my supervisor Asst. Prof. .Dr. Ali KARA for his guidance, advice, comments, insight and invaluable contributions throughout the research.

GCRIS

TABLE OF CONTENTS

GCRIS

GCRIS

GCRIS

LIST OF TABLES

GCRIS

LIST OF FIGURES

LIST OF ABBREVIATIONS

RTU	:	Remote Terminal Unit
ISM	:	Industrial, Scientific and Medical
ASCII	:	American Standard Code for Information Interchange
CRC	:	Cyclical Redundancy Check
PRS	:	Pseudo Random Sequence
UART	:	Universal Asynchronous Receiver Transmitter
DSSS	:	Direct Sequence Spread Spectrum
GFSK	:	Gaussian Frequency Shift Keying
FSK	:	Frequency Shit Keying
ASK	:	Amplitude Shit Keying
OOK	:	On-Off Keying
GOOK	:	Gaussian On-Off Keying
MSK	:	Minimum Shift Keying
IF	:	Intermediate Frequency
LOS	:	Line of Sight
NLOS	:	None Line of Sight
LAN	:	Local Area Network
RF	:	Radio Frequency
USB	:	Universal Serial Bus
SRAM	:	Static Random Access Memory
CPU	:	Central Processing Unit
OEM	:	Original Equipment Manufacturer
HVAC	:	Heating, Ventilation, and Air Conditioning
MMDS	:	Multi-channel, Multi-point Distribution System
LMDS	:	Local Multi-point Distribution System
MAC	:	Media Access Control
IP	:	Internet Protocol

WPAN : Wireless Personal Area Network

PID : Proportional, Integral, Derivative

PWM : Pulse Width Modulation

SNR : Signal to Noise Ratio

BER : Bit Error Rate

ISI : Inter Symbol Interference

RSSI : Received Signal Strength Indicator

ZigBee : This is the name of a specification for high level communication protocols using small, low-power digital radios based on the IEEE 802.15.4 standard for WPANs.

Throughput: This is the amount of digital data per time unit that is delivered to a certain terminal in a network from a network node or from one node to another in communications networks. The throughput is usually measured in bps.

CHAPTER 1

INTRODUCTION

Modbus is a wired serial communication protocol published by Modicon in 1979 for a multi-point network based on master/client architecture [1]. Modbus standard is flexible, and its implementation is easy. Therefore, Modbus is adapted by many manufacturers. Because of this, Modbus became the first widely accepted fieldbus standard. It allows communication between many devices connected to the same network. Many intelligent devices like micro-controllers, PLCs and sensors equipped with a Modbus interface are able to communicate with Modbus and send their data to the master system.

Each device intended to communicate using Modbus is given a unique address. Any device can send out a Modbus command. A Modbus command contains the Modbus address of the device it is intended for. Only the intended device will act on the command, even though other devices might receive it.

All Modbus commands contain checking information, ensuring that a command arrives undamaged. The basic Modbus commands can instruct an RTU (remote terminal unit) to change a value in one of its registers, as well as commanding the device to send back one or more values contained in its registers.

The physical layers of the Modbus interface are RS232 and RS485. There are also standards for wireless communications and TCP/IP over Ethernet networks.

Long range data transmission has been a serious problem for many industrial applications. Nowadays, traditional approaches such as wired transmission networks are neither efficient nor applicable. With the advent of low-power data transmission, using wireless link needs to be examined in terms of cost, installation and system flexibility. At site, where cable installation is difficult or not applicable, penetration capability of RF energy through walls might be a good solution.

ISM (Industrial, Scientific and Medical) bands between 900 MHz to 5.8 GHz are commonly used; however, national authorities have defined different specifications for its licence. They differ in the number of allocated RF channels, their bandwidth and maximum RF power.

The range is limited within a few hundreds of meters. In our country, the allowable operation specs for the long range are frequencies of 869 MHz with a maximum transmitter power of 500 mW and 434 MHz with a maximum transmitter power of 10 mW.

The low-power RF module is a good alternative to wire over short and medium ranges. When the cost of an RF module is compared with that of data cabling and communication with many control points, this comparison emphasizes an RF module’s low-cost installation and physical flexibility.

In this study, our motivation was to investigate the feasibility of an RF module for several industrial applications using Modbus.

1.1 SCOPE OF THE THESIS

The main topic is to transfer small data through wireless channel using Modbus Protocol at point-to-point topology. In this thesis, it is aimed to design a portable RF module, which is low-power and low-cost, and examine its performance for commercial purposes.

GCRIS

This study aims to design a system which uses unlicensed data transceivers in the 900 MHz band and employs Modbus communication protocol depending on the required data collection rate and accuracy.

Two wireless RF modules provide a wireless interface between two points. Modules communicate using a master-slave technique where the master initiates transactions called queries. Slave responds by supplying the requested data to the master or by taking the action requested in the query. Each of the slaves or clients follows the master and transmits the data only when allowed to by the master. Before communication is established, each module is configured either as a master or as a slave.

Before achieving a satisfactory performance, various problems have been encountered and solutions have been provided. Our experiments have shown that it is possible to design a reliable RF module. To implement the system, the RF module has been designed and produced.

The structure of the thesis is as follows: Chapter 2 presents literature survey. Besides, background information about Modbus protocol and wireless data communication are given and a requirement analysis is presented in Chapter 2. In Chapter 3, RF board design and implementation of the RF module are explained. Details of the RF module and its implementation are described in Chapter 3. Chapter 4 describes the results of the tests. The system performance is examined in Chapter 4. In the light of the tests results as mentioned in Chapter 4, conclusion and future work are emphasised in Chapter 5.

CHAPTER 2

BACKGROUND INFORMATION AND LITERATURE SURVEY

2.1 MODBUS AND MODBUS PROTOCOL

2.1.1 Modbus Protocol and Message Structure

The Modbus communication interface is built around messages whose format is independent of the type of physical interface. For RS232 or RS485; the Modbus messages are sent over the network which is dedicated to Modbus. For more versatile network systems such as TCP/IP or wireless; these are embedded in packets with appropriate format. The main Modbus message structure is based on peer-to-peer network. However, Modbus is able to function on both point-to-point and multi-point networks [1].

The message structure shown in Table 2.1 has four elements in the same structure. In the Modbus network, a master module starts the communication. A master sends a message with address and the targeted slave takes action and responds to it. The other nodes ignore the message because of the mismatch of their address field [1].

Table 2.1 Modbus Message Structure

Field	Description
Device Address	Address of the receiver
Function Code	Code defining message type
Data	Data block
Error Check	Numeric check value to test for comm. errors

2.1.2 Transmission Modes, Addressing and Function Codes

There are two basic transmission modes, which are ASCII and RTU.

In ASCII mode, all messages are coded in hexadecimal and are readable. The main advantage of this mode is to allow time intervals of up to one second between characters without any errors.

In RTU mode, binary coding is used which makes the message unreadable but reduces the size of the message. The main advantage of this mode is that its greater character density allows better data throughput than ASCII for the same baud rate [1].

The address is the first field of the message. This contains one byte address information where valid module addresses are in the range of 1 to 247. A slave receiving a message always responds to the master. Besides, the device with a Modbus interface has an address map where registers, inputs and outputs are assigned addresses as shown in Table 2.2 [1].

Table 2.2 Data Types and Numbers

COIL/REG. NUMBERS	ACTION	DESCRIPTION
1-9999	Read / Write	Output Coils
10001-19999	Read	Input Coils
30001-39999	Read	Analog Input Reg.
40001-49999	Read / Write	Analog Output Reg.

The other parameter is the function code. This defines the message type and action required by the slave. This also contains one byte of information. Valid function codes are in the range 1 to 255 but not all Modbus devices use all of these codes.

The most common codes are listed in Table 2.3.

Table 2.3 Common Modbus Function Codes

Code	Description
01	Read Coil Status
02	Read Input Status
03	Read Holding Registers
04	Read Input Registers
05	Force Single Coil
06	Pre set Single Register
07	Read Exception Status
15	Force Multiple Coils
16	Pre set Multiple Registers
17	Report Slave ID

2.2 WIRELESS DATA COMMUNICATION

There are certain radio frequencies in electromagnetic spectrum that you can use without a license in most countries. These bands are generally referred to as ISM bands. The ISM bands are defined by the ITU-R (International Telecommunication Union) in 5.138 and 5.150 sections of the Radio Regulations. Individual countries' use of the bands designated in these sections may differ due to variations in national radio regulations [2].

In recent years, ISM bands have also been shared with license-free error-tolerant communications applications such as wireless LANs (Local Area Network) and Bluetooth.

ISM band applications and max. power rates:

902 to 928MHz

- Spread spectrum 1 W
- Microwave ovens 750 W
- Industrial heaters up to 100 kW
- Military radar up to 1000 kW

2.4 to 2.4835GHz

- Spread spectrum 1 W
- Microwave ovens 900 W

5.725 to 5.850GHz.

- Spread spectrum 1 W

A very typical example is the 2.4 GHz band where Wireless LAN systems defined in standards like IEEE (Institute of Electronic and Electrical Engineering) 802.11; 802.11b and 802.11g are operating around. For instance, IEEE 802.11b/g wireless Ethernet operates on the 2.4 GHz band.

2.2.1 Wireless Communication Specifications

The relationship between the transmitted and the received power is expressed by the path loss [2]. The propagation in air (free space) is categorized in two forms LOS (line of sight) and NLOS (non line of sight). LOS corresponds to a clear transmission path between the transmitter and the receiver. The satellite communications are given as an example of LOS case. In NLOS case, communication relies on reflection, scattering and/or combination of them. Transmitted electromagnetic waves loose energy while travelling to the receiver. The higher the frequency of transmission, the quicker they will lose energy. Higher frequency waves also lose energy quicker when they are penetrating walls, trees, or other obstructions. For example, if a 900 MHz radio and a 2.4 GHz radio have the same output power and receive sensitivity, and when they are compared side by side, the 900 MHz radio gets almost twice the range of the 2.4 GHz radio.

Transmit power output has a direct correlation to the range and amount of data that a radio system can have. The more power is transmitted from the radio modem, the further your data reaches.

Moreover, the difference in range varies with respect to the environmental conditions and the amount of signal that is absorbed by the different obstacles. In order for electromagnetic waves to propagate the greatest distances, the waves need to travel through as few obstacles as possible. Dense obstacles such as concrete, brick or other heavy construction will inhibit signals more than light obstacles such as a few trees or a simple post.

When trying to increase the range, several factors including antenna height, frequency, antenna type and power output should be considered. The antenna makes the wireless communication more efficient by focusing the transmitted energy. When selecting antennas, it is important to consider factors such as transmit frequency, antenna type and the installation environment. Antennas are tuned to operate at a specific frequency, so proper communication will depend on selecting an antenna. The type of antenna depends on the application, but multiple antenna types can be used in the same wireless network as long as they are operating at the same frequency. The most common type of antenna is the half-wave omni directional dipole. The antenna height allows the signal to travel above obstacles and also reduce any interference from the ground. Since directional antennas can focus energy, they increase the range in fixed installations.

The typical ranges obtained for different output power and different environments are listed in Table 2.4. The listing shows that although electromagnetic waves can pass through objects, allowing for NLOS communication, obstacles absorb a portion of the signal greatly reducing the effective communication range. For example, 1 mW output power at 2,4 GHz has a 30 m range for NLOS and 100 m for LOS.
The industrial applications such as waste water treatment, power management and control, flood control and lighting control are examined and results are shown in Table 2.4. These ranges were recorded when 2.1 dB gain antenna was used [2].

Table 2.4 Power Output and Range

Power Output	Frequency	NLOS (Urban Range) / LOS (Outdoor Range)
1 Watt	900 MHz	Up to 900 m / up to 22 km
125 mW	900 MHz	Up to 300 m / up to 3.2 km
100 mW	900 MHz	Up to 450 m / up to 11 km
4 mW	900 MHz	Up to 100 m / up to 300 m
100 mW	2.4 GHz	up to 100 m / up to 1.6 km
50 mW	2.4 GHz	up to 180 m / up to 5 km
1 mW	2.4 GHz	up to 30 m / up to 100 m

Greater ranges can be achieved by optimizing some variables and parameters. When designing a RF communication system, the list of variables in Table 2.5 should be considered [2]. These variables affect the system's range and can be manipulated to optimize the system performance.

The receiver sensitivity indicates the minimum signal level which is required at the antenna terminals so as to provide reliable communications. It depends on receiver design, modulation format and transmission rate. Low power consumption is maintained in the wireless data communication system by employing greater receiver sensitivity. The receiver sensitivity is the lowest power level where the receiver can detect an RF signal and demodulate it to set the data. The sensitivity is a receiver specification and is independent of the transmitter. As the signal propagates away from the transmitter, the power density of the signal decreases while the distance between the receiver and the transmitter increases. It is more difficult for the receiver to detect the signal.

The overall link margin of the wireless data communication system includes transmission power output, antenna gain, receiver sensitivity and path loss (due to cable and antenna attenuation, air content and obstacles preventing LOS conditions). Achieving long range with wireless transceiver modules requires an effective combination of output power, antenna gain and receiver sensitivity. Each of these specifications plays an important role in the link budget of a wireless link path.

Table 2.5 Range Variables

Range Variable	Range Reducers	Range Enhancers
Receiver Sensitivity	Poor Receiver Sensitivity --> 6 dB halves the range in LOS outdoor environments --> 10 dB halves the range in urban/indoor environments	Excellent Receiver Sensitivity --> 6 dB doubles the range in LOS outdoor environments --> 10 dB doubles the range in urban/indoor environments
	Sensitivity is a measure of the minimum power level at which the receiver is able to detect the RF signal and demodulate the data.	
Transmitter Power	Low Transmit Power --> 6 dB halves the range in LOS outdoor environments --> 10 dB halves the range in urban/indoor environments	High Transmit Power --> 6 dB doubles the range in LOS outdoor environments --> 10 dB doubles the range in urban/indoor environments
Antenna Gain	Low Gain	High Gain
Antenna Cable	Long Antenna Cable	Short Antenna Cable
Fresnel Zone (The environment between transceivers)	Physical Obstructions (walls, trees, buildings, etc.)	No Physical Obstructions between transmitter and receiver
	10 m antenna height achieves 500% more range than 2 m height. The first Fresnel zone is taken free of obstructions which means the transmission is acceptable under the free space conditions.	
Radio Frequency Interference	Interference such as Cell phones, Microwave ovens, Pagers, etc.	Interference-free environment
Data Rate	High Data Rate --> Doubling the data rate can reduce range by 29%	Low Data Rate --> Halving the data rate can increase range by 29%
Frequency	High Frequency --> 2.4 GHz frequency systems will have approximately ½ the range of 900 MHz systems	Low Frequency --> 900 MHz frequency systems will have approximately 2x the range of 2.4 GHz systems

Many applications require compact size, portability, low power consumption and low cost from wireless data communication solutions. Improving receiver sensitivity has proven to be a cost effective means for increasing range without the overhead for power and antenna solutions that are difficult to use.

2.2.2 Transceivers: Types and Specifications

When the range, low power consumption and low cost are critical to the wireless data communication system, finding a transceiver solution providing greater receiver sensitivity is important. Whereas transmission obstructions and interference may be encountered in different environments, some wireless transceivers are designed to penetrate obstructions and block interference to acceptable levels. These abilities allow wireless data communication systems to be more flexible than wired systems when used in portable applications.

The design method of wireless communication module is based on general principles of designing a communication system. It is characterized by using the block diagram of an internal data flow presented in Figure 2.1.

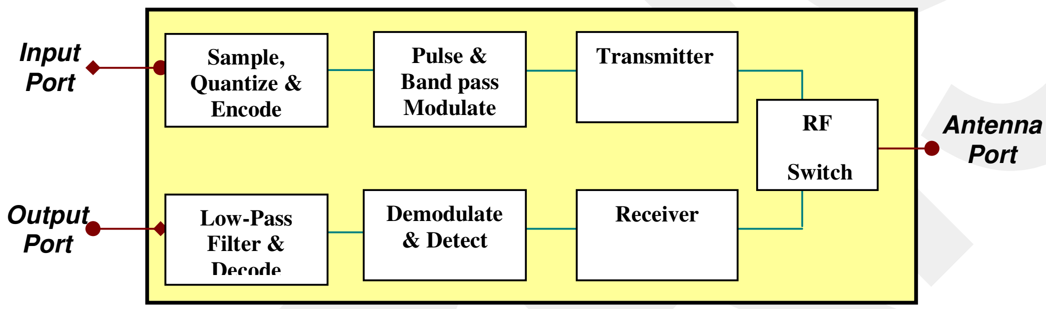

Figure 2.1 Internal Data Flow Diagram

In this figure, the input information source is converted to binary digits, the bits are grouped to form digital symbols [3]. According to our information sources, different a formatting process is applied. For a digital input, this is a sequence of binary digits called bit stream. This form is suitable for the base band processing.

An analog input is formatted using three separate processes, which are sampling, quantization and coding [3]. The sampling process is usually implemented using a sample/hold circuit. The result of the sampling process is PAM (Pulse Amplitude Modulation) signal.

After the quantization process, the PAM signal will be compatible with digital system. PCM (Pulse Code Modulation) signals are obtained from the quantized PAM signals. Each quantized sample is digitally encoded into codeword bits. This codeword map attributes to frequency or phase values in the baseband modulation process. These digits are transmitted through a baseband channel by means of a coaxial cable and represented compatible waveforms. A voltage level assigns to each bit as “0” and “1”. The aim of digital base band modulation is to transfer a digit bit stream over a low pass channel.

In bandpass modulation process, this pulse waveform is modulated by high-frequency carrier waveform, resulting in that the equivalent low pass signal is frequency shifted to a modulated passband signal or RF signal. To avoid harmonic distortion and periodic spectrum, amplification and analog band pass filtering are applied (pulse shaping).

An example of baseband to passband operation is FSK where the waveforms used to represent a 0 and a 1 bit differ by exactly half a carrier period. This is the smallest FSK modulation index that can be chosen such that the waveforms for 0 and 1 are orthogonal. This sinusoidal wave is sent to the transmitter channel. An RF connection is initialized and the RF data is sent.

A received RF signal suffers from ISI (inter-symbol interference) and noise due to the channel effects. The noise, which is produced by electronic components and circuits, is called thermal noise and cannot be eliminated. The primary spectral characteristic of thermal noise in communication systems, which is two-sided power spectral density, is the same and flat for all frequencies of interest. When the noise power is characterized by a constant-power spectral density, it is called as white noise. The thermal noise characteristics, AWGN (Additive, White and Gaussian Noise), are used to model the noise in the detection process and in the design of receivers.

In demodulation process, a received bandpass waveform is transformed to a base band waveform. Demodulation process consists of a receiving filter, an equalizing filter and a sampler. The receiving filter is to recover a baseband pulse with the best possible signal to noise ratio (SNR), free of any ISI. The equalizing filter is used to compensate for channel distortion caused by both the transmitter and the channel.

After a received signal has been transformed to a sample, the shape of the waveform of the signal is not important. All waveform types are transformed to the same value of a Gaussian random variables, z(T) which are identical for detection process. The decision making process is applied the waveform in detection process. z(T) has a voltage value proportional to the energy of the received symbol. Therefore, the larger the magnitude of z(T), the more error free the decision making process will be.

A detector minimizes the error probability using some threshold levels. It is known as a maximum likelihood detector. The amplitudes of the waveforms are detected and the mapping is created using the nearest allowed values of the amplitudes. In this way, the received signal is transformed to the bit stream at the end of the detection process and a discrete version of information is obtained. For an analog type of information, the bit steam is decoded and sent to a low pass filter so as to remove any error correction codes in formatting process [3].

Some wireless transceiver modules offer additional interference rejection or blocking, which are achieved the use of proper filtering and communication. Standard speeds that are commonly used are: 110, 300, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 and 2764800 bit/s.

In order to reduce the cost, many manufacturers combine a separate transmitter and receiver into one package (chips or chipsets). This allows common modules to be shared between the transmitting portion and the receiving portion. Generally the chipset is installed with an antenna board.

Wireless transceiver modules contain the chips/chipsets that allow at all levels of RF experience to integrate a complete wireless system into products. Many modules are manufactured as a drop-in solution where designers create a compatible pin-out on their processor board and supply serial data to the appropriate pins.

The serial data can either be sent in a full duplex or in a half-duplex mode. In full-duplex communication, data can be sent and received at the same time. In half-duplex communication, data can be both sent and received, but not at the same time. RF communication typically runs in a half-duplex configuration. If an application requires that data be transmitted and received in a full duplex, it is possible to simulate full-duplex communication by setting the interface baud rate slower than the RF baud rate and setting a few parameters, appropriately [4].

In a radio transceiver, the receiver is silent while transmitting. An electronic switch allows the transmitter and receiver to be connected to the same antenna and prevents the transmitter output from damaging the receiver. With this kind of transceiver, it is impossible to receive signals while transmitting. This is half duplex mode. Transmission and reception often are done with the same frequency.

Some transceivers are designed to allow reception of signals during transmission periods. This is full duplex mode. The transmitter and receiver operate on different frequencies so the transmitted signal does not interfere with reception. For example, cellular and cordless telephone sets use this mode. Satellite communications networks often employ full-duplex transceivers at the surface-based subscriber points.

We have explored various transceiver types designed for different applications. There are several types of transceivers. For example [5];
--Low power, zero-IF RF transceiver operating in frequency bands of 433 MHz to 464 MHz and 862 MHz to 928 MHz is integrated FSK/GFSK modulation mode.
--Low power, low-IF RF transceiver operates in frequency bands from 433 to 464 MHz and 868 to 928 MHz. Data rates supported are 0.3 to 200 kbps. It operates on a +2.3 V to +3.6 V power supply.
--High performance, FSK/ASK transceiver has an anti-interference performance and is designed for operation in 135MHz to 650MHz at 200 kbps.
--High performance, Narrowband ISM transceiver operates in the 80 MHz to 650 MHz and 862 MHz at 25 kbps.

At the design phase, the main parameter is generally the output power which can be adjusted by the modulation scheme e.g. FSK, GFSK, ASK, OOK. Wireless systems mostly employ FSK for high-data-rate applications. FSK systems exhibit good capture performance but require continuous transmission of the carrier signal, which increases the power consumption of the transmitter. GFSK reduces the bandwidth occupied by the transmitted spectrum by digitally pre-filtering the Tx data. ASK is implemented by switching the output stage between two discrete power levels. OOK is implemented by switching the output stage to a certain power level for a high Tx data bit and switching the output state off for a zero. GOOK represents a prefiltered form of OOK modulation. The sharp symbol transitions are replaced with smooth Gaussian filtered transitions [6]. In FSK/GFSK modulation mode, the output power is independent of the state of the data I/O pin. In ASK/OOK modulation mode, it is dependent on the state of the data I/O pin and the polarity of the Tx data input.

According to the specifications listed above, important parameters are low-power, high data rate and operating frequency for our study. While choosing a transceiver for our module at design phase, FSK modulation mode is considered.

Chipset groups are easily distinguished by other characteristics such as digital and analog I/O capacity, SRAM, Flash RAM, speed and system resources which are important for the application. Table 2.6 shows the general capacity of these characteristics.

Table 2.6 Chipset Characteristics

Digital I/O	**Analog In.**	**Analog Out.**	**Amount of SRAM**	**Amount of Flash**
up to 64 points	up to 48 points	up to 4 points	up to 2 KB	up to 32 KB

2.2.3 Topology and Networking

A wireless transmission system is a system that enables the interconnection of access points wirelessly. As described in IEEE 802.11, it allows a wireless network to be expanded using multiple access points without the need for a wired backbone to link them.

An access point is either a main relay or a remote base station. A main base station is connected to control point by wiring. A relay base station relays data between remote base stations, wireless clients or other relay stations. A remote base station accepts connections from wireless clients and passes them to relay or main stations. Connections between clients are made using MAC addresses rather than by specifying IP assignments. All base stations in a wireless transmission system is configured using the same radio channel.

The wireless transmission system is also referred to as repeater mode because it appears to bridge and accept wireless clients at the same time. It is noted that throughput in this method is inversely proportional to the number of hops, as all traffic uses the same channel.

In most communication systems, it is desirable for data not only to reach the destination, but also to arrive in a reliable and consistent manner. In general, wireless communications tend to be subject to more interference and lost data than a wired system. Because radio frequency transmission causes more errors, some sort of protocol and packing of data are usually used to help ensure data integrity and make sure the data safely arrives at the destination.

The most known modes of data transmission, which are built-in features that aid with reliable data transmission, are enumerated below [7]:

<u>Point-to-point Topology</u>: A point-to-point network is one of the forms of wireless network, composed of two stations and antennas in direct communication with each other. Point to point links are used to provide high performance, dedicated connections or high speed interconnected links. These links are deployed quickly but do not easily scale to create a large network. This kind of network access is very well suited for use in multi-point applications using any protocol in which addressing is built into the data to be transmitted.

<u>Point-to-multipoint Topology (LMDS)</u>: A point to multipoint or a multipoint to point nodes share the link between an uplink node and repeater nodes. This type of network is easier to deploy than point-to-point network because adding a new subscriber only requires equipment deployment at the subscriber site.

Multipoint-to-multipoint Topology (MMDS): This kind of networks creates a routed topology that mirrors the structure of a wired network.

Mixed node Topology: This network is the complex form of wireless network, composed of two stations and antennas in direct communication with each other and a third party wireless bridge or repeater. Mixed nodes are used to provide high performance, dedicated connections or high speeds interconnect links. That indoor unit is a low cost product is one of most important advantages of this kind of topology.

Ad-Hoc Topology: This is a wireless computer network. Each node is willing to forward data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. Such network scenarios cannot rely on centralized and organized connectivity. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks.

2.2.4 Maximizing Range in Wireless Systems and Antenna Considerations

The transmit power, the receiver sensitivity, the antenna replacement and the frequency should all be considered in a wireless communication system. These parameters, which are important factors for achieving long-range performance, are chosen according to the site conditions. A protocol should be developed to allow for graceful recovery from data corruption and reliable delivery of the information.

Whatever the conditions are, performing site tests in the actual environments help to set performance expectations during the design phase of the system. In order to maximize the range in field tests, these parameters are to be controlled as follows.

Maximizing the receiving sensitivity is influenced by several factors. One of them is the tuning crystal which is the accuracy of the reference frequency, which is significant because there are two or more remote devices attempting to operate with each other in a tight bandwidth. To ensure that all intended devices operate as desired, each device is accurately tuned to a known reference frequency. The module gets this reference frequency from a crystal oscillator circuit. Frequency deviation or error from the desired reference frequency is measured in parts per million (ppm). For a 13 MHz ref. frequency, a 1 ppm error translates into 13 Hz [8].

Another factor is the supply voltage. Both transmit power and receive sensitivity increase as the system voltage increases. Current consumption also increases. The transmit strength is increased by up to 1 dBm and the receiver sensitivity is improved by up to 1 dBm for total improvement of 2 dBm when comparing a 2.7V with 3.6V systems. This total increases in transmit and receive performances and also increases the operating range of the system [8].

The supply voltage noise is also another factor. High-frequency noise, which is in the supply voltage, injects noise into the sensitive receiver path of the module, which degrades the overall sensitivity of the receiver. To minimize this effect is used either a linear voltage regulator with low noise characteristics or a boost converter with low-pass filter. The addition of an external band-pass filter to the receive path effectively increases the range.

Antenna type, its orientation and impedance matching are also very important to increase the performance of wireless system.

Various error correction techniques are used to improve the receive sensitivity such as coding gain, minimizing payload size and error concealment.

Maximizing the transmit power is related to the amount of the energy which radiates from the antenna of the transmitting device. In addition to the factors mentioned above, the internal and external power amplifiers are also efficient ways to maximize the transmit power but there are some regulations that limit the power ratio. The maximum allowable output power is 1 Watt for our country. This is considered before the hardware cost.

The last major subject is to minimize the path loss, which is defined as the attenuation of the radio signal. Some factors increase the path loss such as device enclosures and obstacles in the operating environments. Metal enclosures affect the wireless performance. The operating environment is important to determine the range of a radio system. Proximity of other objects in the operating environment contributes to degrading the range.

Using single antenna reduces the receive sensitivity and the path loss. To achieve the maximum range, separate transmit and receive antennas are used. Besides, using long antenna cable reduces the performance because antenna cables add loss to the system. The antenna gain is another important parameter that can be adjusted so as to increase the range. It describes the amount of focus the antenna is able to apply to the system by directing the energy. For example; omni directional antennas focus energy in a nut shape around the antenna. Directional antennas focus energy more in one direction. Each application has different antenna requirements as determined by the desired transmit distance, LOS conditions and network architecture. There are various options for antennas with trade-offs of cost, size and performance.

Quarter-wave antenna pattern is shown in Figure 2.2, which requires a ground plane [9].

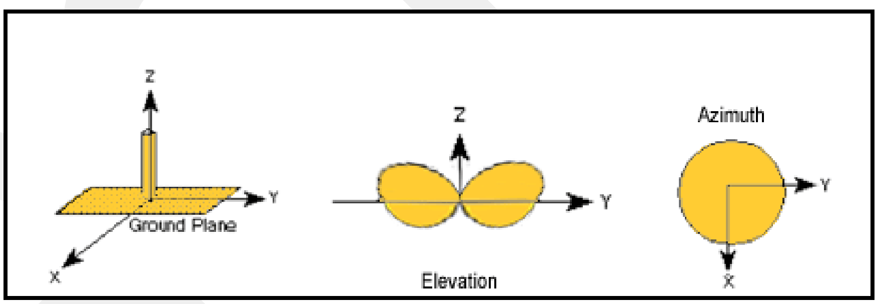

Figure 2.2 Monopole Radiation Patterns [9]

Half-wave antenna pattern is shown in Figure 2.3, which is made up of two quarter-wave length elements [9]. The gain they provide promotes a greater omni-directional transmission range than quarter-wave antennas. Half-wave antennas do not require a ground plane.

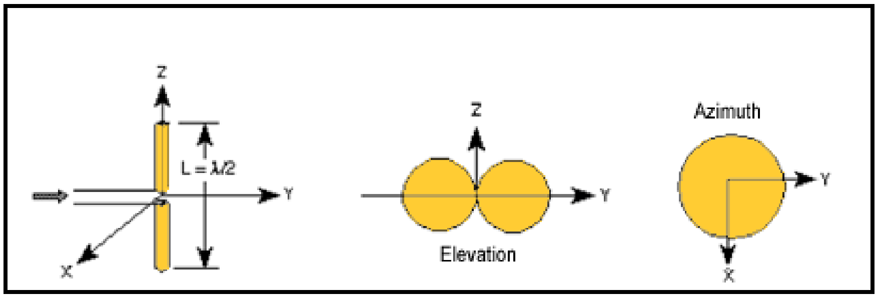

Figure 2.3 Dipole Radiation Patterns [9]

Antennas with higher gain focus the energy over a smaller area. High gain antennas are limited to use in extending the range in a NLOS environment. In a NLOS environment the obstructions contribute more losses to the system.

Moreover, the high gain antenna has a narrower beam width. The multi various angles effects of a NLOS environment cause the signals arriving at the antenna at odd angles after reflecting off nearby objects. A lower gain antenna with a larger beam width is better at collecting the bounced signals. A metric combining antenna gain and transmit power is ERP (Effective Radiated Power). It is the sum of antenna gain and transmit power in dB. For example; if a system has two 2.1dBi omni-directional dipole antennas at both ends. By replacing a high gain antenna instead of one of them the overall system gain increases 12dBi [9].

On the other hand, when low-cost is important, omni-directional antenna is considered. Cost table of RF module is given in the next chapter.

2.2.5 Transceiver Modules and Their Applications

Several manufacturers design RF solutions. Some of their modules are compared in Table 2.7 [2], [10], [11], [12].

Table 2.7 Device Comparison Table

Module Type	Data Rate	Range	Frequency – MHz	Power Out-mW
X2010 / X2011	20 kbps	300 m LOS	434, 868 and 914	10
X8000	4800 to 9600 bps	1 to 3 km NLOS, 10 to 20 km LOS	130 to 180 380 to 500 860 to 960	5 to 1000
9Xtend	115 kbps	900 NLOS, 22.000 LOS	900 MHz	1000
9XStream	19.2 kbps	450 NLOS, 11.000 LOS	900 MHz	100
9XCite	38.4 kbps	100 NLOS, 300 LOS	900 MHz	4

Fields of application:

OEM Serial Communication, Data Acquisition, Access Control, Remote Metering, Electronic Message Signs, Domestic and commercial wireless security systems, Remote control for cranes, Robotics, The short range transceivers are suitable for automatic meter reading, Industrial Automation, alarm and security systems, home automation systems, remote controls and other wireless network & telemetry systems, Military and government applications, Remote weather stations, Trucks and other vehicles providing data for fleet management, Home utility meters for automatic meter reading, Lighting and irrigation control systems, Wireless keyboards, Handheld Terminals, HVAC, Escalators & Elevators, Electronic displays, Data loggers and a host of other applications.

The design process starts with the application specifications and requirements analysis. The design criteria are established then the performance requirements are inferred from the application requirements [13].

2.2.6 System Requirements

The survey conducted has been informative in determining the basic limits necessary for the RF module designed to be able to complete with its rivals in the market. This research, which is done to design a module that can address different industrial application needs, has revealed the system requirements clearly. As a result of this survey, which is done prior to the design stage, with the aim of determining the basic requirements, they are enumerated as below:

1- Long range communication. It is a part of important criteria while choosing the transceiver. Table 2.7 clearly illustrates the limits related to this requirement.
2- Low cost. It is an important part of the competition in trade.
3- Data transmission rate. At that point, there is a restriction. It depends on the transceiver supplier specs in the local market.
4- Reliable data transferring. It is important for critical applications. These systems relay on the power of the programming.
5- Maximum achieved data rate which reflects data collection rate.
6- Antenna. As mentioned in Chapter 2.2.4, while maximizing range, type of antenna is considered. Besides; low-cost antenna is also considered.

Furthermore, our system requires the communication modules to operate in many types of environments such as, outdoor, indoor buildings constructions. These are also other important considerations.

According to these requirements, board design criteria are determined as follows:

1- Output power and frequency. As mentioned in Chapter 2.2.1, to ensure long range communication, these parameters have the highest priority.
2- Transceivers. These were examined according to output power, frequency, data rate and modulation type, in Chapter 2.2.2.
3- Chipset. In order to ensure compatibility of Modbus protocol, its programming is important. It is examined in the next chapter.
4- The component availability in local markets. This item is important to have low-cost module.
5- Module size. Avoiding electromagnetic interference between RF transceiver and other components is an important point, which affects the module size.
6- Topology. As mentioned in Chapter 2.2.3, this is another important consideration, because module test scenario is determined according to the topology.

Local manufacturers and suppliers are examined for that purpose. The board design is done according to these considerations.

CHAPTER 3

RF BASE BOARD DESIGN AND IMPLEMENTATION

Board designed for Modbus applications will be described in this Chapter. Design procedure and production phase of the board will be explained in Section 1 and detailed board features will be defined in Section 2. Emulation models used and software will be introduced in Section 3. Implementation details are discussed in Section 4.

The simplicity and low cost of the system are the main objectives. The data link has been implemented with low-cost RF modules. As mentioned in Chapter 2, for our study, an important constraint is the RF modules implementation which is limited to FSK narrow band modulation. This causes lower transmission rates.

Because of multi-path fading, to operate on ground-to-ground wireless link varying propagation path loss is the other constraint. Vegetation and topographic structure are considered while testing [14].

3.1 DESIGN AND PRODUCTION PROCEDURE

Design of a PCB board begins with the system requirements and the selection of the parts appropriately. RF module expectations are determined at the beginning of the design phase. As mentioned in Chapter 2, our main design criterion is long range. As a result of our survey, the RF part which was designed and supplied by UDEA was chosen to achieve long range. Key parameters are given in Appendix A. Its specifications are suitable for our requirements as mentioned in Chapter 2.2.6. This module also supplies small data transferring. Moreover, its cost is examined in the next sub-chapter.

Another expectation is compatibility of Modbus protocol of RF module as mentioned in Chapter 2.2.6. CY8C27443 was chosen as a chipset. Its parameters are given in Appendix B and its specifications are examined in the next sub-chapter.

To control the RF signal performance is the other expectation. For this purpose, hardware requirements are two digital inputs and outputs and one RS 485 interface. These are also examined in the next sub-chapter.

The board has two main parts, which are an RF part and a base part. A commercial schematic design program has to be used to construct a schematic design of the board and layout of the PCB. A schematic design shows pin connections between parts and additionally shows ground and power connections of the board parts. When schematic design is completed, PCB board layout showing places of the integrated circuits (ICs) and passive elements such as resistors, capacitors on the board and connections between them are created. At the end of this process, the manufacturing files, called Gerber files, are created. These files are sent to the PCB producer for the production. After the PCB production, components are connected on the board and tests are performed.

The schematic design layout has been prepared by using a commercial schematic design program PCB design tool with selected components. These components were a RF module, a chipset, two regulators, a RS485 driver and four transistors. The board size was not considered in this first design so as to ensure enough space between the RF module and the other components to minimize the interference, because this study intends to develop a prototype that would be further improved for commercial purposes later.

The baseboards are built on 10x19 cm size with a 5 cm separation between RF module and other components. This arrangement, which is recommended by RF module manufacturer [15], protects electromagnetic interference shielding of sensitive RF parts from noisy digital circuitry. Test results showed that this approach worked well.

In order to use different control signals digital I/O pins and a serial data port are designed. The RF module power consumption is related to the rates of transmission. Our module consumptions are min. 40 mA for 5 Vdc, min. 600 mA for 3 Vdc. The protocol is based on asynchronous characters transmission with specific coding. Each data packet consists of multiple characters.

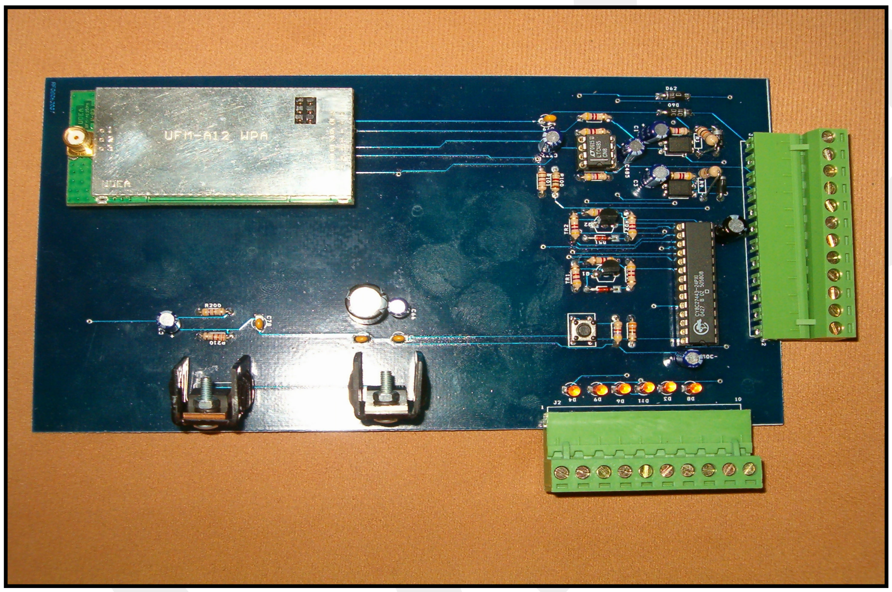

Figure 3.1 Designed RF Module

3.2 DETAILED BOARD FEATURES

The block diagram and picture of the designed RF module are shown in Figure 3.1 and Figure 3.2. In this board, an UFM-A12WPA RF module and a CY8C27443 chip were used. Two forms are considered for the incoming data; digital and analog. Serial and digital data enter the board through an RS485 driver and digital input pins.

The transceiver section controls the data transfers between the nodes. Its RF input and output terminals are connected to an antenna.

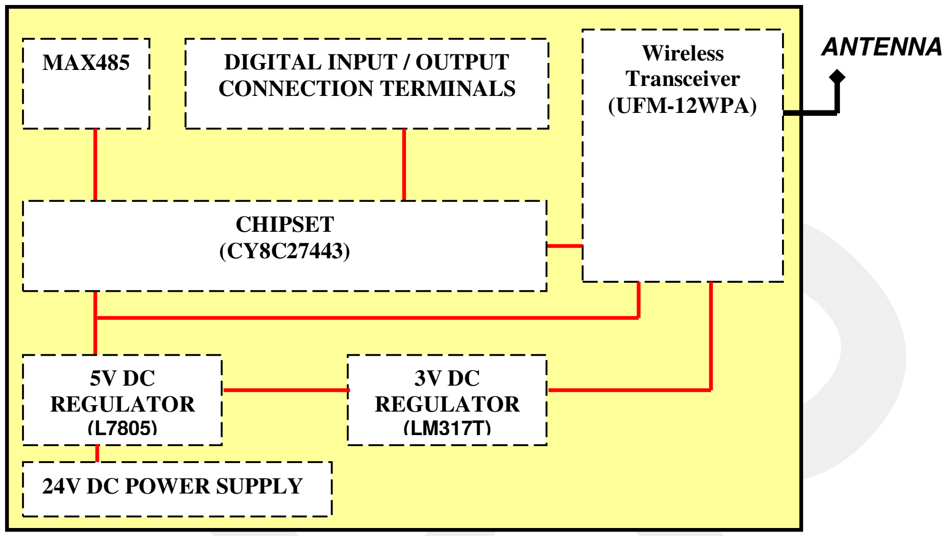

Figure 3.2 Block Diagram of The Board

In our transceiver, Frequency Shift Keying (FSK) modulation method, where the modulating signal shifts the output frequency between predetermined values, was used [15].

The design characteristics of each of these components provide the proper transport functions for the information content. The information throughput and the channel bandwidth are also critical parameters in determining which modulation scheme to be used for the system.

The chipset operates in five modes: Idle, Transmit, Receive, Sleep and Command.
In idle mode, there is no data transfer.

In the transmitter mode, TX buffer register is used. The first byte of serial data is received from the UART and the master module initiates an RF connection with the slave. This is the channel initialization that synchronizes the slave with the master modules sending an RF initializer. After transmission is completed, the master returns to idle mode. The RF initializer contains channel information. Its lengths depend on the amount of time required to prepare a receiving mode for the slave.

Similarly, in the receiver mode, RX buffer register is used to ensure data stream. The slave detects RF data while operating in idle mode. Unless the valid RF data is detected in the slave, the module stays in idle mode.

There are two formats supported for the transmitter and receiver modes: a) A 10-bit frame size including one start bit, eight data bits and one stop bit or b) an 11-bit frame size including one start bit, eight data bits, one parity bit and one stop bit.

The sleep mode enables the module to enter the state of low-power consumption. There are three kinds of sleep modes: pin, serial port (weak on serial port activity) and cyclic (wake on RF activity). In the sleep mode, the module does not transmit or receive data until the first transitions to the idle mode. These sleep modes can be enabled and disabled by using a programming command.

In the command mode, the module parameters are modified and read using programming port. The achieved data rate is 2.4 Kbps with 27dBm output power. The data speed is limited to less than 9.6 Kbps [15]. One of the disadvantages of narrow band communication is to achieve high-speeds in communication, since the receiver bandwidth is narrow. The other one is that a narrow band RF module comprises discrete components, thus cost is higher and size is bigger than a wide band RF module.

We used a half-duplex RF narrow band transceiver at 869.4336 MHz. The transmission ranges of narrow band and wide band device are different. Narrow band refers to a channel, which occupies only a small amount of space on the radio spectrum and the channel is sufficiently narrow and its frequency response can be mostly considered flat in practice. The merit of narrow band communication is to realize stable long range communication. In addition, the carrier purity of transmission spectrum is very good; therefore it is available to manage an operation of many radio devices within the same frequency bandwidth at the same time. In other words, it leads to a high efficiency use of RF wave within the same frequency band. Narrow band communication is the optimal in solution sites where many RF equipment are used, such as construction sites or industrial plants.

The components referred above are preferred because of availability in the market and also the cost. The components used and their specifications are discussed in the following sections.

3.2.1 Specifications of UFM-A12WPA RF Module

The RF Module is manufactured according to the ERC Recommendation on Short Range Device (SRD) standards at 869.4336 MHz ISM Band and affords Original Equipment Manufacturers (OEM) and integrators an RF solution. The module transfers a standard asynchronous serial data stream between devices [15]. Wiring diagram which applied while implementing RF module is shown in Figure 3.3. Serial data transfers were done throught Tx and Rx terminals. Terminal 1 and 2 were used for 3 V power supply. Specifications are given in Appendix A.

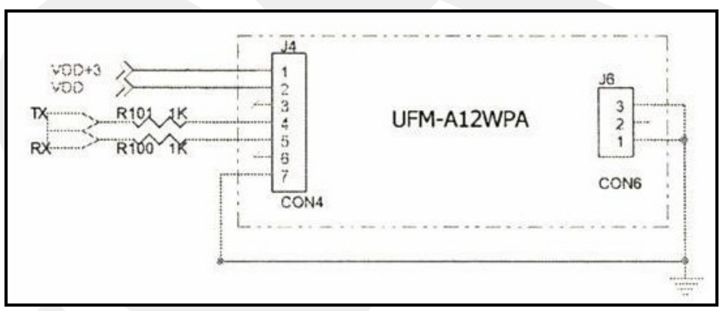

Figure 3.3 Wiring Diagram of UFM-A12WPA RF Module

3.2.2 Specifications of Base Board

Features of the baseboard and components are explained in details in the following sub-sections.

3.2.2.1 CY8C27443 Chipset

CY8C27443 was chosen as a low power processor and it draws low current [16]. I/O point capacity and local market availability was considered in choosing this device.

The block of the chipset diagram is shown in Figure 3.4.

There are eight sections in the chipset. All these sections are configured with several different function sets and communications among them provided by a network of the system bus. The programming phase enables us to control all of them.

The flash memory section contains module configuration and address, integer and floating-point constants, program code. Besides it stores the initial values of the data.

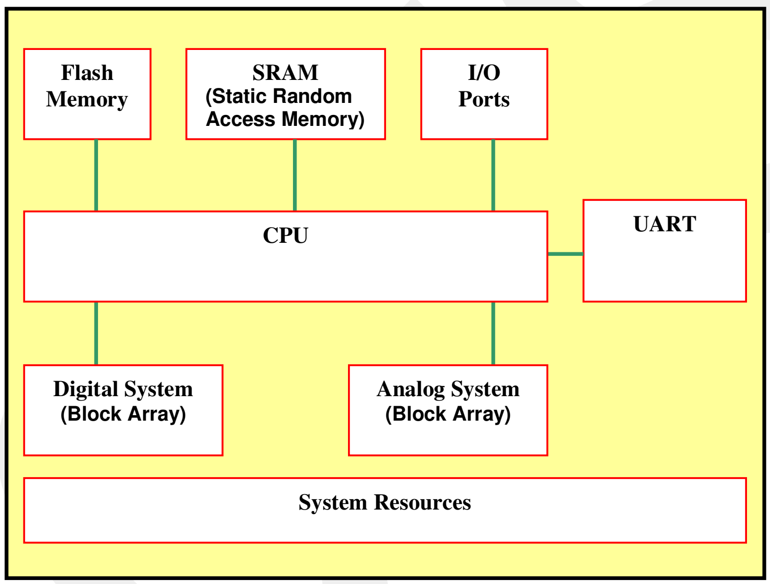

Figure 3.4 The Chipset System Building Blocks

The SRAM section contains data memory area, which includes temporary variables used by C compiler, C global variables and C definitions.

In the I/O Port section, discrete and analog type data can be supplied to the module. By this way, controlling of several parameters such as run-stop, open-close and PID is possible. The I/O capacity is selectable.

There are two types of digital blocks: basic and communication. Modules such as an UART is placed in communication blocks, a PWM is placed in basic block [16]. Analog blocks are user configurable system resources. Each of analog blocks has many potential inputs and outputs. The inputs include analog signals from external sources, which are analog signal driven from analog blocks or various voltage reference sources. The analog output bus is an analog bus resource that is shared by all of the analog blocks.

Some functions, which are enumerated below, operate the capacity of the analog blocks: Analog-to-Digital Converters, Digital-to-Analog Converters, Analog Comparators, Low-Pass Filter, Band-Pass Filter, FSK modulator etc. By modifying these registers, some benefits are gained as follows: cost affectivity, flexibility and functionality [16].

The CPU section involves a microprocessor, which can be selectable processor clock speed from 93,7 kHz to 24 MHz. It has five internal registers that are used in program execution [16].

The System Resources include an USB port, a digital clock, a system reset, an internal voltage reference, an IO Analog multiplexer, a serial interface. Specifications are given in Appendix B.

Wiring diagram which applied while implementing RF module is shown in Figure 3.5. Discrete type inputs were assigned PRT0-1 and 2-1 and outputs were assigned PRT0-0 and 2-0. In order to ensure communication between module and a computer, RS485 connections were made using pin no 17-18. Tx and Rx terminals were connected to UFM-A12WPA transceiver. VDD indicates 5 V power supply. J3 was used to reset the cipset. To control data exchange, RSENABLE input was used.

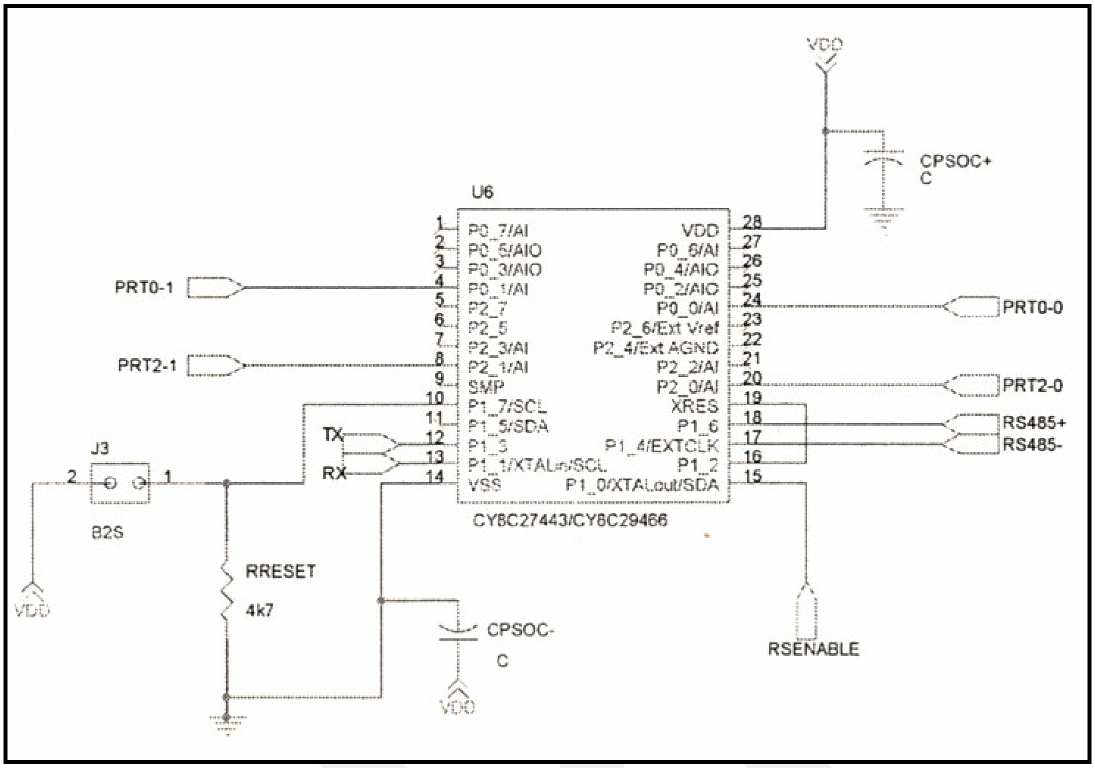

Figure 3.5 Wiring Diagram of CY8C27443 Chipset

3.2.2.2 MAX485

The MAX485 is low-power transceiver for RS-485 and RS- 422 communication. Each part contains one driver and one receiver. The driver slew rates of the MAX485 is not limited, allowing that to transmit up to 2.5Mbps. This transceiver draws between 120µA and 500µA of supply current when unloaded or fully loaded with disabled drivers. All parts operate from a single 5V supply. Driver is short-circuit current limited and is protected against excessive power dissipation by thermal shutdown circuitry that places the driver outputs into a high-impedance state.

Pin arrangement of MAX485 is given in Appendix C. The receiver input has a fail-safe feature that guarantees a logic-high output if the input is open circuit.

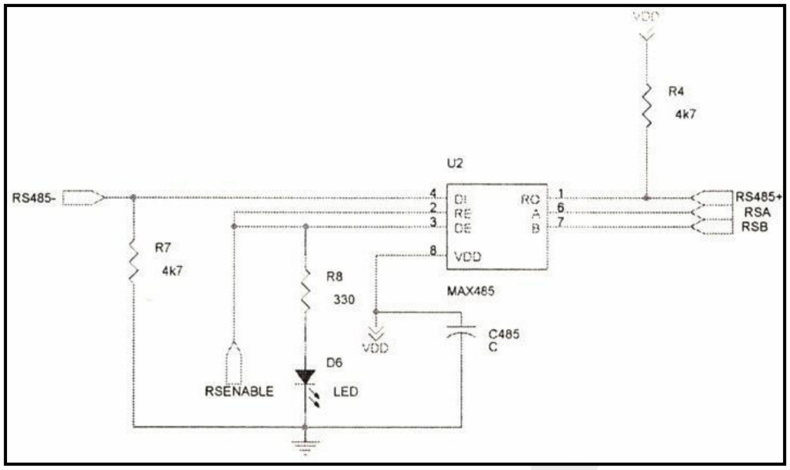

Figure 3.6 Wiring Diagram of MAX 485

The MAX485 is designed for half-duplex applications. It is used for data logging to control module performance. Besides, communication between the baseboard and a peripheral such as a PC, a device with Modbus protocol ensures by means of this component. The MAX485 will be used for future studies. Wiring diagram which applied while implementing RF module is shown in Figure 3.6.

3.2.2.3 Power Management

The board is powered by 12 to 24V dc power supply unit. For 5V regulation, L7805 (Positive Voltage Regulator) was used. This output is used for CY8C27443 power supply voltage, UFM-A12WPA RF module and MAX485. For 3V regulation, LM317T (Adjustable Voltage Regulator) was used. 3V output is used for UFM-A12WPA RF module. Electrical characteristics of these regulators are given in Appendix D.

3.2.2.4 Digital Inputs And Outputs

The board has 2 digital inputs and outputs for control signals as mentioned in Chapter 3.2. The input voltage level is 24V dc. In order to transfer an input signal to CY8C27443 chip, PS 2501-1 (High Isolation Voltage Single Transistor) was used. Wiring diagram which applied while implementing RF module is shown in Figure 3.7.

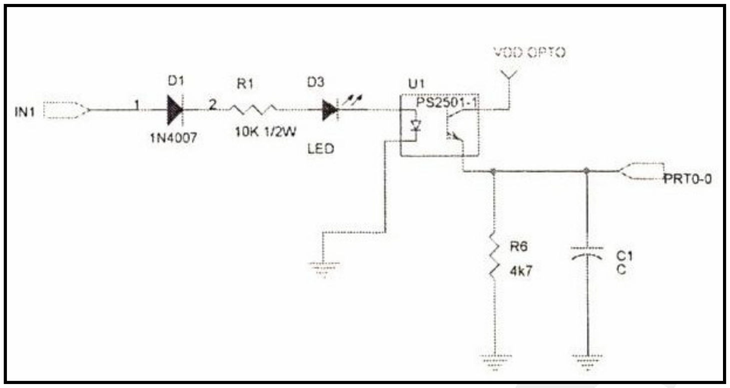

Figure 3.7 Wiring Diagram of PS2501-1

The output voltage level is 24V dc. In order to transfer an output signal to an output terminal, BC237C (Amplifier Transistor NPN-Silicon) was used. Wiring diagram which applied while implementing RF module is shown in Figure 3.8. Electrical characteristics of these transistors are also given in Appendix E.

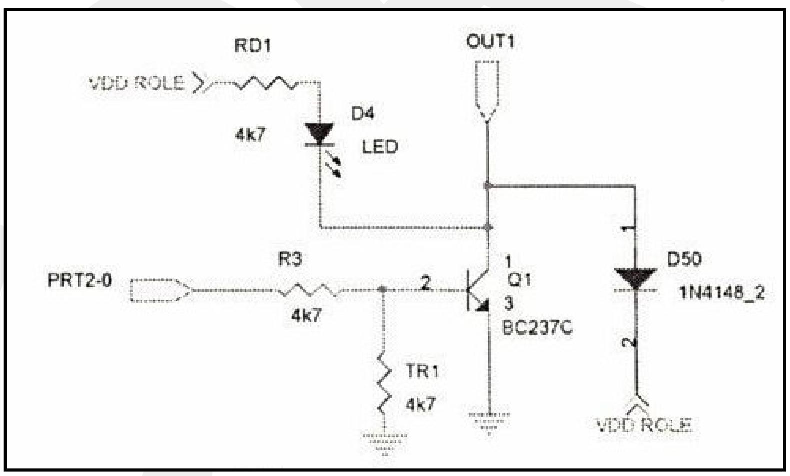

Figure 3.8 Wiring Diagram of BC237C

3.2.2.5 Cost

Table 3.1 gives approximate total cost for a PCB board.

Table 3.1 Price of Components and PCB Production in US Dollars

Name	Qnt.	Unit Price	Total Price
CY8C27443	1	6,10	6,10
MAX485	1	2,97	2,97
L7805	1	1,21	1,21
LM317T	1	1,50	1,50
UFM-A12WPA	1	94,44	94,44
BC237C	2	0,09	0,18
PS2501-1	2	0,30	0,60
Passive Elements	1	3,00	3,00
PCB	1	8,00	8,00
Component Placement	1	4,00	4,00
TOTAL	-	-	122,00

The total cost of the system is 122,00._$. This figure satisfies our expectation as mentioned in Chapter 2.2.6. The production cost for the first PCB is 400._$. Because of this, PCB is considered for volume production only.

Moreover, this production cost has to be added to the cost of an antenna. As mentioned in Chapter 2, the cost changes according to the type of the antenna. For example, UGPA Antenna is low-cost omni-directional antenna and its cost is 13,33._$. This has to be added to the cost of each board.

3.3 SOFTWARE IMPLEMENTATION

3.3.1 UFM-A12WPA RF Module

The communication subsystem is divided in three layers: Application, security subsystem and physical [17]. The application layer is the highest protocol layer and its functionality depends on the system application. Different applications can be implemented depending on the topology. In our case, the broadcast addressing system was implemented, and application layer consisted Modbus transmission frame There are three restrictions over the structure of the applications:

Small packet size: Application layer determines small data size, because the wireless link is a few bits length. Our data length is 72 bytes.

Identical packets: Identical packets are transmitted when acknowledge message is not received by the master module. This transmission is done according to the number of retry in the program.

Missing packets: Some packets could be missing, so the packets must be decipherable without any knowledge of other packets that have been previously transmitted.

The security subsystem layer provides confidentiality and data integrity. The physical layer adapts the packet and generates the levels to be transmitted over the radio link. The low bit rate is determined by the utilization of low cost RF module. Manchester encoding is not necessary, because the bandwidth used can be reduced to the half and the bit rate can be higher. Besides, the physical layer inserts the flag bytes when it acts as transmitter or extracts them when it acts as receiver. These flags are used to synchronize the transmitter with the receiver.

The data frame is shown in Table 3.2. Start of frame is used for channel initializing. It indicates starting of RF data. In this way, receiver is notified for communication request coming from the transmitter. Following data consists of RF data whose length is 72 bytes. Modbus data, as mentioned in Chapter 2, are written in this field. End of frame indicates ending of RF data. LF (Line Feed) and CR (Carriage Return) are control codes which are used to verify that the RF data has not been corrupted. Start and end frame structures are designed by the supplier. These are not modified or changed by the user. RF data frame is modified for Modbus communication by us.

Table 3.2 Structure of Data Frame

$	R	F	DATA	E	N	D	CR	LF
24h	52h	46h	BYTE (Max. 72 Byte)	45h	4Eh	44h	0Dh	0Ah

Start of Frame ($, R, F) — Data Frame (DATA) — End of Frame (E, N, D, CR, LF)

There are several error codes such as overflow, time out and format error. When the user enters data larger than 72 bytes, the module executes an overflow error message shown in Table 3.3.

Table 3.3 Structure of Overflow Error Frame

$	C	O
24h	43h	4Fh

Time out check time refers to the duration of the waiting time for the master module until the send sequence is initialized. When there is a gap between data sequences longer than 500 ms, the module executes a timeout error message shown in Table 3.4. This parameter was used for our RF module transmitting sequence.

Table 3.4 Structure of Timeout Error Frame

$	C	T
24h	43h	54h

When the data structure is different from that described in Table 3.2, the module executes a format error message shown in Table 3.5.

Table 3.5 Structure of Format Error Frame

$	C	E
24h	43h	45h

RSSI (Received Signal Strength Indication) is a measurement of the received radio signal strength. RSSI is used to determine when the amount of radio energy in the channel is below a certain threshold at which the card is clear to send (CTS). Once the card is clear to send, a packet of information is sent.

The end-user can observe an RSSI value when measuring the signal strength of a wireless network through the use of this message structure. RSSI measurements vary from 10 to 67. This is useful in determining range of RF module under various conditions. It consists of a one-byte integer value. A value of 10 indicates the minimum signal strength detectable by the card.

RSSI frames are shown in Table 3.6 and Table 3.7. This parameter was used to measure our RF module range performance. Related results are given in next chapter.

Table 3.6 Structure of RSSI Request Frame

$	C	R
24h	43h	52h

Table 3.7 Structure of RSSI Response Frame

$	C	10 to 67
24h	43h	0Ah to 43h

3.3.2 Base Board

The software implementation is examined within two parts debugging – emulation and software – programming.

3.3.2.1 Debugging and Emulation

The PSoC Designer Debugger provides in-circuit emulation support that allowed us to test the project with the ICE-4000 in a hardware environment while viewing and debugging device activity in a software environment. For these purposes, PsoC IEC-4000 In-Circuit Emulator was used [18]. This kit employs all necessary tools and programs with auxiliary accessories.

Figure 3.9 PSoC IEC -4000 Emulator [18]

This PSoC Development Kit shown in Figure 3.9 includes an In-Circuit Emulator (ICE), which consists of a base unit, USB 2.0 cable, and power supply. The base unit is connected to the host PC via the USB port. The ICE is driven by the Debugger subsystem of PSoC Designer. This software interface allows the user to run, halt, and single program installation to the processor. Besides, different Emulation Pods are available. They plug into the user's circuit board to provide the physical interface.

Development Kit includes;

- Image Craft C-Compiler License
- ICE-Cube Unit
- 28 pin PDIP Emulation Pod for CY8C27*43-24PXI
- 28 pin CY8C27*43-24PXI PDIP PSoC Device Samples
- PSoC Designer Software CD
- ISSP Cable
- MiniEval Socket Programming and Evaluation board
- Universal 110/220 Power Supply (12V)
- European Plug Adapter
- USB 2.0 Cable

C Compiler is integrated into the PSoC Designer software, which supports C source level debugging. The program developed was installed and run using this kit. Some modifications were done while getting best result about coupling between RF module and the chipset.

3.3.2.2 Software and Programming

Addition to the things mentioned in Chapter 3.3.1, some registers were created by us so as to use for software implementation. Some command descriptions are listed below:

Module Address:

This command was used to read the source address of RF module. Module address was assigned at the beginning of transmission.

Tag Name: MA

Parameter range: 0 – 20h

Number of Byte: 1

Destination Address:

This command was used to set the address of slave RF module. This module listens to all transmissions to stay synchronized, but not send any data.

Tag Name: DA

Parameter range: 0 – 20h

Number of Byte: 1

Received Packet Counting:

This command was used to set/read the count of received RF packets. Each ACK message increased this counter. The maximum value is manually reset.

Tag Name: PC

Parameter range: 0 – FFFFh

Number of Byte: 2

Retry Counting:

This command was used to set/read the count of retried RF packets. Each timeout command increased this counter. The maximum value is manually reset.

Tag Name: RC

Parameter range: 0 – Fh

Number of Byte: 1

GCRIS

<u>Transmit Command:</u>

This command was used to set/read the transmit/receive behaviors of RF module.
Tag Name: TX
Parameter range: 0
Number of Byte: 1

<u>Failure Counting:</u>

This command was used to report the number of transmission failures. The number of this counter indicated how many packets were not successfully received. Each overflow of retry counter command increased this counter. The parameter is not non-volatile and is manually reset to zero.
Tag Name: FC
Parameter range: 0 – FFFFh
Number of Byte: 1

PSoC Designer is the software interface for configuring and programming analog- and digital-peripheral functionality into a PSoC device. Inside the interface, the user can select and place user modules, write C and/or Assembly source, and debug and program the project.

PSoC Designer contains three subsystems: Device Editor, Application Editor, and Debugger.

Device Editor

Device Editor subsystem of PSoC Designer is where chip hardware is configured. We have selected, placed, configured, and connected our modules (peripherals) and set global parameters such as CPU_Clock, 32K_Select, PLL_Mode etc. Then we have established chip pin-out and port characteristics and generated the project configuration files.

Device Editor is used after a project is created and before source is written in the Application Editor subsystem. All of them are done prior to debugging and programming which are the parts in the Debugger subsystem.

GCPIS

Our project was designed according to CY8C27443 chipset. Two UARTs were used: one for RF transmission other for RS485 interface. A part of the configuration page is shown in Figure F.1 in Appendix F. The suitable connection was made according to the wiring drawing.

Application Editor

Application Editor subsystem of PSoC Designer is the component in which all source-code programming (editing and adding files) takes place. We have completed configuring the user's device and generating application code and programmed the M8C micro controller.

Application Editor is used after a project is created and is generated in Device Editor. Editing and adding source is the process that precedes debugging, which takes place in the Debugger subsystem.

Debugger

Debugger subsystem sets breakpoints and watches variables, runs events, programs the part, and emulates the configured functionality of the PSoC micro controller.
Debugger subsystem is used after a project is created and source is written in Application Editor. It is the final step to implement the project.

3.4 IMPLEMENTATION

3.4.1 System Architecture

Conventional topologies, as mentioned in Chapter 2, provide wireless communication between nodes. Depending on coverage requirements and customer preferences, communication is provided through digital wireless communication links or a combination of these topologies. Besides; the wireless digital networks provide long range and the lowest cost solution, but the coverage that they provide is limited [19].

Our system is based on point-to-point topology. Each node provides a wireless link between them. This system corresponds to tele-command applications where a master sends orders to a client. The packet is transmitted and the client response is expected in a specific time interval. Two way communication design is significant where these systems have the capability to request the retransmission of lost or corrupted data packets [20]. During the packet reception, a timeout mechanism is activated for checking the packet integrity.

According to our requirements as mentioned in Chapter 2.2.6, two cases were planned to test our module performance at two different environment conditions. Case 1 was planned to measure the range performance of RF module by taking RSSI values.

Other requirements are data rate and reliable data transfer. To check the performance of RF module according to these parameters, Case 2 was planned in indoor environments. For reliable data transfer performance, the test was done without retries and with acknowledgements enabled. Moreover, achieved or collected data rate were examined in terms of several data transmission rates, a period of the transceiver on/off time and the number of transmitted bytes. Measured values were saved in RF module memory as mentioned in Chapter 3.2.2.1. Besides, the master module was also connected to a computer. As mentioned in Chapter 3.2.2.2, these data were collected and saved in it by means of a MAX485 transceiver.

Case 1: The master module was located in the roof of a building and the mobile client was in a car. The system provided two-way messaging between modules. This technique is limited to power supply battery lifetime of the client module. One bit size packets were sent to the slave module by the master module. Acknowledgement messages from the slave were listened at the master module side. These signals were logged into a computer. The aim of this case is to check the range performance of the RF module. The test detail is explained in field tests section.

Case 2: The master module was installed in a central control room. The client module was located in the other two story building which was 450 m away from the master module. There was no direct line of sight between the two points. Seventy-two bit size packets were sent to the slave module by the master module. Acknowledgement messages from the slave were listened at the master module side.

These signals were logged into a computer and the ratio of these signals were examined. In this way, reliable data transfer performance of RF module was tested.

Moreover, to examine data collection rate, two different configurations were done. Firstly, seventy-two bit size packets were sent to the slave module by the master module and receiving signals were logged into a computer at the slave side. Then, one bit size packets were sent to the slave module by the master module and receiving signals were logged into a computer at the slave side. Acknowledgement messages were not expected for both tests. The test detail is also explained in field tests section.

3.4.2 Hardware Setup

3.4.2.1 RF Base Board

The data was transmitted using a half-duplex RF narrow band transceiver at 869.4336 MHz. Transmission parameters were 2.4 Kbps, 8-bits, 1 start bit, no parity and 1 stop bit. Constraints over the transmission data rate is because of the RF module specs. For the other parameters, as mentioned in Chapter 2, in RTU mode, the format uses binary coding which makes the message unreadable but reduces the size of the message. Besides, it is compatible with Modbus message structure.

3.4.2.2 Antenna

As mentioned in Chapter 2, factors that affect the performance of the antennas are RF cable length, height of antennas off the ground, obstructions, radiation pattern and gain of the antennas. When designing an RF communication system these factors should be studied well.

A whip antenna is the most common example of a mono-pole antenna, an antenna with a single driven element and a ground plane. The length of the whip determines its wavelength, half-wave and quarter-wave whips.

Vertically mounted antenna causes vertical polarization. Whips are omni-directional antennas and they radiate equally in all directions in a horizontal plane, although they have a conical blind zone directly above them [21].

In our implementation, ground plane ¼ λ whip antennas were used. It has 50-Ω impedance and 2.2 dBi gain. The antenna length is 6 cm. The height of antenna off the ground is 5 cm. The cable is RG58, 50 Ω, coaxial type and the length is 1 m. In our cases, the antenna cable was used. This added some losses to the system.

3.4.3 Software Implementation

Module addresses, configuration parameters and processing algorithms were programmed in C code then installed onto the micro controllers using PsoC IEC-4000 Emulator, and then the system was implemented. The data were collected from the client inputs and they were controlled by the master. The RF block allowed the data rate 2.4 kbps.

Timeout error and frame check were provided for error detection of packets. Eight control bytes were added for one message packet. An automatic packet formatting was performed by our program structure to test the RF link.

Not only to measure RF module performance according to the planned tests as mentioned in Chapter 3.4.1, programming is important for reliable data delivery, data collection and logging as well. In our program, transmissions were addressed to the slave module. The destination address was matched with its own address and then a packet was accepted by the slave. Flow chart for address checking is shown Figure 3.10. As defined in Chapter 3.3.2.2, DA is the destination address, and MA is own address of the module.

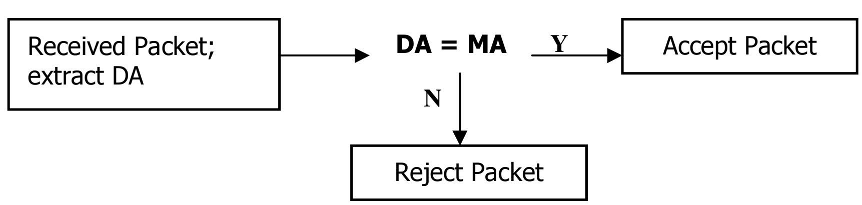

Figure 3.10 Address Recognition

Basic communication was accomplished by checking acknowledge information. Flow chart is shown in Figure 3.11. As mentioned in Chapter 3.4.1, for Case 1 and 2 sequences, main related commands were DA (destination address), RC (retry count), FC (failure count) and timeout checking. When transmission began, data buffer memory was checked to be empty. After initializing channel and assembling packets, packet was transmitted. An RF initializer was sent each time for a new connection sequence in order to ensure synchronizing between the modules. After transmitting a packet, the master module waited to receive an acknowledgement from the slave.

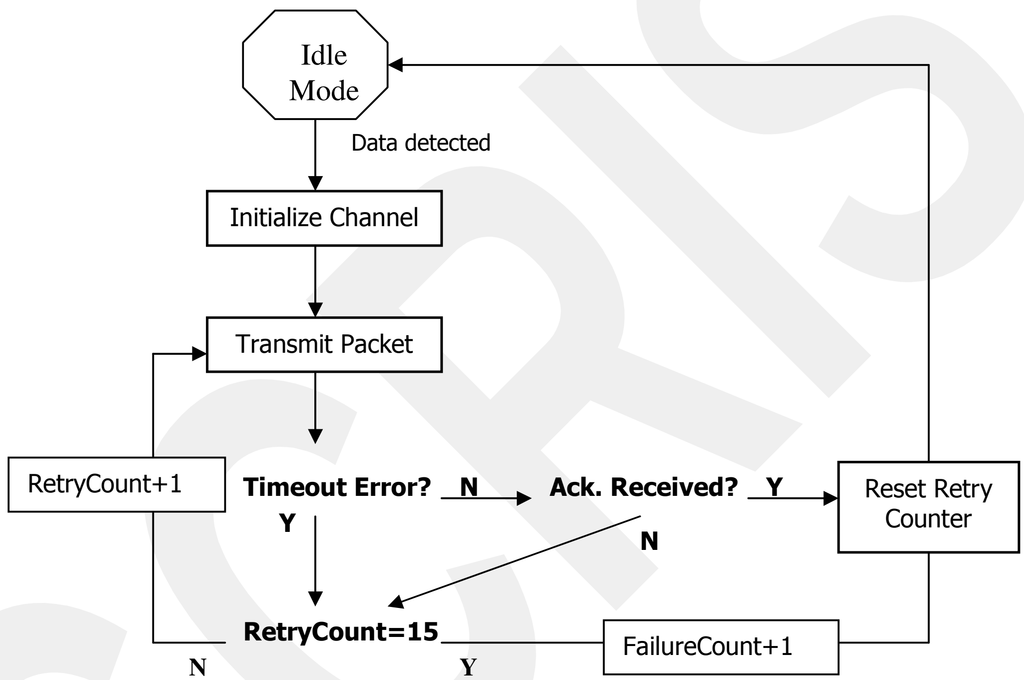

Figure 3.11 Transmission Sequence

When it was received, the master module turned to idle mode. If the acknowledgement was not received in the period of timeout, the original packet was transmitted again. This cycle repeated until an acknowledgement was received or until the packet was sent RC times.

The slave module sent an acknowledge message for each received transmission after checking error frame bit. Then received packet was sent data output buffer and the slave module returned to idle mode. When serial data including requested information by the master module was sent to data input buffer, transmission sequence was started again.

In Case 2, to measure data collection rate, PC (received packet count) command was used. Acknowledgement was not expected by the master module.

Other feature of the system was a log file. Dynamic records of connection and disconnection events, RSSI values were updated. This file including detailed data communication events was used to prepare the test results.

This system does not support remote configuration changing. Each module was based on permanent addressing scheme and functions and run in automatic mode. The changing can be made reinstallation of the new program.

3.4.4 Field Tests

The first case was implemented in an open area. The antenna was installed out of the roof and the connection was done by a cable, which is RG58, 50 Ω, coaxial type and 1 m length. The client was in a car. The power was supplied by a battery group for the module. This supply limited the test duration. It took 20 minutes. Before the test, a specific route was determined in line of sight conditions. It was approximately 2.4 km. The signal strength varied because of the multi path environment. A mixture of direct and reflected signal paths resulted in fading. Therefore, LOS condition was considered taking RSSI measurements.

The second case was implemented inside an industrial area. The master module was installed in a central control room at first floor. The antenna was installed out of the room and the connection was done by a cable, which is RG58, 50 Ω, coaxial type and 1 m length. The power was supplied by an UPS for the module. The client module was mounted on the first floor of a two story building which was far from the master module about 450 m. The client antenna was inside the room. Between these two points, there were a concrete wall and a separate concrete building. The signal went through four walls, in this case.

3.4.5 Performance Issues

As mentioned in Chapter 2.2.6, the range performance, reliable data transmission and the achieved data rate are important for our study. RSSI measurement results give us an idea about the range performance of the RF module.

There are four units of measurement that are all used to represent RF signal strength. These are: mW (milliwatts), dBm ("dB"-milliwatts), RSSI and a percentage measurement. All of these measurements are related to each other, some more closely than others. It is possible to convert one unit to another.

The IEEE 802.11 standard defines a mechanism by which RF energy is to be measured by the circuitry on a wireless network. This numeric value is an integer called RSSI. When the module wants to transmit a packet, it must be able to detect whether or not the channel is clear which means nobody is transmitting.

To evaluate in terms of the achieved data rate within minimal period of time, two equations are considered [22].
For single byte transaction:

$$R_{max} = \frac{1}{\left[Trf + \left(\frac{16}{R}\right)\right] + \left[Trf + \left(\frac{48}{R}\right)\right]} \quad \text{..........} \ (1)$$

For N bytes transaction:

$$R_{max} = \frac{n}{\left[Trf + n\left(\frac{16}{R}\right)\right] + \left[Trf + \left(\frac{48}{R}\right)\right]} \quad \text{..........} \ (2)$$

Where n is the number of bytes, Trf is RF transceiver on/off time and R is RF transceiver data rate.

Our system employed two-way communication depending on the required data collection rate and accuracy. As mentioned in Chapter 3.4.1, behavior of the system under the effects of these parameters were observed. Tests result are examined in the next chapter in detail.

GCRIS

CHAPTER 4

TEST RESULTS

In this Chapter, the performances of the tests for two cases are examined, and in following sub sections, Case 1 and Case 2 test results are given. In the last section, test results are discussed.

4.1 IMPLEMENTATION EXPERIMENTS

Sensitivity is defined as the lowest power level where a receiver can detect an RF signal and successfully demodulate the data. Thus, a receiver with a smaller sensitivity rating will be able to detect weaker RF signal and demodulate the data at an acceptable BER (bit-error rate).

Because the receiver signal strength can vary due to multi-path, interference or other environmental effects, RSSI may not give a true indication of communication performance or range.

Our results and their comparisons were given in the next sub sections. Our study was based on RSSI measurements and the situational analysis for both cases.

4.1.1 Case 1 Performance Test

In this test, as mentioned in Chapter 3.4.1, the master module was located in the roof of a building and the mobile client was in the car and transmission parameters were 869.4336 MHz, 2.4 Kbps, 8-bits, 1 start bit, no parity and 1 stop bit. The range performance of the RF module was tested. The test was done once and its results are given in Figure 4.1.

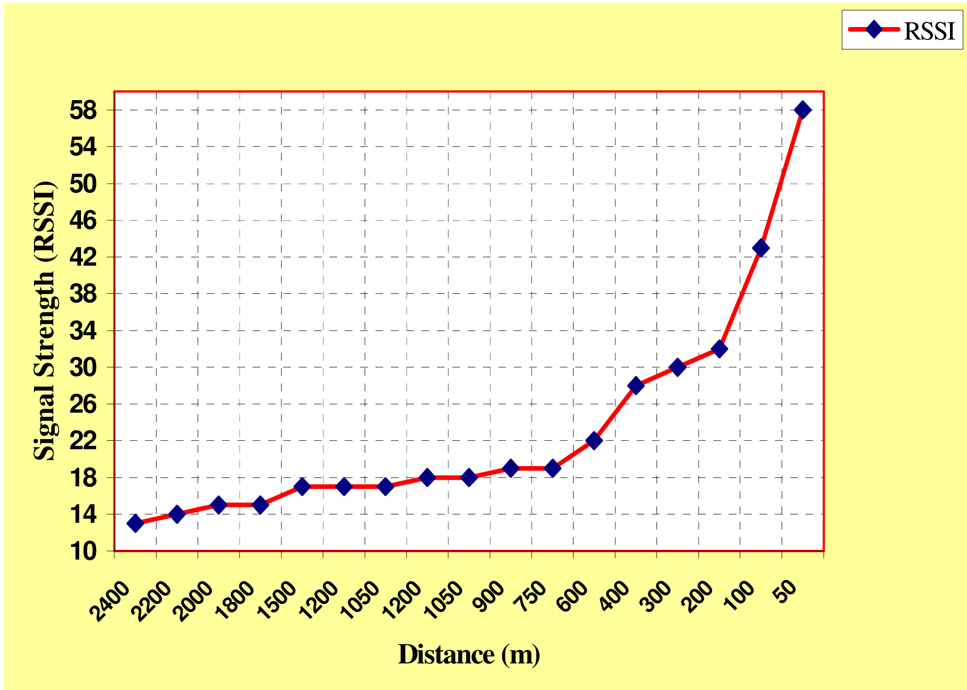

Figure 4.1 RSSI Measurement

On this chart, the measured RSSI values were assigned on the vertical axis and the measured distance between the master and the client in meter values were assigned on the horizontal axis. As seen from the results, the range performance of the RF module for the case was effective up to 2000 m. A sharp rising point occurred at 200 m. Our system works more efficiently between 200 m and 50 m.

4.1.2 Case 2 Performance Test

In this test as mentioned in Chapter 3.4.1, transmission parameters were 869.4336 MHz, 2.4 Kbps, 8-bits, 1 start bit, no parity and 1 stop bit. There was no direct line of sight between the two points. The transmission performance of the RF module was tested. The test results are given in Figure 4.2 and Figure 4.3.

From measurements made in NLOS environment we have good transition at 450 m range. According to Figure 4.2, there is an optimum balance between the transmission data rates. The RSSI level accuracy is clear. In Figure 4.2, the measured received signal values, which were detected peak holding algorithm, were assigned on the vertical axis and the time in ms were assigned on the horizontal axis. This algorithm provides a reasonable estimate of the average RSSI. Signal averaging over a few seconds improves RSSI estimate but it reduces response speed for transition. In Figure 4.2, a signed part by a circle shows us one transition between both modules. RF initializing is shown by A, sending message signal level is shown by B and receiving acknowledge signal level is shown by C.

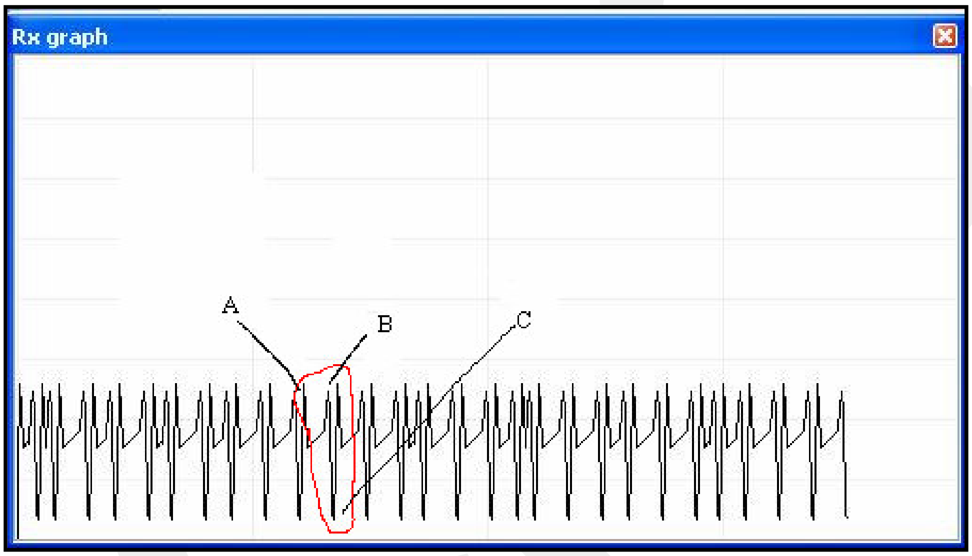

Figure 4.2 Signal Strength Measurements

As mentioned in Chapter 3.4.1, an evaluation was done and its results were presented in Figure 4.3. In these figure, data collection rate was assigned on the vertical axis and data transmission rate was assigned on the horizontal axis.

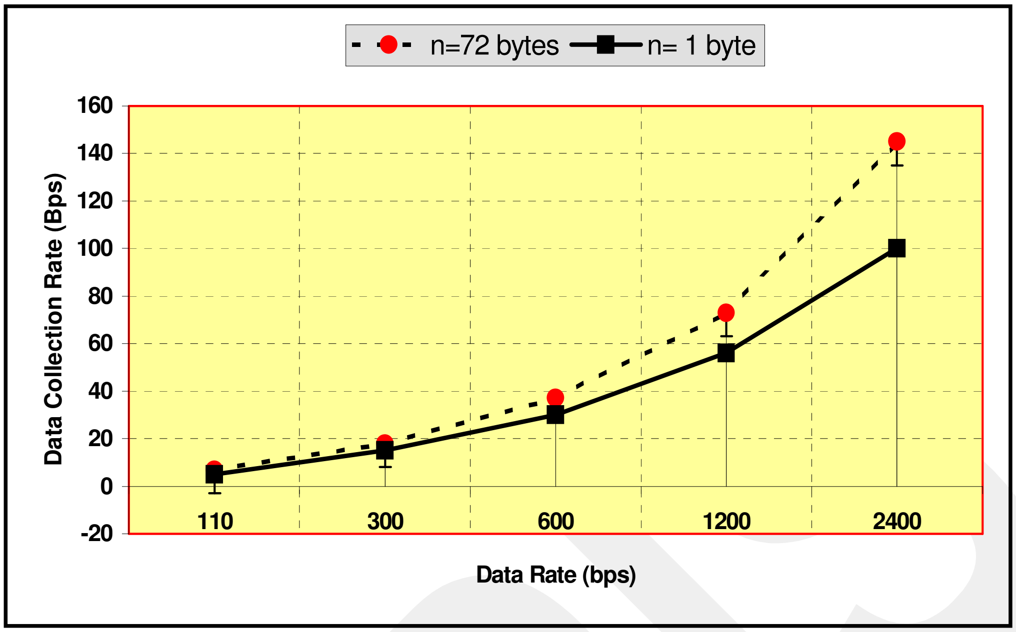

Figure 4.3 System Performances for 2 ms Transmission Time

In Figure 4.3, dotted line parameters were Trf = 2 ms and n = 72 bytes and solid line parameters were Trf = 2 ms and n = 1 byte. Because RF modules data rate were not adjustable, data collection levels were calculated using equations (1) and (2) for transmission data rates except 2400 bps data rate while constituting this chart. As mentioned in Chapter 3.4.1, the master module was adjusted according to mentioned parameters above. The data collection rate varies according to these parameters. Figure 4.3 shows the importance of number of transmitted data to get maximum achieved data rate.

4.2 DISCUSSION OF THE TEST RESULTS

In this section, the test results given above are discussed for both cases.

For the first case, our system was constrained by fading. From this test, it can be concluded that a sharp rising curve which occurred between 200 m and 50 m highlighted efficient performance range. These measurements confirmed that the range performance of the designed module is up to 750 m in LOS conditions.

Another comparison can be done with similar modules in Chapter 2. For example; X8000, 9Xtend and 9XStream modules are higher than our module capabilities. These examples show us the weakness of our system. To utilize our system, data rate performance should be recovered and a high gain directional antenna should be used.

As mentioned in Chapter 3.4.1, the aim of Case 2 test was to check data collection performance of the RF module. Table 4.1 and Table 4.2 show data collection rate for Case 2. As shown in Table 4.1, when transceiver on/off time was decreased to 2 ms, data collection rate increased. The gap between the levels was not remarkable. This situation confirmed that the data transmission rate and transceiver on/off time did not affect the system while sending 72 bytes.

Table 4.1 Data Collection Rates for 72 bytes Transmission

	110 bps	***300 bps***	***600 bps***	***1200 bps***	***2400 bps***	***Data Rates***
n=72 bytes, Trf=10 ms	7	18	37	73	145	**Bps**
n=72 bytes, Trf=2 ms	8	19	39	76	150	

In the second part of the test with the same transmission parameters, Trf was 2 ms and n was adjusted first 72 bytes and then 1 byte. When n was decreased to 1 byte, data collection rate decreased. The gap between the levels was larger than levels which were in the Table 4.1. The results shown in Table 4.2 confirmed that the system was affected by changing of number of bytes. When number of bytes were increased, data collection rate also increased. Large number of bytes were transmitted within a minimal period of time and with high accuracy. Transceiver on/off time became less important by the large number of transmitted data bytes. The test emphasized that to get more data collection rate, transmission data rate should be higher and transceiver on/off time should be less then 2 ms.

Table 4.2 Data Collection Rates for 2 ms Transmission Time

	110 bps	*300 bps*	*600 bps*	*1200 bps*	*2400 bps*	***Data Rates***
n=72 bytes, Trf=2 ms	8	19	39	76	150	**Bps**
n=1 byte, Trf=2 ms	5	15	30	56	100	

4.2.1 Situational Analysis

For indoor communication, the construction materials that make up the obstructions are the largest attenuators. In practice, metallic masses, such as towers, panels, fences or vehicles act as reflectors and scatterers of electro-magnetic radiation. Macroscopic blocking effects, moving bodies, doors opening and closing change the overall RF link attenuation. Because indoor environments vary and reflection and multi path can make it difficult to predict the actual path of the RF signal, our tests were performed in real indoor environments. For industrial applications, reliable data transferring is important. More applications rely on reliable communication system. Because of this, RF modules should ensure this reliability. According to the predefined conditions as mentioned in Chapter 3.4.1, Case 2 test was examined without retries and with acknowledgements enabled, and 85 % of the packets were successfully received. According to this result, the RF module satisfied our expectations as mentioned in Chapter 2.2.6.

CHAPTER 5

CONCLUSION

In industrial area, lack of long range RF module is known. In this thesis, development of a wireless transmission module and checking its performance are mainly aimed.

As mentioned in Chapter 2.2.6, the first requirement to be met was to ensure long range. To find an RF transceiver was the first problem related to this issue. Many web sites and publications as mentioned in the reference list were examined. Finding out that the transceiver had a range of 750 m contrary to the 10 km claimed by its producer was another problem point to be mentioned. To provide a functional support for RSSI measurement was the second difficulty at the design phases. By supporting a scanning algorithm, RSSI measurements were recorded. In the light of our experiences, the base board was designed.

The second requirement was low cost, which was also realized by our module. As mentioned in Chapter 4, our test results have indicated that wireless transmission system, which was low-cost and low- power as mentioned in Chapter 3.2.2.5, can be considered for commercial purposes. However, for the end-users its performance has to be improved and stable operation should be studied.

Our two-way wireless system is capable of retrieving data from a large number of devices with accuracy in a period of time as short as possible. RF modem operations were achieved designed transmission parameters which were 869.4336 MHz , 2.4 Kbps, 8-bits, 1 start bit, no parity and 1 stop bit. Interfacing protocols RS232 and

RS485 offer multi-point connection capability where up to 32 nodes can be connected. The supported protocol which is Modbus protocol can be easily configured and operated in unlicensed radio band.

While trying to obtain reliable data transfer, the importance of the programming was clearly observed. Another problem was to match different data structures between the transceiver and the micro-processor. To arrange some specific packets so as to provide ideal tagging and control algorithm was the major difficulty.

Antenna and RF module placements helped us avoid some obstacles while testing. Nevertheless, the path losses were inevitable. Whatever the conditions, doing site testing in actual environment was an aid for us to decide setting performances of the RF module for future work.

Our system can be customized to different applications, like remote data monitoring and control, and can be operated fixed location remote units. In this study, we have constructed a basis for a prototype and tested it successfully.

5.1 PROPOSED FUTURE WORK

In our thesis, we tried to examine several wireless phenomena in special cases. Potential future work can be examined within two parts. RF transceiver, which is one of them, should be modified in terms of the data structure and communication modes.

The other part is the RF module. Including the antenna, the module size, protection class and programming can be modified. Some additions to the system can be done such as increasing the number of I/O points and adding analog I/O points.

Our portable system is not ready to be used at site. With enough financial and human support it can be developed as a commercial product for industrial applications.

REFERENCES

[1] http://www.modicon.com, 10 May 2007.

[2] http://www.maxstream.net/products, 22 May 2007.

[3] B. Skalar, ”Digital Communications Fundamentals and Applications”, Second Edition, pp.4-92, 2001.

[4] T. Rappaport, ”Wireless Communications: Principles and Practice”, 1987.

[5] T. Itoh, ”RF Technologies for Low Power Wireless Communications”, 2001.

[6] R. K. Crane, ”Propagation handbook for wireless communication system design”, 2003.

[7] C. Smith, ”Wireless Network Performance Handbook”, 2003.

[8] Cypress Semiconductor Corporation, ”Maximizing Range in Wireless Systems”, February 2004.

[9] MaxStream, Inc., ”Technical Hand Book-XST AN010a”, 2004.

[10] http://www.analog.com, 20 May 2007.

[11] http://www.ti.com, 20 May 2007.

[12] http://www.radiotelemtry.co.uk, 20 May 2007.

[13] A. Iraqi, A. Barwicz, P. Mermelstein, R. Z. Morawaski, W. J. Bock, ”Design of a Wireless Communication Module for Telemetry in Civil Infrastructure Monitoring”, IEEE Trans. on Instr. and Measur., Vol. 52, pp.973 – 976, 2003.

[14] P. Eskelinen, J. Ruoskanen, H. Heikkila, ”Low-cost ground to ground mobile telemetry link”, IEEE Aerospace and Electronic Systems Magazine, Volume 19, pp.27 – 31, 2004.

[15] http://www.udea.com.tr/index.php?categoryID=92, 02 June 2007.

[16] Cypress MicroSystems, Inc., ”General Technical Documents”, 2004.

[17] A. Ortiz, J. Munilla, A. Peinado, ”Secure Wireless Data Link for low-cost Telemetry and Telecommand Applications”, IEEE Electrotechnical Conference (Melecon), pp.828-831, 2006.

[18] Cypress MicroSystems, Inc., PSoC Development Kit Manual, 2004.

[19] B. Nejikovsky, E. Keller, ”Wireless Communications Based System to Monitor Performance of Rail Vehicles”, Railroad Conference, 2000., Proceeding of the 2000 ASME/IEEE Joint, pp.111-124, 4-6 April 2000.

[20] S. D. Baker, S. W. King, J. P. Welch, ”Performance measures of ISM-band and conventional telemetry”; IEEE Trans. on Engineering in Medicine and Biology Mag., Vol. 23, pp.27-36, 2004.

[21] C. A. Balanis, ”Antenna Theory Analysis And Design”, Third Edition, pp.9-36, 2005.

[22] T. Antonakopoulos, C. Powers, N. Kanopoulos, ”A versatile wireless system for real-time telemetry applications”, Electronics, Circuits, and Systems, 1996. ICECS ‘96., Proceeding of the Third IEEE International Conference on, Vol. 2, pp.1194-1197, 13-16 October 1996.

GCRIS

APPENDICES

Appendix A – UFM-A12WPA RF Module

Key Features:

Long Range Data Integrity

- 500 mW Power Output
- 4,800 bps data rate
- up to 10 km / Whip antenna
- -123 dBm Receiver Sensitivity

Low Power

- 3,3 – 5 V Supply voltage
- Pin and Serial port

Advanced Networking and Security

- Point-to-Point, Point-to-Multipoint
- UART Transceiver
- Retries and Acknowledgements
- RS232-TTL (0-5 Vdc) Link

Use

- Transparent Operation
- Portable
- Multiple data formats
- Narrow band FSK Modulation ISM transceiver operates in 869.4336 MHz.

Compatibility

- EN 300 220 Compliant (Emission Unit Testing Standard)

Table A.1 Pin Arrangements of UFM-A12WPA RF Module

Pin	Name	Input Output	Description	Note
1,3,4	GND	-	Ground Connection Point	-
2	ANT	-	Antenna Connection Point	-
5	NC	-	Unused	Not Connected
6	TX	O	TX-UART	3 Vdc
7	RX	I	RX-UART	3 Vdc
8	NC	-	Unused	Not Connected
9	Vcc-1	-	5 Vdc Power Supply	Max. 40 mA
10	Vcc-2	-	3 Vdc Power Supply	Max. 600 mA

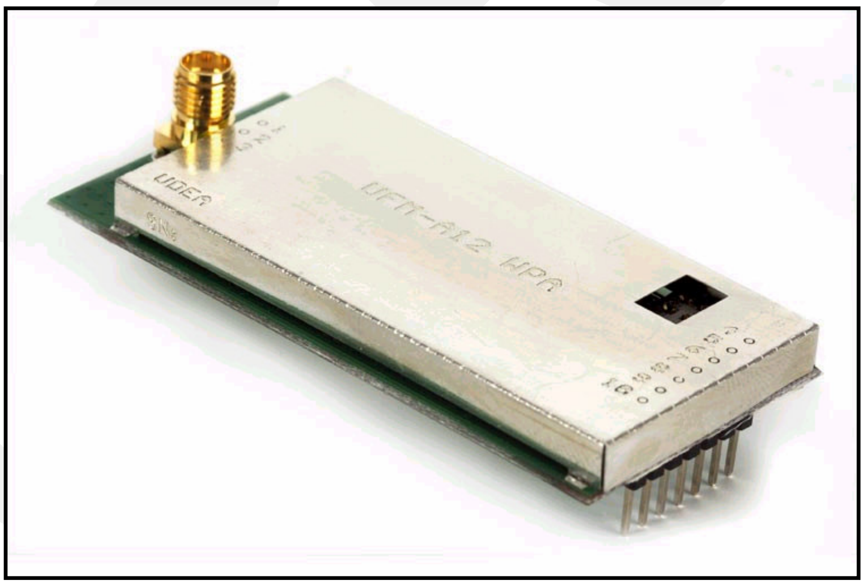

Figure A.1 UFM-A12WPA RF Module [15]

Table A.2 Specifications

Performance	Min	Typical	Max	Unit	Note
Transmit Power Output	-	23	27	dBm	-
Outdoor LOS Range	1	-	10	Km	-
Data Rate	1.8	4.8	38.4	Kbps	Manchester Coding
Receiver Sensitivity	-	-120dBm	-123	dBm	2.4 k Baud
Frequency	869	869.4336	869.6064	MHz	-
Bandwidth	-	7.5	-	KHz	2.4 k Baud
Power Requirements					
Supply Voltage	3.3	-	5	V	-
Current Consumption TX Mode	-	500	-	mA	-
Current Consumption RX Mode	-	50	-	mA	-
Logic “0” DI	0	-	0.6	V	-
Logic “1” DI	3.5	-	5	V	-
Logic “0” DO	0	-	0.6	V	-
Logic “1” DO	3.5	-	5	V	-
Physical Properties					
Serial Connector	-	10	-	Pin	-
Operating Temperature	-10	-	+50	℃	-
Board Size	*70X33X8*			mm	-
Antenna					
Connector	*SMA*				-
Impedance	*50 ohms*				-

Appendix B – CY8C27443 Chip

Key Features:

Powerful Harvard Architecture Processor

- M8C Processor Speeds to 12 MHz
- Low power at high speed
- 4,75V to 5,25V Operating Voltage
- Extended Temp. Range: -40 °C to +105 °C

Precision, Programmable Clocking

- Internal 24 MHz Oscillator

Flexible On-Chip Memory

- 16K Bytes Flash Program Storage
- 256 Bytes SRAM Data Storage
- Partial Flash Updates
- Flexible Protection Modes

Programmable Pin Configurations

- 25 mA Sink on All GPIO
- Up to 12 Analog Inputs on GPIO
- Four 30 mA Analog Outputs on GPIO

Additional System Resources

- Integrated Supervision Circuit

Advanced Peripherals

- Up to 14-Bit ADCs, Up to 9-Bit DACs
- 8 to 32-Bit Timers, Counters and PWMs
- Up to 2 Full-Duplex UARTs
- Connectable to all GPIO Pins

GCRIS

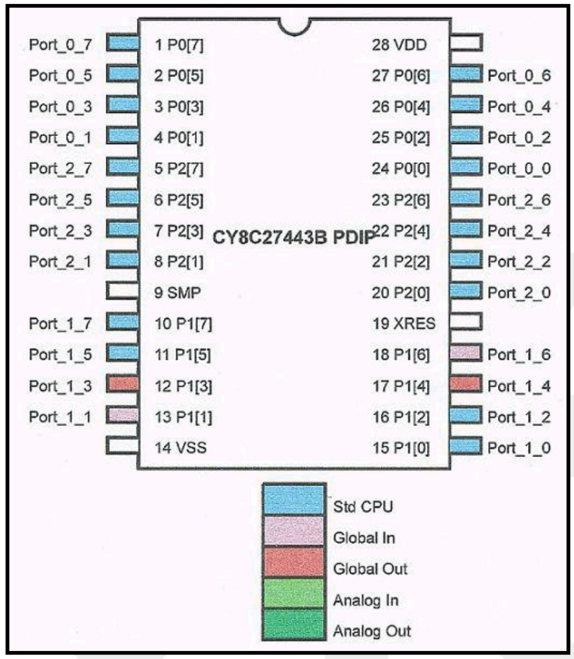

Figure B.1 CY8C27443 Chipset [18]

Appendix C – MAX485

Table C.1 Pin Arrangements of MAX485

Pin No	Name	Description	Note
1	RO	Receive Output	RS485+
2	RE	Receive Output Enable	-
3	DE	Driver Output Enable	-
4	DI	Driver Input	RS485-
5	GND	Ground Signal	-
6	A	Non-inverting Receiver Input	RSA
7	B	Inverting Receiver Input	RSB
8	VCC	Positive Supply	4,75V <= VCC <= 5,25V

Appendix D – L7805 and LM317 Regulators

Table D.1 Electrical Characteristics of L7805 Regulator

Symbol	Parameter	Min	Typical	Max	Unit
Vi	Input Voltage	-	24	35	V
Vo	Output Voltage	4,8	5	5,2	V
ΔVo	Line Regulation	-	3	50	mV
ΔVo	Load Regulation	-	-	100	mV
SVR	Supply Voltage Rejection	68	-	-	dB
Io	Output Current	Internally Limited			
Isc	Short Circuit Current	-	0,75	1,2	A
Iscp	Short Circuit Peak Current	1,3	2,2	3,3	A

Table D.2 Electrical Characteristics of LM317 Regulator

Symbol	Parameter	Min	Typical	Max	Unit
Vi	Input Voltage	-	5	-	V
Vo	Output Voltage	Adjustable {Vo=1,25*[1+(R2/R1)]}			
ΔVo	Line Regulation	-	0,01	0,04	%/V
ΔVo	Load Regulation	-	20	70	mV
SVR	Supply Voltage Rejection	68	80	-	dB
Iomax	Max. Load Current	-	0,4	-	A

Appendix E – PS2501 and BC237C Transistors

Table E.1 Electrical Characteristics of PS2501-1 Transistor

Parameter		Symbol	Min	Typical	Max	Unit
Diode	Forward Voltage	Vf	-	1,17	1,4	V
	Reverse Current	Ir	-	-	5	uA
	Terminal Capacitance	Ct	-	50	-	pF
Transistor	Collector to Emitter Current	Iceo	-	-	100	nA
Coupled	Current Transfer Ratio	CRT	80	300	600	%
	Collector Saturation Voltage	Vce	-	-	0,3	V
	Isolation Resistance	Ro	10^{11}	-	-	Ω

Table E.2 Electrical Characteristics of BC237C Transistor

Parameter	Symbol	Min	Typical	Max	Unit
DC Current Gain	hfe	-	270	-	-
Collector – Emitter on Voltage	Vce	-	0,07	0,2	V
Base – Emitter Saturation Voltage	Vbe	-	0,6	0,83	V
Base – Emitter on Voltage	Vbe	-	0,5	-	V
Noise Figure	NF	-	2	10	dB
Collector – Base Capacitance	Cobo	-	-	4,5	pF

Appendix F – PSoC Designer Software

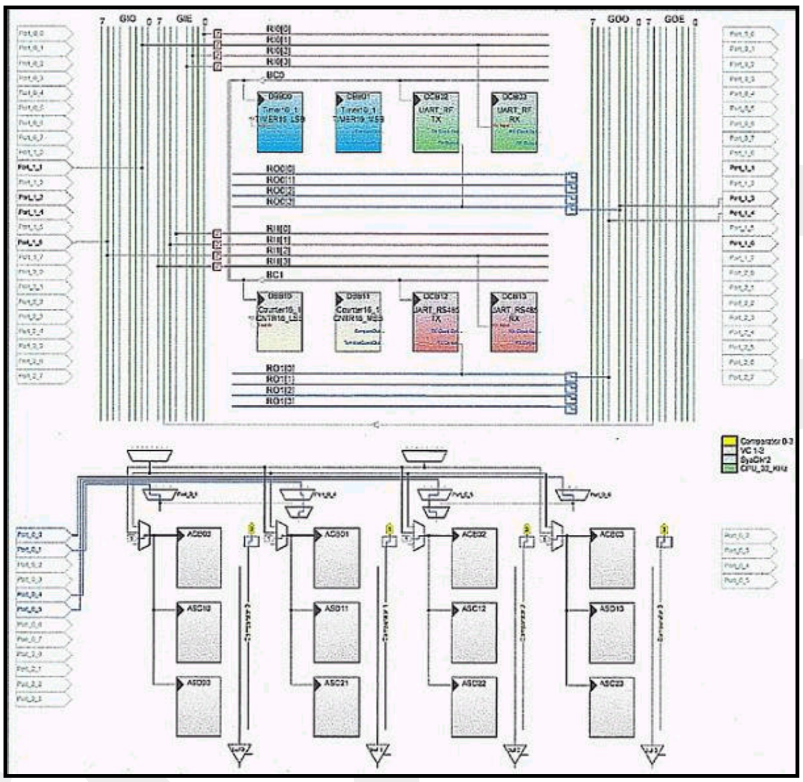

Figure F.1 Configuration Page of CY8C27443 Chip [18]