



THE UNIVERSITY OF QUEENSLAND

**A Security System Using
Wireless FSK Communications:
Hardware Aspects**

by

Priscilla Lay

School of Information Technology and Electrical Engineering
UNIVERSITY OF QUEENSLAND

Submitted for the degree of
BACHELOR OF ENGINEERING (pass)
IN THE DIVISION OF ELECTRICAL ENGINEERING

October 2003

29 October 2003

The Head of School
School of Information Technology and Electrical Engineering
The University of Queensland
St Lucia, QLD 4072
Australia

Dear Professor Kaplan,

In accordance with the requirements of the degree of Bachelor of Engineering in the division of Electrical Engineering, I present the following thesis entitled:

A Security System Using Wireless FSK Communications: Hardware Aspects.

This thesis was performed in partnership with Ron Ng under the supervision of Dr. John Homer (Sem 1, 2003), Dr. Adam Postula (Sem 2, 2003) and co-supervision of Wai Yie Leong.

I declare that the work submitted in this thesis is my own, except as acknowledged in the text, or references, and has not been previously submitted for a degree at the University of Queensland or any other institution.

Yours Sincerely,

Priscilla Lay

To Mum and Dad...

Acknowledgements

There are a number of people I wish to thank for their help and support during the course of this thesis.

To my thesis supervisors, **Dr John Homer** and **Dr Adam Postula**, for offering support and help throughout the project;

To my co-supervisor, **Wai Yie Leong**, for your support throughout the year;

To my thesis partner, **Ron Ng**;

To the staff at the EPSA Electronic Workshop, especially **Keith Bell**;

And finally, to all my family and friends, for their love, support and encouragement during the hard and stressful times.

Abstract

Security is the precaution taken to protect items from theft or/and danger [1]. For this reason, security systems have been developed to cater for these tasks. There are numerous types of security systems and the most commonly used device involve infrared sensors, as they are easy and neat to fit, extremely reliable and low in cost. Currently, most of the standard security devices only consist of a sensor and siren, which produces a loud sound when the sensor as been triggered.

The aim of this thesis is to develop and implement a security system, which uses Frequency Shift Keying (FSK) wireless communications. However, the design and implementation of the system will not include the entire system. This thesis will primarily concentrate on the hardware development of the system, though a brief discussion of software will be mentioned.

The security system has been design mainly as a prototype and will incorporate the concept of current security devices and most importantly, the use of FSK modulation scheme. FSK is a scheme which transmits digital information (1's or 0's) across an analog channel [2]. This security system will allow users to view the location of the security breach, resulting in a drastically reduced response time of authorized personals.

The system is required to use the Nordic nRF401 transceiver and will primarily consist of three parts; the transmitting module, receiving module and power supply. The transmitting module will detect and send information to the receiving module, where it will process the received information and display the results for viewing. The power supply will provide the required voltage to operate the system.

Overall, the security system was successfully implemented and demonstrated how the FSK modulation and demodulation scheme could be use in a design of a security system.

List of Figures

- Figure 2.1** Digital signal represented by an analog signal
- Figure 2.2** Magnet contact detector
- Figure 2.3** Beam detector
- Figure 3.1** Hardware layout
- Figure 4.1** Block diagram of the PIC 16F876
- Figure 4.2** USB MOD2 module
- Figure 4.3** nRF401 transceiver block diagram
- Figure 4.4** The overall system design
- Figure 4.5** Security system hardware
- Figure 4.6** Final packaging of the transmitter and receiver units
- Figure 6.1** Battery lifetime

List of Tables

Table 4.1	Comparison of different PIC microprocessors
Table 4.2	FSK transceiver chip comparison table
Table 4.3	Required connections from the processing unit to the RF unit

Table of Contents

ACKNOWLEDGEMENTS	V
ABSTRACT	VI
LIST OF FIGURES	VII
LIST OF TABLES	VIII
INTRODUCTION	1
1.1 Thesis Introduction	1
1.2 Prior work	2
1.3 Thesis Objective	2
1.4 Thesis Structure	2
BACKGROUND INFORMATION	5
2.1 What is Frequency Shift Keying (FSK)	5
2.2 Existing products	6
2.2.1 Low Level Security Systems	6
2.2.1.1 Magnetic contact detectors	6
2.2.1.2 Dual technology sensors	7
2.2.1.3 Inertia/vibration detectors	7
2.2.1.4 Beam detectors	7
2.2.1.5 Infra-red detectors	8
2.2.2 High Level Security Systems	8
PRODUCT SPECIFICATION	9
3.1 Base specification	9
3.2 Product constraints	10
3.3 Engineering Specifications	10
3.4 Target Market	11
3.5 The Design Specifications	11

3.6	Hardware Specification	11
3.6.1	Power Supply	13
3.6.2	Sensors	13
3.6.3	Transmitting Processing Unit	13
3.6.4	FSK Transmitting Unit	13
3.6.5	FSK Receiving Unit	14
3.6.6	Receiving Processing Unit	14
3.6.7	Display unit	14
3.7	Software Specifications	14
HARDWARE IMPLEMENTATION		17
4.1	The Transmitting Unit	17
4.1.1	Sensors	17
4.1.2	Microprocessor	18
4.2	The Receiving Unit	20
4.2.1	Microprocessor	20
4.2.2	Display unit communication	20
4.3	Display Unit	21
4.4	RF Communications	22
4.4.1	RF FSK transceivers	22
4.4.2	Nordic nRF401 Transceiver	23
4.4.2.1	Nordic Hardware implementation	23
4.4.2.2	Nordic Software implementation	24
4.2	Power Supply	24
4.3	PCB design and packaging	25
SOFTWARE IMPLEMENTATION		27
EVALUATION		29
6.1	Product Review	29
6.2	Personal Assessment	30
FUTURE DEVELOPMENTS		33
7.1	Hardware Design Improvements	33
7.2	The Dream	34

CONCLUSION	35
REFERENCES	37
APPENDIX A	41
APPENDIX B	42
APPENDIX C	43
APPENDIX D	44
APPENDIX E	45
APPENDIX F	46

1

Introduction

1.1 Thesis Introduction

Security systems are commonly used around the world in homes, offices, buildings, laboratories, storage areas, banks and the list is endless. A home is 2.2 times and a business is 4.5 times more likely to be burglarized than one with a security system [3].

The general purpose of a security system is obvious. A house with a small number of entry points can be simply protected with detectors, which produce a sound when triggered. The location of the security breach can be easily located as the area is quite small. However what happens when a building with multiple levels, a large number of rooms and hundreds of entry points needs to be protected? How does security personals know which entry point has been breached?

This security system will assist in the location of the security breach by sending information, corresponding to the particular sensor or entry point of the building by the use of FSK modulation and demodulation techniques. This will reduce the response time to catch the offenders.

1.2 Prior work

This thesis project has not been previously carried out by a University of Queensland thesis student however the use of the FSK communications was commonly used in many 2002 thesis topics. These include the ‘BlueNanny – Child Monitoring System’ [4] and ‘Wireless ECG Monitors’ [5].

1.3 Thesis Objective

The aim of the project is to design and build a security system using the Nordic nRF401 FSK RF transceiver for wireless communication [6].

The objective of the thesis is to build the hardware of a prototype that;

- uses the modulating and demodulating technique of Frequency Shift Keying
- has the concept to function as a security system

The thesis focuses only of the hardware aspects of the security system. The software aspects of the security system can be read in the thesis entitled, “A Security System using FSK Wireless Communications: Software Aspects [7].” Together, the two theses are intended to complete the security system.

1.4 Thesis Structure

The design and implementation of the security system hardware will be discussed in detail in this report. This, the first chapter discusses the objectives of the thesis whereas the following chapters will deal with:

Chapter 2 provides background information of Frequency Shift Keying and discusses some security devices currently available.

Chapter 3 looks at the system's hardware requirements and specifications. It also gives a brief outline of software requirements.

Chapter 4 discusses how the hardware was implemented and the major components used.

Chapter 5 gives a summary of software implementations of the system.

Chapter 6 provides an evaluation on the product and personal assessment is discussed.

Chapter 7 looks at how the product can be improved and the possibilities of future developments.

Chapter 8 concludes the thesis report by giving a brief summary of the project.

2

Background Information

2.1 What is Frequency Shift Keying (FSK)

Frequency Shift Keying (FSK) is a scheme that transmits digital information across an analog channel [8]. The two digital binary states, logic 0 (low) and logic 1 (high) are represented by different analog waveforms [9]. Figure 2.1 is an example of how a digital signal can be represented by an analog signal.

There are many advantages and disadvantages of FSK, compared to other modulation techniques. These advantages include improved signal to noise ratio, use of less radiated power and ease of implementation [10]. A disadvantage is that FSK requires a larger bandwidth.

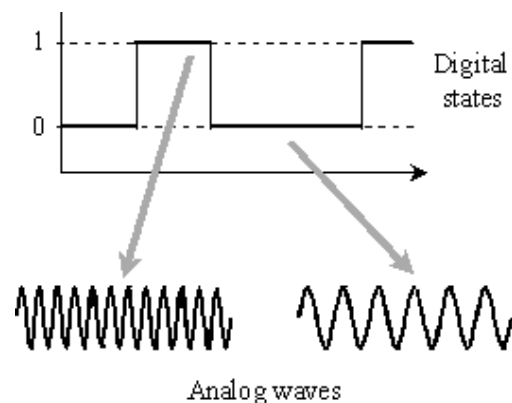


Figure 2.1 Digital signal represented by an analog signal

2.2 Existing products

The concept of a security system is similar to everyone. Its job is to protect valuables and/or irreplaceable items, from theft or damage and to alert a person when an intrusion has occurred in an unauthorized area. Security systems can be classified into two different levels; low and high.

2.2.1 Low Level Security Systems

A majority of security systems only detect when an intrusion has occur. These security devices rely on sensors, which only produce a loud warning noise once they have been triggered and are often used in low security areas. The advantage of these devices is that they are portable and additional electrical wiring is often not required. A few examples of these devices include:

2.2.1.1 Magnetic contact detectors

This detector contains two parts – a reed switch and an operating magnet [11]. In general, the reed switch is fitted to the frame of a door and held close together by the magnet, fitted to the door. The alarm would be triggered if the door were to be opened [12]. Figure 2.2 is an example of such a detector.



Figure 2.2 Magnet contact detector

2.2.1.2 Dual technology sensors

The combination of infrared and microwave technology makes up the dual technology sensor [11]. The infrared detects any change in temperature while the microwave detects any movement. This type of detection will only trigger the security system if both detectors are tripped.

2.2.1.3 Inertia/vibration detectors

As the name implies, these detectors sense any sudden movements in a room and are usually fitted to windows frames [11].

2.2.1.4 Beam detectors

These detectors are best used when detecting any movement across a large area. They normally consist of separate transmitting and receiving units where a beam is formed between the two units. When movement is detected, crossing the beam, the detector is triggered. Mirrors or reflectors, which have been properly positioned, can increase the area of detection [11]. Figure 2.3 is an example of a beam type detector.



Figure 2.3
Beam detector

2.2.1.5 Infra-red detectors

These are the most commonly used detector, out in the market. They detect movement of heat, by looking at the room in infrared [13]. There are many other alternatives, which can be added to this detector. The most commonly used variants are the dual technology detector, as mentioned in section 2.2.2 and the tri technology detector. The tri technology detector is identical to the dual technology detector with the addition of a pressure sensor [11].

2.2.2 High Level Security Systems

These days, high level security systems are required in Government buildings, banks, high rise office buildings and practically any environment, which instantly require the location of the intrusion. These systems are often especially tailored for the situation and large amount of electrical wiring and planning are required to display such information. Video surveillance cameras also assist in the capturing of the intrusion.

3

Product Specification

The most important hardware requirement for the security system is to use the Nordic nRF401 transceiver for the FSK communication. Based on this requirement and many more, specifications will be derived which will be used to implement the hardware prototype of this system and will be detailed in chapter 4.

3.1 Base specification

A security system is required to protect valuables from theft and/or damage. A typical and simple security device requires [14]:

- A sensor
- A siren

The sensor is required to detect when an intrusion as occurred while the siren is needed to alert others of the intrusion and to intimidate the intruder to think twice. Often, both these requirements are integrated into the one unit. In addition, a security system will take that extra step and display the location of the security breach, obviously with additional circuitry.

3.2 Product constraints

The development of this security system was defined largely by the time constraint. The project must be completed, from design to implementation, in a time frame of approximately 27 weeks (excluding holidays). The School of Information Technology and Electrical Engineering has provided funding for this project, however the final cost of the product has not been set. A vital constraint is the availability and delivery time, of the required components, to complete the hardware of the system.

3.3 Engineering Specifications

It is necessary to define some engineering specifications for this system.

- **Fast** – the system reaction time to the intrusion must be quick or there is no purpose to the security system.
- **Reliable** – the system must be expected to work when in operation.
- **Ease of use** – the system should be easy to use.
- **Ease of installation** – installing the system should be simple and should not require a high cost.
- **Light in weight** – the units should be light so it can be placed anywhere without causing architectural damage.
- **Low operating cost** – when running a system of this nature, the only associated cost is the power consumption.
- **Low maintenance** – the system must require low level maintenance.
- **Ease of future enhancements** – hardware and software, if needed, should be easy to add or changed in the system.

3.4 Target Market

Presently, this system will be built as a prototype, mainly to demonstrate the use of FSK communications in a security-breached situation. The targeted market would eventually be large organizations, which would require the instant location of the security intrusion. Such organizations would include the Government, schools, Universities, high rise office buildings etc.

3.5 The Design Specifications

After considering the required specifications and constraints listed in the above sections, the ideal security system would have the following requirements:

- Low operating cost
- Low maintenance
- Ease of use
- Ease of installation
- Reliable
- Small in size and light weight
- Ease of future developments

3.6 Hardware Specification

Currently, a majority of security devices do not show the location of where the intrusion has actually occurred. For example, if a security detector has been triggered, in a building with numerous rooms and many levels, the problem is the difficulty to pin point the actual location of the intrusion.

Using wireless FSK communications to send and receive a specific signal, each corresponding to a particular sensor/detector, would be a solution to this problem, mentioned above. It would help reduce the response time of authorized personals. This system can be easily designed and individually catered for any type of building, needing this form of monitoring.

The security system prototype, for this project will have the following main hardware features;

- Sensors
- Transmitting device
- Receiving device
- Display unit

The figure below gives the intended hardware layout.

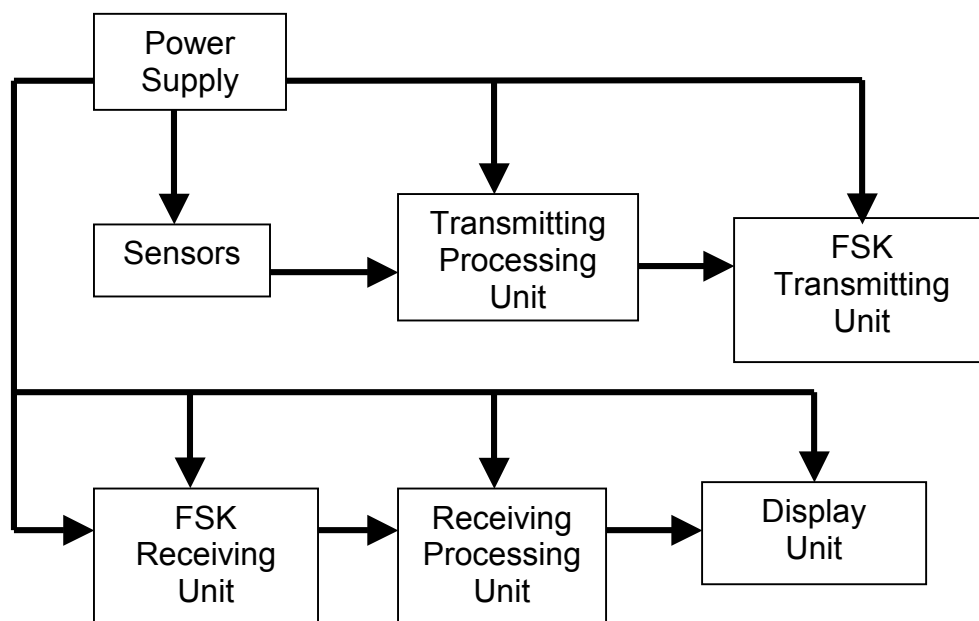


Figure 3.1 Hardware Layout

3.6.1 Power Supply

Two types of power supply will be required for this security system, 240Volts AC (alternating current) and DC voltage (direct current). The use of 240Volts AC can potentially be dangerous and safety must be taken when using this source of power. DC currently allows the device to be portable.

3.6.2 Sensors

The importance of sensors is to detect the moment an intrusion has occurred. Without this hardware feature, the installation of the security system would be useless.

3.6.3 Transmitting Processing Unit

This unit is responsible for processing which sensor has been trigger. It must also have the ability to output digital data into the RF transmitting unit. Choosing the right processing unit is important, as it must have enough memory to comply with all software requirements. Low power consumption is also required.

3.6.4 FSK Transmitting Unit

The security system requires the use of FSK communication therefore circuitry to produce such modulation technique is essential.

3.6.5 FSK Receiving Unit

This unit is required to receive the signal sent by the FSK transmitting unit. Without this unit, the system would fail and not meet the requirements given.

3.6.6 Receiving Processing Unit

As with the transmitting processing unit, section 3.6.3, the requirement of this unit is important. Its task is to process the information received from the FSK receiving unit, section 3.6.5, and in turn, send the collected information to a display unit where security personals are given the exact location of the intrusion. High memory capacity and low voltage must also be considered when choosing the right processor.

3.6.7 Display unit

This unit must have the ability to communicate with the receiving processing unit, section 3.6.6. The display unit is important as it shows security personals the exact location of the intrusion.

3.7 Software Specifications

As with most devices, hardware will not be able to function without the software. The software can be divided into two sections; the operating software of the processing units and the Graphical User Interface (GUI). Both sections of the software should not be accessible to the user of the system. The GUI is required to be easy to use and its main function is to display the location of the security breach. Because the thesis is required

to build the hardware of the security system, the detailed software specifications for the security system can be read in the partnering thesis titled “A Security System Using Wireless FSK Communications: Software Aspects [7].”

4

Hardware Implementation

The design for the security system can be essentially divided into five sections: the transmitting unit, receiving unit, the display unit, RF communications units, and power supply. This chapter will discuss the components used to implement these modules, according to the specifications discussed in chapter 3.

4.1 The Transmitting Unit

This unit consists of the sensors and the processing unit, which must send digital information to the RF transmitting unit. The schematic diagram for the transmitting unit can be seen in Appendix A.

4.1.1 Sensors

The design of the security system requires sensors which will detect any intrusion. Four push buttons will be used to imitate as the detection device, each representing four separate rooms. As mentioned in section 2.2, there are many sensors/detecting devices available and each sensor has situations where they work the best. The main reason for implementing push buttons, as sensors, is to allow the option to add the best-suited sensor for an individual tailored security requirement.

The numerical value of push buttons was selected to demonstrate the system's ability to show the different locations of the security breach. This can be increased if necessary.

4.1.2 Microprocessor

From all the available microprocessors, the selection was made within the PIC range. The following table compares the some different PIC microprocessor chips available [15].

	PIC 16F873	PIC 16F874	PIC 16F876	PIC 16F877
Operating Frequency	DC – 20M Hz	DC – 20M Hz	DC – 20M Hz	DC – 20M Hz
FLASH program memory	4K	4K	8K	8K
Data memory (bytes)	192	192	368	368
EEPROM data memory	128	128	256	256
No. of I/O ports	22	33	22	33
Number of Interrupts	13	14	13	14

Table 4.1 Comparison of different PIC microprocessors

The PIC 16F876 microprocessor was chosen mainly due to the past experience in using the chip as well as its availability. Another reason for choosing this 8-bit microprocessor is because of its significant number of I/O (input/output) ports, which can be defined by the embedded software. It has 256 bytes of EEPROM (Electrically Erasable Programmable Read Only Memory) data memory, which provides more than sufficient storage capacity for the security system. The PIC microprocessor was also chosen due to its low cost and the availability of devices and software to program the chip. This is useful if any problems occur, a replacement chip could be easily obtained. In addition, the PIC 16F876, consumes very low current when in operating mode and even lower current when in standby mode. Finally, the programming language for the

microprocessor can be written in either Assembly or C. Figure 4.1 shows the block diagram and internal components of the PIC 16F876.

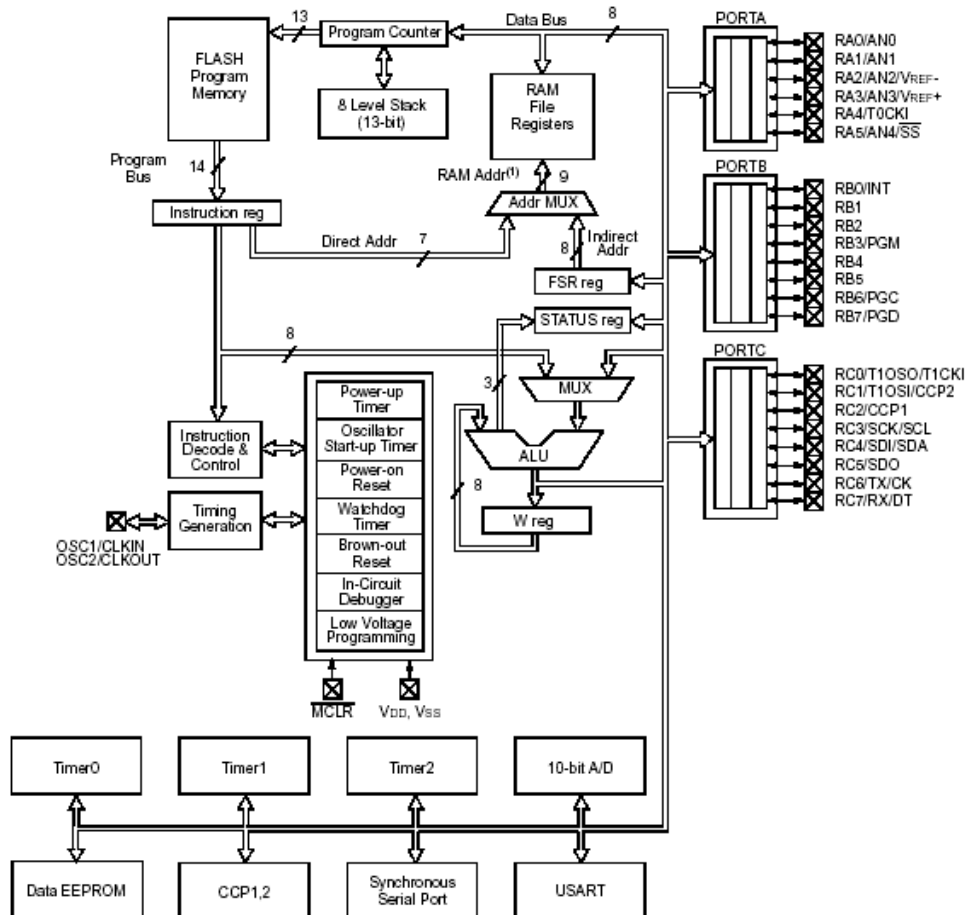


Figure 4.1 Block diagram of the PIC 16F876.

For this microprocessor to operate correctly, a 20MHz external oscillator crystal is required between pins 9 and 10. Its purpose is to imply the instruction cycle rate.

4.2 The Receiving Unit

As with the transmitting unit, there are two sections associated with the receiving unit; the processing unit and the communication link between the processing unit and the display unit. The schematic diagram can be seen in Appendix B.

4.2.1 Microprocessor

The PIC16F876 was again chosen, for the receiving processing unit, for the same reasons stated in section 4.1.2. The large number of I/O ports was more than enough to allow a communication link with the display unit, which is required to display the location of the intrusion. The same microprocessor was chosen for processing the digital information, for both transmitting and receiving units, would ease the software implementation. This is because there would be no need to learn an additional microprocessor programming language.

4.2.2 Display unit communication

The USB MOD2, manufactured by Ravar [16], (figure 4.1) was chosen to produce the communication link between the display unit and the receiving PIC16F876 (section 4.2.1). It was chosen to ease the implementation of the system and is powered by the USB port. Additionally, most computers today contain at least one USB port, which will allow a simple connection between the display unit (section 4.3) and the receiving unit. The module is a parallel 8-Bit FIFO

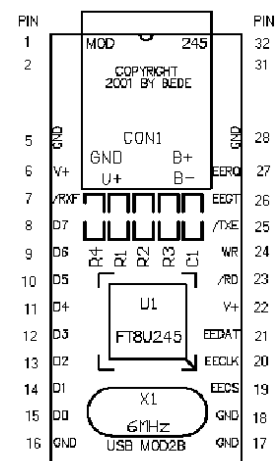


Figure 4.2 USB MOD2 Module

which is suited to the system as the digital code, being transmitted and received by the PIC 16F876, is 8 bits. More information on the digital code can be read in the thesis entitled “A Security System Using Wireless FSK Communications: Software Aspects.” The USB MOD2 features a multi-function data transfer chip and is compatible with many Virtual Com Port drivers for operating systems such as Windows 98/2000/ME and XP.

Furthermore, the USB MOD2 module produces a power supply of approximately 5 Volts DC. This will be elaborated in section 4.5. Appendix C gives a table of the pin function of the USB MOD2. To operate the USB MOD2, no external components were needed only the PCB routing connection with the microprocessor.

4.3 Display Unit

There are many options which could be used as a display unit. These would include a LCD, using LEDs to display the security breached room or a computer/laptop. The chosen solution was the personal computer/laptop, which must contain a USB port. The reason for this choice was mainly due to the fact most computers/laptops today have at least one USB port, which would allow the simple connection to the USB MOD2 module, using a USB cable. Furthermore, the computer allows software packages which can be used to produce the Graphical User Interface. This display unit is intended to be the central control base where the location of the security breached is showed on the screen. No additional hardware or electrical wiring is required for the communication with the USB MOD2, which meant ease of implementation.

4.4 RF Communications

A requirement of the system is to use the FSK communication scheme. As defined in section 2.1, FSK is a modulation scheme which sends digital information across an analog channel. This unit must have the ability to convert the specific digital data packet, sent by the PIC 16F876, into RF (radio frequency) signals and to transmit this signal to the receiving RF module. In turn, the receiving module must demodulate the received signal and convert it back into digital format.

4.4.1 RF FSK transceivers

There are many possible RF transceivers which could be used to implement this wireless FSK security system. The table below shows a comparison table between a few chips that can be used to implement the FSK modulating and demodulation technique.

	Units	Nordic nRF401 [19]	TI TRF5901 [17]	TI TRF6900 [18]
Frequency (min/max)	MHz	433.93/434.33	902/928	850/950
Operating Voltage (min/max)	Volts	2.7-5.25	3-3.6	2.2-3.6
Output Power	dBm	10	5	9
Supply Current (RX mode)	mA	8	28	24
Supply Current (TX mode)	mA	8	26	26
Standby Current	uA	8	0.5	0.6
Maximum Bit Rate	Kbits/s	20	100	100

Table 4.2 FSK transceiver chip comparison table

Due to a requirement to use the Nordic nRF401 transceiver the decision on which chip to use was made. The availability of a Nordic nRF401 evaluation board, application notes and data sheets assisted in developing the hardware. The operating voltage between 2.7 – 5.35 Volts DC was also within the range required by the microprocessors and USB modules. As shown in the table above, an additional feature of the Nordic nRF401 transceiver is its low power consumption and its ability to be placed in standby or operating modes.

4.4.2 Nordic nRF401 Transceiver

As mention in the previous section, the Nordic nRF401 transceiver is a hardware requirement for the security system. This single chip transceiver is designed to be operated in the ISM frequency band of approximately 433.92MHz and features Frequency Shift Keying modulation and demodulation ability. This is a very important feature. Figure 4.2 shows the block diagram of the nRF401 transceiver.

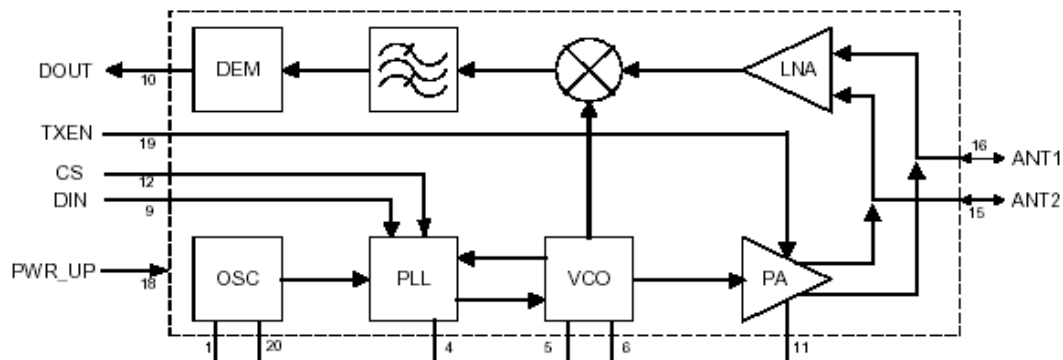


Figure 4.3 nRF401 transceiver block diagram

4.4.2.1 Nordic Hardware implementation

The values of external components, required for the operation of the chip, was provided by the chip manufacturer, Nordic. Before purchasing any external components needed, data sheets explaining the importance of the individual component specifications was read. Appendix D illustrates the schematic diagram of the RF circuitry.

4.4.2.2 Nordic Software implementation

The actual Nordic nRF401 transceiver chip can not be programmed. The method to operate this 20-pin transceiver is by implementing at least four input pins of the chip. This is done by either hardwiring the circuit, to either power or ground, or connecting the corresponding transceiver pin to a digital processing unit. The following table shows the pins required to operate the transceiver, in either transmitting or receiving mode. Appendix E shows all the pin functions of the Nordic transceiver.

Mode	Pin	Pin Name	Description
TX	9	Din	Digital Data Input
RX	10	Dout	Digital Data Output
TX & RX	12	CS	Frequency selection “0” = 433.92 MHz
TX & RX	18	Pwr_up	Operating or standby mode
TX & RX	19	Txen	Transmit or Receive mode

Table 4.3 Required connections from the processing unit to the RF unit

4.2 Power Supply

As mentioned in section 3.6.1, the system requires two different power supplies of 240Volts AC and DC voltage. The display unit, i.e. personal computer/laptop, will require a 240Volt AC outlet which can be obtained by the building’s current electrical circuitry. The USB port from the computer/laptop will power the receiving modules of the system. As mentioned in section 4.2.2, the USB port produces approximately 5V DC which is within the range for operating both the PIC 16F876 and the Nordic nRF401 transceiver, hence the reason to power the receiving end of the system with the USB port. This reduces the need for batteries and allows the receiving units to be constantly powered.

The transmitting end of the system is powered by 2xAA batteries, totaling 3Volts. This was implemented as the transmitting end, of the security system, must be portable to display the range of the signal.

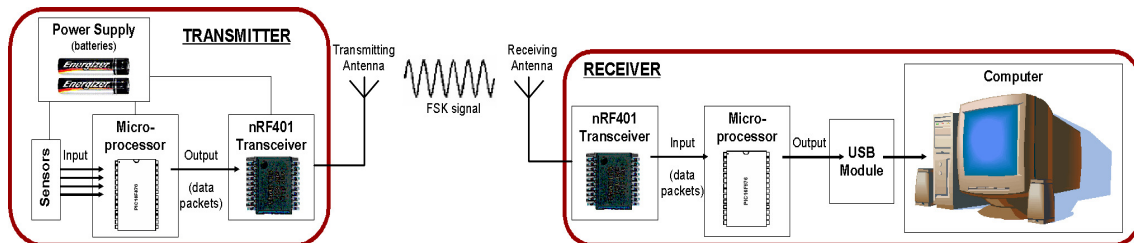


Figure 4.4 The overall system design

4.3 PCB design and packaging

The final stage of the hardware implementation was the PCB design and packaging. Digital and analog circuitry and PCB design might work well separately, however when placed on the same PCB board can be more complex [20]. Consequently, it was decided to implement the digital (microprocessor) and analog (nRF401 transceiver) PCB boards separately to allow the ease of troubleshooting.

Firstly, the digital circuit PCB, for the transmitting and receiving ends of the system, had to be designed and implemented. Both these boards had to be ground plated as the overall system was using RF signals. Furthermore, the wires used to connect the output pins of the digital circuit to the required four input pins of the nRF401 transceiver, had to be twisted with a wire connected with ground. Without doing this, the RF signal could be corrupted.

The artwork of the PCB (printed circuit board) design was provided by the chip manufacturer however header footprints were added to allow the connection between the corresponding receiving and transmitting processing modules. This assisted in any

troubleshooting. If designing the PCB artwork from scratch, there are many PCB guidelines which are recommended for optimum performance. These details can be found in the nRF401 Transceiver datasheet [19].

Two different types of PCBs manufacturing technique was used to implement the system. Simple etching was used for the digital circuit PCBs and plated-through PCB was used to fabricate the RF circuitry. This was required as the RF PCB artwork, was ground plated on both the top and bottom layers of the PCB and the transceiver was a surface mount chip. Figure 4.5 shows the completed hardware for the security system. The final packing of the transmitting and receiving modules is shown in Figure 4.6.



Figure 4.5 Security system hardware



Figure 4.6 Final packaging of the transmitter and receiver units

5

Software Implementation

This chapter will briefly discuss the software required to complete the security system. As mentioned in section 3.7, this thesis required the hardware development of the system and a detailed software discussion can be read in the partnering thesis.

The software implementation can be divided into two sections: the embedded software of the microprocessor and the Graphical User Interface (GUI). Although the software packages available, to program the PIC, could be written in either Assembly or C, the language chosen to program the PIC microprocessor, was in Assembly. The reason to this choice can be read in the partnering thesis. Visual Basics (VB) was used to develop the Graphical User Interface on the computer/laptop. This was chosen as VB is simple to use and allow simply retrieval of digital information sent via the USB MOD2 device.

The two software sections operated the overall security system. When a particular push button was pressed, the transmitting PIC 16F876 was program to send the corresponding 8-bit data packet to the DIN pin of the Nordic nRF401 transceiver. Each push button is allocated a different 8-bit data packet to represent four different rooms. The receiving Nordic nRF401 transceiver demodulates the received RF signal back to its original 8-bit data packet and sends it, via the DOUT pin, to the receiving PIC 16F876. The Graphical User Interface is programmed to extract the digital packet, obtained by the receiving PIC 16F876, and to display the corresponding push button that was pressed.

.

6

Evaluation

This chapter will assess the final design of the security system by comparing it with the design and system specifications outlined in chapter 3.

6.1 Product Review

The important system requirement of using wireless FSK communications was successfully fulfilled. The transmitting and receiving range of the system reached approximately 20m.

A majority of the engineering design requirements, listed in section 3.5 were met. The transmitting module draws approximately 3.1mA current, in standby mode and 38.1mA, if in operating mode. The graph below shows the battery life of the transmitting module [21]. The batteries operating the transmitting end of the security system can last

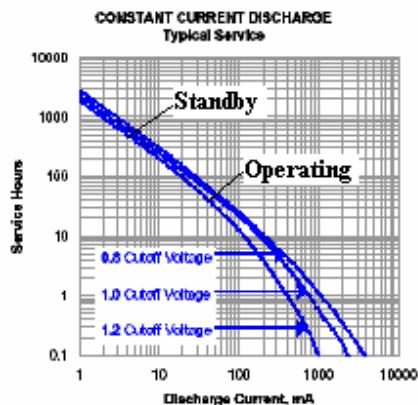


Figure 6.1 Battery lifetime

approximately 600 hours (25 days), in standby mode however only 50hrs if constantly in operating mode. The receiving end of the system is powered by the USB module via the computer and therefore the lifetime would be infinite, unless there was a power failure to the entire building's electrical circuitry. Due to these results, operating costs would be low.

The maintenance of the system is very low as it is only a prototype. The current system produced and implemented, was designed to show the new innovative idea of using FSK communications in a security system application. The prototype developed does not require any changes to the building's circuitry to operate. The reliability of the system was good, as the transmission of the RF signals was often instant and without error. However, at times, the push buttons needed to be held down, to provide proper contact for the microprocessor to detect.

The weight of the system, excluding the display unit, is light however the packaging size of the transmitting and receiving modules could have been smaller. This was due to the shortage of time left to package the modules and was caused by lack of time management. There was no set budget for the final cost of the project however the total cost of development is shown in Appendix F. As this system is a prototype, mainly to show the use of FSK communications, future developments can easily be implemented on the system. These developments will be discussed in chapter 7. Overall, the initial prototype system, shown on figure 4.4 was fulfilled and implemented meaning a successful design and development of the hardware.

6.2 Personal Assessment

The main goal of implementing a working product, to demonstrate at Innovation Expo was achieved. In addition, after 27 weeks of working on this thesis project, I believe I have learnt a lot in the progress of designing and implementing a product.

Because this system was broken up into two sections, hardware and software, it was aimed to have the hardware completed half way through the project. Unfortunately, due outside University commitments, this aim was not met, delaying the software development of the system. Luckily, a Nordic evaluation board was available for the

partnering thesis student to begin work on the software, for the system. Furthermore, the troubleshooting of the RF communication hardware took longer than expected.

My strengths are usually time management and organization, however too much time was spent on hardware selection and researching on the theory of Frequency Shift Keying. Time allocation to troubleshoot the PCB boards was under-estimated. In addition, many unexpected events occurred throughout the project making it difficult to follow the project plan, set out at the beginning of the project.

Other weaknesses included my attitude towards thesis and my lack of development skills. I would think of ways of improving the system however it was too late to implement a new design as time constraint was a major factor. The best solution to address my weaknesses will be by practical experience. The more projects I undertake, the more experience and knowledge in time management and industrial use requirements will be gained.

On a positive note, many skills were developed throughout the project. This mainly included the use of the Protel99 SE software package to implement PCB designs and the soldering surface mount components onto a PCB board. Additionally, I have learnt a lot after the completion of this thesis project. I have increased my knowledge of the FSK modulating and demodulating scheme and the functionality of the Nordic nRF401 transceiver.

7

Future Developments

7.1 Hardware Design Improvements

This system was designed to be a prototype of a security system using FSK communications. As the main objective was to use wireless communication, the system is of a simple design to demonstrate how the FSK modulation scheme could be used in the development of a security system. Furthermore, it was designed to allow the flexibility to tailor the system for individual needs. Nevertheless, a few improvements could be made to the prototype itself such as having a back up power supply for the receiving unit of the system, in case a power cut to the building's electrical circuitry was to occur. Integrating the digital and RF circuitry onto the one PCB board and decreasing the packaging are other possible improvements to the system prototype. LEDs (Light Emitting Diodes) could be placed on the PCB board, to show that the transmitting and receiving modules are powered.

In addition, the microprocessor's (PIC 16F876) memory capacity exceeded the need for the prototype therefore another microprocessor of smaller size and memory capacity could be found. Another improvement would be to implement four transmitting units, each consisting of one push button and a Nordic chip. This would demonstrate the different location of the sensor better.

The overall packaging of the individual modules can also be improved. This can be achieved by especially designing a case which would make the system more attractive.

7.2 The Dream

The development of a security system using FSK communications was successfully implemented, giving another solution to displaying the exact location of an intrusion and reducing the response time to the area. As mention above, the design is quite simple. This system can allow the best suited detecting device to be added, to cater for maximum security detection. There is possibly hundreds of detecting combinations, which can be added to the implementation this prototype security system, using FSK communications. The ultimate dream is to have this form of communication technique applied in security systems and to be used in the world.

8

Conclusion

The objective of this project was to design and implement the hardware of a security system using FSK communications, in particular using the Nordic nRF401 transceiver. Research was required into the functionality of the Nordic transceiver as well as the requirements of a security system.

The system was developed as a prototype which used push buttons to act as sensors. This was implemented to allow the option to apply the best suited sensor for the individually required security situation. The FSK modulation and demodulation technique was used to transmit information to a display unit, which showed the location of the security breach.

The design specifications of the system included low operating cost, ease of use and most importantly, reliability. The security system was successfully implemented and proved to be a method which could be used in the future. It is a flexible design which can be tailored to suit all situations which require security.

References

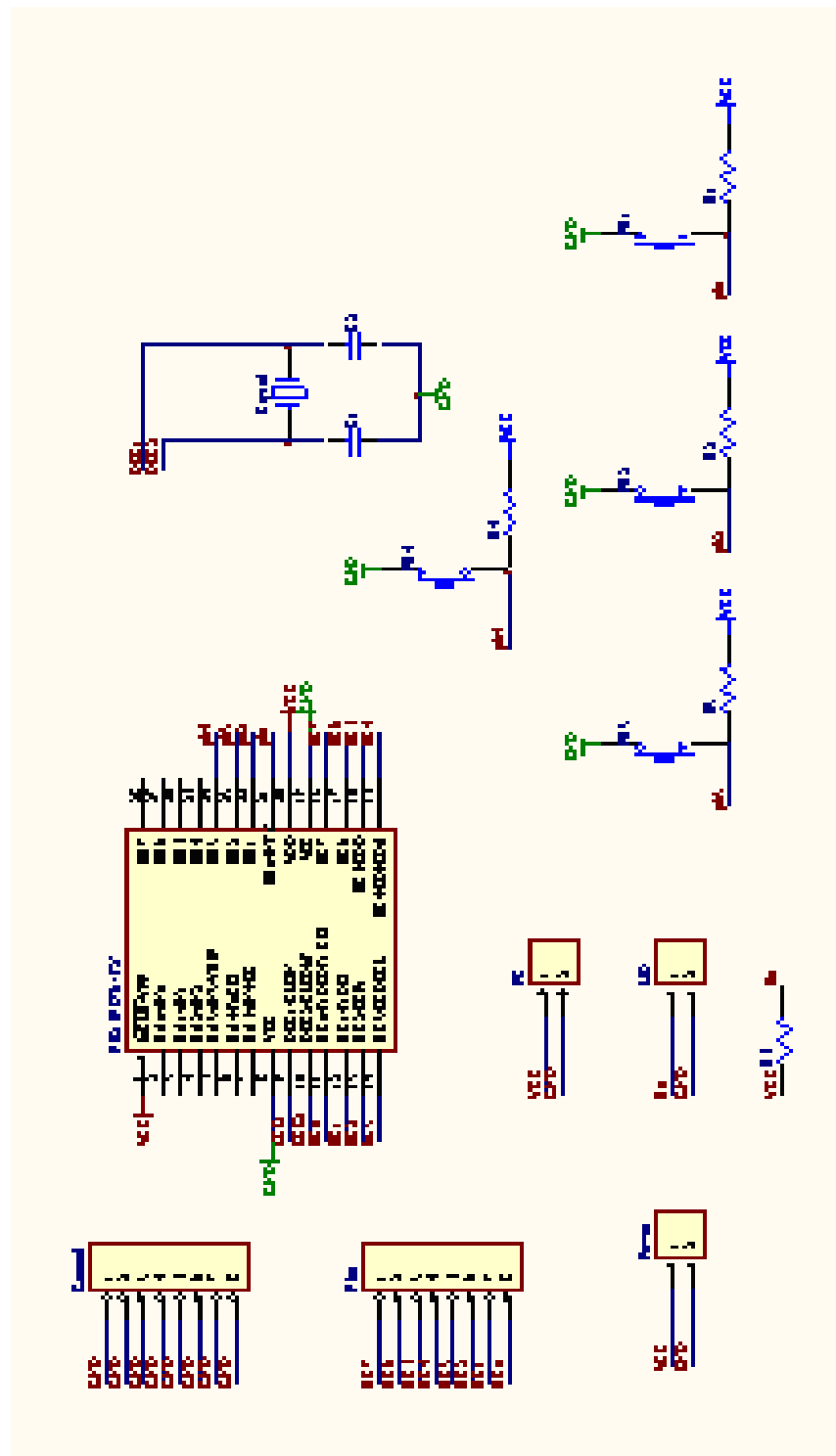
- [1] *Collins Compact English Dictionary*, England: HarperCollins Publishers; 1992.
- [2] Tectarget, "Frequency Shift Keying,"
http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci213936,00.html,
5 April 2003.
- [3] Safety and Security Center, "Security Systems DO Make a Difference,"
<http://www.wirelesshomesecurityalarmsystems.com/whyyouneedahomesecuritysystem.htm>, 15 October 2003.
- [4] A. Hardcastle, "BlueNanny – Child Monitoring System," Volume 2,
Thesis, University of Queensland, Queensland, Australia, 2002.
- [5] W. Brims, "Wireless ECG Monitors," Thesis, University of Queensland,
Queensland, Australia, 2002.
- [6] J. Homer, "Projects Lists,"
<http://www.itee.uq.edu.au/~projectdb/showProjects.php?offering=5&supervisor=homerj&status=all&discipline=&submit=Show+projects>, 3 March 2003.
- [7] R. W. L. Ng, "A Security System Using Wireless FSK Communications:
Software Aspects," Thesis, University of Queensland, Queensland, Australia,
2003.
- [8] Free On-Line Dictionary of Computing, "Frequency Shift Keying,"
<http://wombat.doc.ic.ac.uk/foldoc/foldoc.cgi?Frequency+Shift+Keying>, 10
October 2003.

- [9] L. W. Couch, *Digital and Analog Communication Systems*, USA: Prentice Hall, 2001.
 - [10] L. E. Larson, *RF and Microwave Circuit Design for Wireless Communications*, London: Artech House; 1997.
 - [11] The Security Installer, "Alarm Detection Devices,"
<http://www.thesecurityinstaller.co.uk/detectors.shtml>, 8 October 2003.
 - [12] Singer, "Security Systems,"
http://www2.singersl.com/singer/products/security_systems/security_systems.asp?pcode=SIN_HomeGard, 8 October 2003.
 - [13] Resource Protection Management, "Motion Detection Homepage,"
<http://www.rpmadvantage.com/Services/Security%20Systems/Alarm%20Systems/motiondetectors.htm>, 8 October 2003.
 - [14] Sapphire Alarms, "Burglar & Intruder Alarm System design,"
<http://www.sapphire-alarms.co.uk/deshelp.htm>, 4 April 2003.
 - [15] Microchip. "PIC 16F87x datasheet,"
<http://www.microchip.com/download/lit/pline/picmicro/families/16f87x/30292c.pdf>, 10 March 2003.
 - [16] Ravar, "USB MOD2 datasheet,"
<http://www.ravar.net/download/USBMOD2DS.pdf>, 7 July 2003.
 - [17] Texas Instruments, "TRF5901," <http://focus.ti.com/lit/ds/swrs014/swrs014.pdf>, 15 October 2003.
 - [18] Texas Instruments, "TRF6900," www.ti.com, 15 October 2003.
-

- [19] Nordic, “Transceiver nRF401,” www.nvlsi.no, 8 March 2003.
- [20] Nordic, “Design-in of RF circuits,” www.nvlsi.no, 8 March 2003.
- [21] Eveready Battery Company, “Engineering Datasheet,” www.data.energizer.com, 20 October 2003.

Appendix A

Schematic diagram of transmitting unit



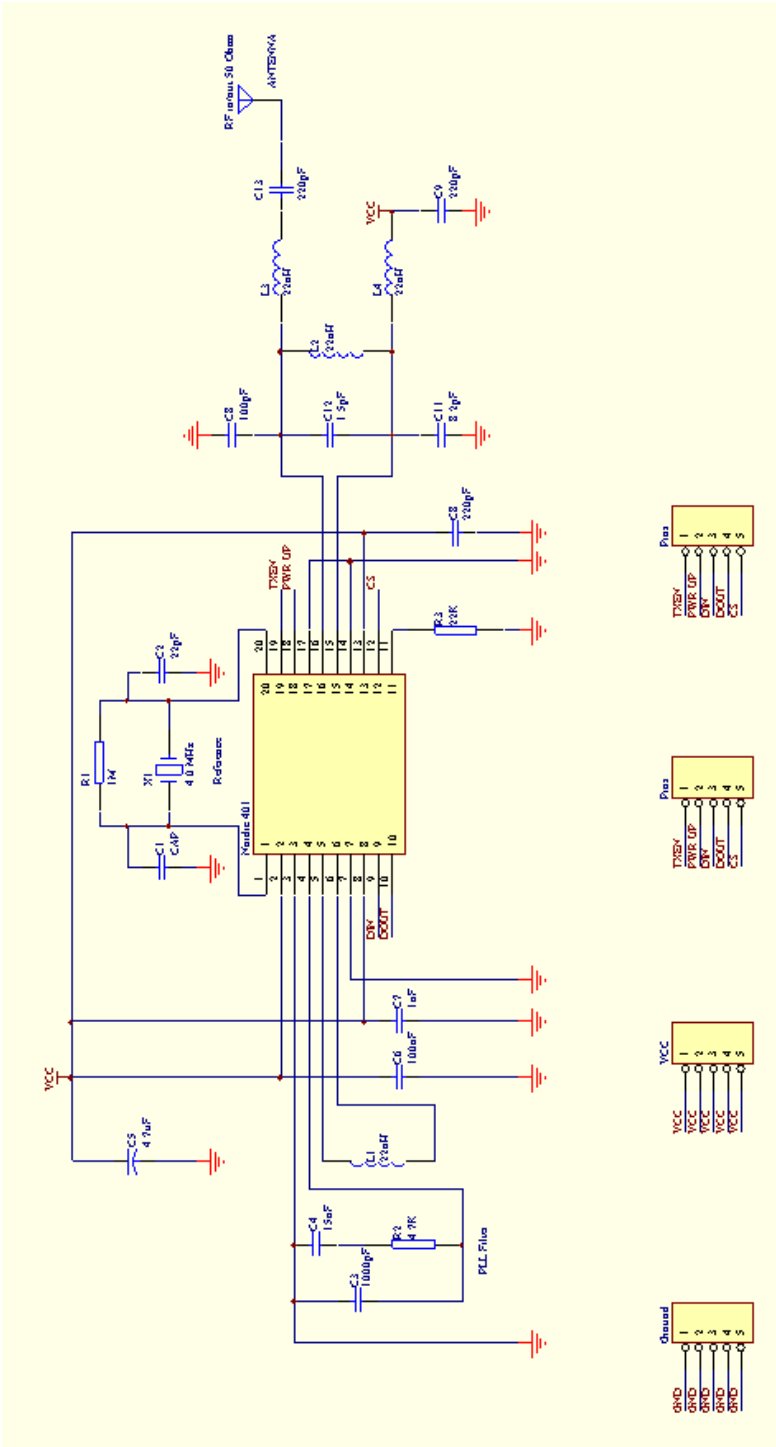
Appendix C

Pin function of the USB MOD2

Pin	Name	Description
1	Mount	Mounting support
2	Mount	Mounting support
3	No pin	-
4	No pin	-
5	GND	Ground
6	VCC	Power Supply
7	/RXF	High = do not read data in FIFO Low = data is available and can be read in FIFO
8	D7	Bi-direction data bus bit #7
9	D6	Bi-direction data bus bit #6
10	D5	Bi-direction data bus bit #5
11	D4	Bi-direction data bus bit #4
12	D3	Bi-direction data bus bit #3
13	D2	Bi-direction data bus bit #2
14	D1	Bi-direction data bus bit #1
15	D0	Bi-direction data bus bit #0
16	GND	Ground
17	GND	Ground
18	GND	Ground
19	EECS	Optional EEPROM – chip select
20	EECLK	Optional EEPROM – clock
21	EEDAT	Optional EEPROM – data I/O
22	VCC	Power supply
23	/RD	Low = Enable FIFO data byte High = Fetches next FIFO data byte
24	WR	Writes data byte into transmit FIFO buffer
25	/TXE	High = do not write into FIFO Low = data can be written
26	EEGT	Allows EEPROM contents to be accessed via data bus
27	EERQ	Requests EEPROM contents to be accessed via data bus
28	GND	Ground
29	No Pin	-
30	No Pin	-
31	Mount	Mounting support
32	Mount	Mounting support

Appendix D

RF circuitry schematic diagram.



Appendix E

Pin functions of the Nordic nRF401 transceiver

Pin	Name	Description
1	XC1	Crystal oscillator input
2	VDD	Power Supply
3	VSS	Ground
4	FILT1	Loop Filter
5	VCO1	Voltage Controlled Oscillator
6	VCO2	Voltage Controlled Oscillator
7	VSS	Ground
8	VDD	Power Supply
9	DIN	Data Input
10	DOUT	Data Output
11	RF_PWR	Transmitting power setting
12	CS	Frequency selection
13	VDD	Power Supply
14	VSS	Ground
15	ANT2	Antenna terminal
16	ANT1	Antenna terminal
17	VSS	Ground
18	PWR_UP	Operating or Standby Mode
19	TXEN	Transmitting or Receiving Mode
20	XC2	Crystal oscillator output

Appendix F

Total cost of security system prototype

Module	Component	Qty	Unit cost	Total Cost
RF Circuitry	0603 22pF capacitor	4	0.11	0.44
	(x2) 0603 1000pF Capacitor	4	0.11	0.44
	0603 15nF Capacitor	2	0.14	0.27
	3216 Dielectric Capacitor	2	0.94	1.88
	0603 100nF Capacitor	2	0.17	0.34
	0603 220pF Capacitor	6	0.12	0.70
	0603 8.2pF Capacitor	4	0.11	0.44
	0603 1.5pF Capacitor	2	0.11	0.22
	0603 22nH Inductor	8	1.84	14.72
	0603 1M ohm Resistor	2	0.04	0.08
	0603 4.7K ohm Resistor	2	0.04	0.08
	0603 22K ohm Resistor	2	0.04	0.08
	4MHz SMD Crystal (HC49/4HSMX)	2	5.07	10.14
	Nordic nRF401 transceiver	2	11.54	23.08
	SMA	2	8.34	16.68
	2xAA Batterys	2	2.50	5.00
	2xAA Battery Holder	2	2.48	4.96
	PCB Manufacturing	2	40.00	80.00
	20 WAY DIL	2	1.48	2.96
	Miscellaneous	1	1.00	1.00
Transmitting	20MHz crystal	1	2.91	2.91
Module	22pF ceramic Capacitor	2	0.06	0.12
	PIC 16F876 Microprocessor	1	22.08	22.08
	Push Buttons	4	1.52	6.08
	Miscellaneous	1	6.00	6.00
	PCB Manufacturing	1	30.00	30.00
	Casing	1	6.94	6.94
Receiving	20MHz crystal	1	2.91	2.91
Module	22pF ceramic Capacitor	2	0.06	0.12
	PIC 16F876 Microprocessor	1	22.08	22.08
	Ravar USB MOD2	1	50.00	50.00
	Miscellaneous	1	15.00	15.00
	PCB Manufacturing	1	30.00	30.00
	Casing	1	6.94	6.94
	GRAND TOTAL (excluding GST)			364.67