ECE 477 Final Report – Fall 2010
Team 7 – Digijock Home Security

From left to right: Linda Stefanutti, Zach Smith, Stuart Pulliam, and William Granger

Team Members:

#1: __Linda Stefanutti____________ Signature: ____________________ Date: _5/2/11__

#2: __Stuart Pulliam_____________ Signature: ____________________ Date: _5/2/11__

#3: __William Granger___________ Signature: ____________________ Date: _5/2/11__

#4: __Zach Smith________________ Signature: ____________________ Date: _5/2/11__

CRITERION	SCORE	MPY	PTS
Technical content	0 1 2 3 4 5 6 7 8 9 10	3	
Design documentation	0 1 2 3 4 5 6 7 8 9 10	3	
Technical writing style	0 1 2 3 4 5 6 7 8 9 10	2	
Contributions	0 1 2 3 4 5 6 7 8 9 10	1	
Editing	0 1 2 3 4 5 6 7 8 9 10	1	
		TOTAL	

Comments:

TABLE OF CONTENTS

Abstract	1
1.0 Project Overview and Block Diagram	1
2.0 Team Success Criteria and Fulfillment	2
3.0 Constraint Analysis and Component Selection	3
4.0 Patent Liability Analysis	8
5.0 Reliability and Safety Analysis	13
6.0 Ethical and Environmental Impact Analysis	19
7.0 Packaging Design Considerations	23
8.0 Schematic Design Considerations	28
9.0 PCB Layout Design Considerations	32
10.0 Software Design Considerations	36
11.0 Version 2 Changes	43
12.0 Summary and Conclusions	44
13.0 References	45
Appendix A: Individual Contributions	A-1
Appendix B: Packaging	B-1
Appendix C: Schematic	C-1
Appendix D: PCB Layout Top and Bottom Copper	D-1
Appendix E: Parts List Spreadsheet	E-1
Appendix F: FMECA Worksheet	F-1

Abstract

Digijock Home Security (DHS) is a home monitoring wireless network. It is capable of detecting smoke, motion, and noise as well as measuring temperature. While it has alarms for local alerts, the DHS system also contains a web server which can remotely warn the customer of threats through a website and text messaging.

1.0 Project Overview and Block Diagram

The Digijock Home Security (DHS) system provides security for home owners and owners of small businesses. The DHS consists of multiple remote sensor units (RSU) wirelessly relaying updates and alerts to a web server in the Central Monitoring Station (CMS). The RSU's detect threats in the form of motion, noise, and smoke. The RSU's can also measure temperature. This information is displayed on local LCD's on all of the devices and remotely displayed on a website hosted by the CMS. If an alert is detected, not only will all of the devices sound an alarm, but the CMS will also notify the customer in real-time via text messaging, email, and a website. The website allows the user not only real-time monitoring but also the ability to control the system remotely.

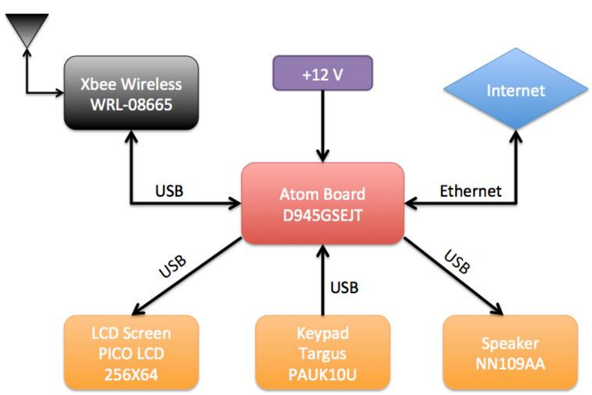

Figure 1.1: CMS Block Diagram

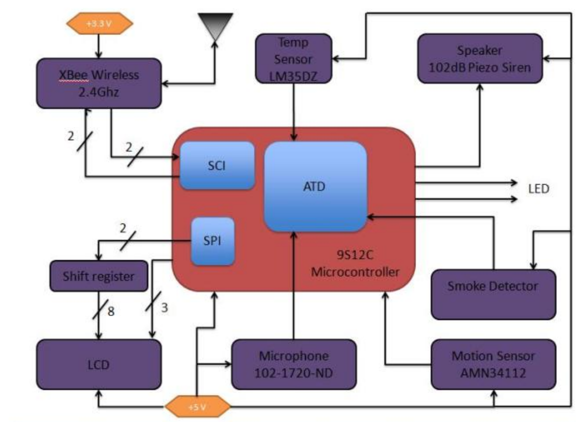

Figure 1.2: RSU Block Diagram

Figure 1.3: The Completed DHS

2.0 Team Success Criteria and Fulfillment

1. An ability to detect motion based on temperature variance, noise above 90dB, the presence of smoke/combustion with a photoelectric amplifier, and to measure temperature with a thermocouple amplifier.
    - The remote sensor units were successfully able to demonstrate this criterion.

2. An ability to encode and transmit data packets wirelessly to/from the remote sensors with a sensor identification address included in each packet.
    - The RSU’s were successfully able to demonstrate this criterion.

3. An ability to arm/disarm the security system and to alert the user (visually, audibly, and through email) of emergency conditions from both the CMS and the remote sensor units.
    - The CMS allowed the user to arm/disarm the system. All devices were able to alert the user of threats through all forms specified and additionally with text messaging.

4. Ability to time stamp events and log them in non-volatile memory on the CMS.
    - The CMS was successfully able to demonstrate this criterion.

5. An ability to display event logs and operational status on an LCD as well as a webpage hosted by an embedded web server.
    - The website could not be hosted on a dedicated IP, but this criterion was successfully demonstrated.

3.0 Constraint Analysis and Component Selection

3.1 Introduction

Our project is a home security system based on a central monitoring station (CMS) running a web server that connects to multiple microcontroller-based remote sensor units (RSU). Wireless modules will allow bidirectional communication between the RSUs and the CMS to share useful information. Our PSSCs are:

1. An ability to detect motion based on body infrared emission, noise above 90dB, the presence of smoke/combustion with a photoelectric amplifier, and to measure temperature with a thermocouple amplifier.
2. An ability to encode and transmit data packets wirelessly to/from the remote sensors with a sensor identification address included in each packet.
3. An ability to arm/disarm the security system and to alert the user (visually, audibly, and through email) of emergency conditions from both the CMS and the remote sensor units.
4. An ability to time stamp events and log them in non-volatile memory on the CMS.
5. An ability to display event logs and operational status on an LCD as well as a webpage hosted by an embedded web server.

3.2.0 Design Constraint Analysis

In this design we will consider the following constraints: protocols supported and number of pins available on the microcontroller, compatibility of the wireless system with the microcontrollers and computer board, ease of integrating the wireless system with a PCB, power supply needed by each device, ease of use in interfacing the computer board with required peripherals, ease of running a web server, email server, and a database from the computer board, and size and cost of the products and of the packaging.

3.2.1 Computation Requirements

<u>Central Monitoring Station</u> (Figure 1.1): The computer board will be connected to a USB keypad. The client will use it to check and change the status of the RSUs. The LCD screen will guide the user to a menu of different actions, performed only with the use of the CMS password: 1) Deactivate (only the smoke detector is on), 2) Activate, 3) Test the alarm system (triggering the smoke sensor), 4) Change password.

It will also be able to time stamp events and log them in non volatile memory in order to give the user an event history of the house. In case of emergency, the CMS will emit an alarm sound through two speakers and will send an email and a text to the user about the type of emergency detected.

Remote Sensor Units (Figure 1.2): The microcontroller in each RSU will manage the data from the different sensors which detect the condition of the room. Through the use of the RTI protocol, the RSU will send to the CMS updated information about the room's status every second. In case of emergency, the following actions will be performed:

1. Alarm information will be sent to the CMS which will relay it to the other RSUs
2. Alarm messages will be displayed on the units LCDs
3. Speaker turn on

The system will return to the idle state only when the emergency trigger (smoke) is no longer present or after a command from the CMS or the web server is sent (1. Deactivate).

3.3.2 Interface Requirements

Peripherals:

- Noise detector: made with an electrets microphone and an amplifier circuit. Voltage need: 5V. One ATD I/O pin needed for communication with microcontroller [1].
- Temperature sensor: made by a thermocouple amplifier. Voltage need: 5V. Analog output, one ATD pin needed for communication with microcontroller [2].
- LCD: two rows for sixteen characters with backlight. Voltage need: 5V. Current: 20mA (backup light off), 80mA (light on), fourteen I/O pins [3]. It will also need a 8-bits shift register to communicate with the microcontroller.
- Speaker: controlled by a digital I/O pin. Impedance ~8 ohm. Voltage need: 5V.
- Smoke detector: photoelectric detector made with infrared LED and a smoke chamber. Analog output, one ATD pin needed for communication with microcontroller. Voltage need: 5V.
- Motion sensor: it detects the infrared emissions of human body. 10m range with a mirror of 110^{o} horizontal and 93^{o} vertical. Operating voltage: 3(Min)-6(Max) volt, current consumption: 170 μA, one pin needed for interfacing with microcontroller (digital I/O) [4].

- Wireless system: Xbee module, voltage need: 3.3 V.

3.2.3 On-Chip Peripheral Requirements

We will need eight digital I/O pins, one each for: motion sensor, serial LCD (3 pins), bicolor LED (2 pins), speaker and power failure signal from the backup battery. Four pins for SCI protocol: Xbee module. Two pins for SPI protocol: serial LCD. Four pins for ATD protocol: microphone, thermocouple, smoke sensor and backup battery level. In conclusion we will need a total of fourteen pins for peripherals communication. The computer board will need four USB ports for the LCD, speaker, wireless module and the keypad. It also needs an Ethernet port.

3.2.4 Off-Chip Peripheral Requirements

Our design is based on the use of sensors that can be directly connected to the PCB and does not need any intermediate device between the sensors and the microcontroller. For this reason we do not list any off-chip peripherals.

3.2.5 Power Constraints

Our project is designed to use wall power for the CMS and for the two RSUs. The RSUs have also a backup battery system that will be activated in case of power failure. The microcontroller will receive a digital signal from the circuit that notifies the power problem .At the same time the ATD channel will sample the level of the battery left (displayed on the RSU LCD). The battery will be an alkaline 9V battery.

3.2.6 Packaging Constraints

The first packaging constraint will be related to the weight and size of the RSUs. These units are supposed to be hung on a wall, so the total weight of each unit should be below ~500 g. Moreover the packaging of the two RSUs must not interfere with the wireless communication, the detection of smoke, and temperature measurement. Ideally, the thermocouple will be located far from any internal source of heat. Additionally, the RSU should be located close to window or doors and far from home phones in order to detect an intruder and not be triggered by the phone ringing. There are no major packaging constraints for the CMS except for being of reasonable size.

3.2.7 Cost Constraints

On the market there are already several home security systems that can potentially compete with ours. Most of them (like the 2GIG-CNTRL2KIT5 for $459.75) are composed of a standard package to which the user can add different accessories for various kinds of alarm detection. The standard package is composed of door/window contacts, motion detection, and a key ring remote control. Other detectors like smoke or noise can be added for an average cost of $70 per unit. In this sense, our project tries to minimize the cost (especially packaging and microcontroller count) by including all these sensors in a single package.

3.3.0 Component Selection Rationale

Our major components are the computer platform, microcontroller, and wireless module. For the computer platform we have taken into consideration the following models: an Intel Atom board (D945GSEJT) and an Asus WL-500GP wireless router.

The Intel Atom board is capable of running either Windows XP or Linux, which both support most software and hardware. However, the WL-500GP router is only capable of running DD-WRT, which is a bare-bones distribution of Linux. It would be a challenge to find DD-WRT drivers for the specialized hardware we need for the computer platform. Documentation is readily available for both platforms. Both platforms are capable of running a web server and an email server. The router would need external storage for storing a database. The router is only able to connect to an 802.11 network, but the Atom board can connect to 802.11 or 802.15.4.

The router is both smaller and cheaper than the D945GSEJT motherboard, which is advantageous, but due to its shortcomings in the previously mentioned areas, it is overall the inferior option for our project. We have decided to use the D945GSEJT motherboard.

For the microcontroller we have taken into consideration the following models: Freescale MC9S12C and Microchip PIC18F25K22.

To determine which model better suits our needs; we had to consider the amount of memory (flash and ram) available, the number and the type of protocols supported, and the total number of pins available for each protocol. In terms of amount of memory available, both present very similar specifications (32 Kb flash, 2Kb SRAM). Since our project does not require huge memory capacity, both models meet our needs.

The MC9S12C offers eight ATD channels, six PWM channels, eight timer channels, and one UART. It supports an input voltage range from 2.97 to 5.5 volt and is available as a 48-pin LQFP [5]. This is more than enough pins. The Freescale microcontroller supports background debug mode, which is useful during development and debugging.

The PIC model offers 17 ATD channels with ten bit resolution, three timer channels, supports SPI communication and four PWM channels [6]. It has an operating voltage between 1.8 and 5.5 volts and a total pin count of 28. This is more than enough pins. Since both models suit our needs, we have decided to pick the MC9S12C. The reason is related to the fact that we have previously used this model, so our familiarity with the technology will help us to use its resources more efficiently. Furthermore, the BDM capability is appealing.

For the wireless communication module we have taken into consideration: a MRF24WB0MA Wi-Fi module and a WRL-08665 Xbee module.

The MRF24WB0MA Wi-Fi module from Microchip is an IEEE 802.11b compliant transceiver designed to easily interface with microcontrollers using an SPI connection. Since it uses an 802.11b wireless network, it is simple to connect to the Atom board using a USB Wi-Fi dongle. The range is up to 1300 feet (396.24 m). It connects to a PCB via through-holes.

The WRL-08665 Xbee module from Digi implements the ZigBee IEEE 802.15.4 standard for Low-Rate Wireless Personal Area Networks. It interfaces with a microcontroller via SCI. A ZigBee USB dongle is available for connecting the Atom board to the 802.15.4 network and the range is up to 300 feet [7]. It connects to a PCB via through holes. Xbee modules can operate in transparent mode (which acts like a simple SCI connect) and API mode, which allows the host controller to interact with the networking capabilities of the module.

In our final decision we have considered that the Xbee's 802.15.4 is specifically designed for uses such as wireless home security systems, so it is better suited for our application than 802.11b. The MRF24WB0MA has a better range, although if the range is a limitation for the Xbee, there is a more powerful Xbee model available. By default the API includes a module-specific address field, thus eliminating the need to include dip switches to identify the remote sensor units. In conclusion we have decided to use the Xbee technology.

3.4 Summary

In this report we have considered several constraints and problems that we must meet in designing our home security system. These constraints are related to the type of protocols used in interfacing the peripherals to the microcontrollers, the adaptability of the wireless system to the microcontrollers as well as to the computer board, and the operating specifications of the entire system. After a thorough analysis of the components available in the market and consideration of our ability to utilize them in our design, we made a final decision on which parts to use.

4.0 Patent Liability Analysis

4.1 Introduction

Digijock Home Security (DHS) is a home security system that implements the standard lines of protection from fire and burglary. With this system in place, it will monitor several aspects of common fire and burglary scenarios and relay the information to the Central Monitoring Station (CMS), which runs a web server. This functionality will allow the user to login to the web server and view information and statistics. The user may also choose to communicate directly with the CMS with a keypad and LCD interface. This will allow the user to set the security system into multiple modes of operation. The remote sensor units will be controlled by a microcontroller, which will send updates via Xbee wireless to the CMS. The CMS stores the information in a database, which will be accessed by a .NET web application.

4.2 Results of Patent and Product Search

Several patent search engines were used to find and locate patents that were very similar to our design project. The primary to two engines included: freepatentsonline.com and google.com/patents. Key search words that I used to identify patents included: "Wireless Home Security", "Home Security", "Wireless Fire Detector", and "Digital Smoke Detector".

2.1) Patent Application 10,909,354 - "Home Security System" [8] Filed Date: Aug 3, 2004

A home security controller that is connected to a home network, it monitors and collects data and then determines and alerts when a state of emergency occurs. The controller possesses a remote control function that allows the devices in the home to be operated through a remote control signal via an external network.

Claim 1: "a home security controller for collecting monitor data from said monitoring means via the home network and determining when a state of emergency occurs, said home security controller possessing a remote control function that allows devices in the home to be operated through a remote control signal via an external network". [8]

Patent Application 10,909,354 was published on Feb 2, 2006. [8]

2.2) Patent 5,705,988 – "Photoelectric Smoke Detector" [9]   Filed Date: July 8, 1996

A photo-emitter and a photo-sensor are used to detect the presence of smoke. A light beam produced by the photo-emitter is directed at the photo-sensor providing an analog signal voltage proportional to the light reflected out by the smoke particles. It also specifically mentions using an Analog-to-Digital converter to interpret the signal into a digital representation.

Claim 1: **"**A smoke detector including a digitally stored alarm threshold and comprising:

> a photo-emitter and a photo-sensor, said photo-emitter producing a light beam and said photo-sensor providing an analog signal voltage proportional to light reflected out of said beam by smoke particles; an analog-to-digital converter converting said analog sample to a digital representation of said sample; and, a control comparing said digital representation to said digitally stored alarm threshold;". [9]

Patent 5,705,988 was published on January 6, 1998. [9]

2.3) Patent Application 20,080,007,403 – "Home Security System Intergrading Local Wireless…" [10]   File Date: June 25, 2007

This Patent publicizes that it's a home security system that is capable of linking to an external network using N terminals. To link the terminals together it uses wireless communication using the IEEE 802.15.4 standard, which is the standard for all Xbee and Xbee-pro RF modules. An external network is defined by either a radio telecommunication system network, a wireless wide area network, or the Internet.

Claim 1: "A home security system capable of linking to an external communication network, N terminals being capable of linking to the external communication network, N being a natural number, said home security system comprising of M sensing units, each of the M sensing units comprising; a transmitting module, electrically connected to the sensor, for transmitting the trigger signal in a wireless local communication protocol;" [10]

Claim 2: "The home security system of claim 1, wherein the wireless local communication protocol is an IEEE 802.15.4 standard". [10]

Patent Application 20,080,007,403 was published on January 10, 2008. [10]

2.4) Patent 7,755,480 – "Security System" [11] File Date Jan 30, 2006

This Patent mentions that a Server A is connected to an external network that can connect to a Server B. Server B stores information that is collected from the system and can be accessed through Server A.

Claim 2: "A security system according to claim 1, including: a first server connected via a network to a second server, a second server for storing information collected from multiple nodes, wherein the first server is capable of accessing information stored in the second server by storing storage destination information showing the storage destination of the information, and the first server or the second server detects matching conditions." [11]

Patent 7,755,480 was published on July 13, 2010.

4.3 Analysis of Patent Liability

3.1) Patent Application 10,909,354 - "Home Security System" [8]

The Digijock Home Security System could be infringing upon this patent with it monitoring external events and having the system being triggered off events that are deemed to be of a security risk. Once an event is triggered it will sound an alarm and it will be in a state of emergency. This is specifically mentioned in the Patents claim, but I feel this is too broad of terminology. It does not say anything how it gets into this state of emergency other than when the system detects an abnormality, again very broad.

The second part of this Patent is having the system controlled by a remote system hooked up to an external network. Our system could possibly be infringing on this Patent because we are connecting our system up to a web server that will give access to the user in an offsite location. Obviously the web server is connected to an external network to give it access anywhere in the world if connected to the Internet. It also allows the user to control the state of the system when having access to the web server.

Both of these specific cases could be a possible patent infringement on the doctrine of equivalence, but I don't believe that any of these key features warrant the infringement. These are all very common practices in software, which would make it impossible to control.

3.2) Patent 5,705,988 – "Photoelectric Smoke Detector" [9]

The Digijock Home Security System is 100% infringing on this Patent. We are literally using the exact same way in our remote sensors to detect the presence of smoke. We too are using a photo-emitter and a photo-sensor. It will be housed in a chamber that will allow entrance for the smoke particles. We have the emitter directed towards the sensor, and when there is no smoke it will detect the presence of the infrared signal, which creates a high resistance that brings our voltage to an extremely low voltage. If smoke does enter the chamber the light will deflect away from the sensor and the voltage will increase.

This Patent also specifically mentions the use of an Analog-to-Digital converter to convert the signal into a digital representation. Our remote sensor will perform an ATD conversion on this signal and if it exceeds a certain predetermined threshold it will set a smoke flag. This smoke flag will then alert the Central Monitoring Station of an event and trigger the alarm.

By our use of a photoelectric smoke detector and using the ATD to convert this value into a digital representation we are in violation of this Patent via literal infringement. This will cause a need for action by us to use this method of detecting smoke in our design project.

3.3) Patent Application 20,080,007,403 – "Home Security System Intergrading Local Wireless…" [10]

The Digijock Home Security System is literally infringing on this patent. This patent clearly states that it uses the standard IEEE 802.15.4 wireless communication channel for the purpose of a Home Security System. All Xbee modules use this standard wireless protocol. For our system we are using the same standard protocol for our means to wirelessly communicate with the Central Monitoring Unit and each remote sensor for the purpose of a home security system.

Our Home Security System is in direct violation of this Patent via literal infringement. We use the same wireless protocol for the exact same application. This will cause a need for action by us to use this way of wirelessly communicating with the remote sensors in our design project.

3.4) Patent 7,755,480 – “Security System” [11]

The Digijock Home Security System is infringing on this patent by Doctrine of Equivalence. The application is the same but it doesn’t specifically mention how Server A connects to Server B and get the information as well as it doesn’t mention how the information is stored. It is very similar in nature that we are accessing our web server that has the information stored in a database that the user can remotely access from another computer to check in on the security of their home via a website application written in C# and aspx. But again it doesn’t specifically mention how it goes about doing these operations in the patent. This will cause for a need for action from our team to handle this patent.

4.4 Action Recommended

Before the Digijock Home Security System is put into mass production, a patent attorney should be contacted and consulted in regards to all the patents reviewed in sections 2.0 and 3.0. There are two patents that have been identified above that are likely to have infringed upon by our design. For Patent 5,705,988, Patent 7,755,480, and Patent Application 20,080,007,403, it is likely that licensing is our best option.

4.1) Patent 5,705,988 – “Photoelectric Smoke Detector” [9]

I believe the best thing to do is contact a patent lawyer and get his thoughts on the matter, but I would assume the lawyer would want our team to contact the owner of the patent and see if they would be willing to license it to us. After doing a little bit of research I couldn’t find any useful information on the owner. I was hoping that this patent was designed for your average, simple home fire detector and had nothing to do with the home security side of things. I would believe that if they were not in that specific market then the owner would be more willing to license out the patent to us.

4.2) Patent Application 20,080,007,403 – "Home Security System Intergrading Local Wireless…" [10]

This specific Patent is very specific on its means of using the IEEE 802.15.4 wireless standard for a Home Security System. Something that stands out is the fact that they mention ZigBee (Xbee), which means that I don't believe they can use someone else's product in a patent unless they are the owners of the ZigBee module. I would need to do further investigation, but I think our best option is to again contact a lawyer and get his/her input on the matter. If the lawyer believes we can take them to court and get the patent nullified then I think that would be our best option. Otherwise, we would have to contact them and ask them to license it out to us for our project.

4.3) Patent 7,755,480 – "Security System" [11]

Our design project is infringing on this patent due to having a home security system connected to a server that stores the information and another server accesses the server remotely or from an external location. We will need to contact a lawyer and get his/her advice on what to do in this matter. I think that we need to contact the owners of this patent ask for a license to use this method of storing and sharing information.

4.5 Summary

There are many patents that exist in similar/same applications as the Digijock Home Security System. After extensive research and looking up many different patents it is concluded that our Security System does in fact literally infringe on two patents. It would be in our best interest to consult a patent lawyer, but the Digijock Home Security plans to license the technology from the patent owners.

5.0 Reliability and Safety Analysis

5.1 Introduction

Digijock Home Security (DHS) is a multi-faceted home monitoring system that is designed to detect both fire and intruders using Remote Sensing Units (RSUs), to log sensor readings on a Central Monitoring Station (CMS), and to notify the homeowner of incidents via e-mail and

SMS messages. Data collected by the RSUs include temperature, motion, noise, and smoke measurements, and the data are transmitted wirelessly back to the CMS.

Because DHS is designed to protect users facing potentially life-threatening situations, it is of utmost importance that it be both safe and reliable, especially in detecting fires. Presented below are two analyses of the overall reliability and robustness of DHS's system design. The focus of the analysis is the circuit design of the RSUs, which are manufactured using PCBs.

5.2 Reliability Analysis

To analyze the reliability of DHS, certain circuit components have been chosen for statistical modeling of their probability of failure. The criterion for choosing the components is to select specific ones that are perceived to have a higher likelihood of failure based on their function in the circuit or the inherent complexity of their design/manufacturing. To perform the analysis, guidelines from the DoD Military Handbook: Reliability Prediction of Electronic Equipment are used. This analysis technique is a widely used method for reliability prediction [12].

The four parts chosen for analysis are listed below along with the reasons for selecting them:

- The MC9S12 MCU is chosen by virtue of it being a high complexity IC (includes a 16-bit core, 128KB Flash EEPROM, 4KB SRAM, and numerous sub modules) [13]. Furthermore, it is one of the more significant sources of heat generation in our circuit.
- The 74LVC8T245 voltage translator is chosen because it is a high complexity IC (8-bit dual supply translating transceivers) [14]. Also, it has a high pin count at 24 pins.
- The LM340T5/LF33CV voltage regulators are chosen because they will be operating above room temperature due to the power dissipation of voltage regulators.
- The 2N3904 NPN BJT is chosen because one of these transistors will be used in the highest-current trace of the circuit.

The models chosen for each part for MIL-HDBK-217F reliability analysis are listed below:

- The MC9S12 is modeled as a 16-bit MOS microprocessor
- The 74LVC8T25 is modeled as an MOS digital gate/logic array with fewer than 100 gates because according to the datasheet, 18 logic gates make up this MOS device [14].
- The LM340T5 and LF33CV are modeled as low-frequency diodes because the handbook specifies that this is the model to use for voltage regulators. One device is a 5V regulator and the other is a 3.3V, but since they are modeled equally, they are analyzed in unison.

- The 2N3904 is modeled as a low frequency bipolar transistor since it is operating at a frequency under 200 MHz (the highest frequency signal in the circuit is 25 MHz).

Below are pairs of tables and calculations that are used for the reliability analysis of the four components. The tables include the parameters used in the calculations along with the specific justification for the chosen values. The calculations themselves are to solve for λ_p, which represents the predicted number of failures per 10^6 hours, and the mean time to failure (MTTF), which is the average amount of time that passes before the device irreparably fails.

Table 5.2.1: Reliability analysis parameters for MC9S12 microcontroller [12].

Parameter Name	Description	Value	Comments
C_1	Die complexity failure rate	0.28	MOS microprocessor with up to 16 bits
π_T	Temperature factor	0.49	Operating temperature up to 45 Celsius
C_2	Package failure rate	0.032	Non-hermetic SMT with 48 pins
π_E	Environment factor	2.0	Ground fixed
π_Q	Quality factors	10	Commercial product
π_L	Learning factor	1.0	Product in production >2 years

λ_p and MTTF calculation for MC9S12:

$\lambda_{p1} = (C_1 \cdot \pi_T + C_2 \cdot \pi_E) \cdot \pi_Q \cdot \pi_L = \mathbf{2.012}$ failures per 10^6 hours

$MTTF = \frac{1}{\lambda_{p1}} = \mathbf{497,000}$ hours

Table 5.2.2: Reliability analysis parameters for 74LVC8T245 voltage translator [12].

Parameter Name	Description	Value	Comments
C_1	Die complexity failure rate	0.01	MOS digital gate/logic array with <100 gates
π_T	Temperature factor	0.49	Operating temperature up to 45 Celsius
C_2	Package failure rate	0.0062	Non-hermetic DIP with 14 pins
π_E	Environment factor	2.0	Ground fixed
π_Q	Quality factors	10	Commercial product
π_L	Learning factor	1.0	Product in production >2 years

λ_p and MTTF calculation for 74LVC8T245:

$\lambda_{p2} = (C_1 \cdot \pi_T + C_2 \cdot \pi_E) \cdot \pi_Q \cdot \pi_L = \mathbf{0.173}$ failures per 10^6 hours

$MTTF = \frac{1}{\lambda_{p2}} = \mathbf{5,780,000}$ hours

Table 5.2.3: Reliability analysis parameters for LM340T5/LF33CV voltage regulators [12].

Parameter Name	Description	Value	Comments
λ_b	Base failure rate	0.0020	Value specifically for voltage regulator
π_T	Temperature factor	1.5	Operating temperature up to 45 Celsius
π_S	Electrical stress fracture	1.0	Value specifically for voltage regulator
π_C	Contact construction factor	1.0	Metalurgically bonded contacts
π_Q	Quality factors	8.0	Plastic package
π_E	Environment factor	6.0	Ground fixed

λ_p and MTTF calculation for LM340T5/LF33CV:

$\lambda_{p3} = \lambda_b \cdot \pi_T \cdot \pi_S \cdot \pi_C \cdot \pi_Q \cdot \pi_E = \mathbf{.144}$ failures per 10^6 hours

$MTTF = \frac{1}{\lambda_{p3}} = \mathbf{6,940,000}$ hours

Table 5.2.4: Reliability analysis parameters for 2N3904 NPN BJT transistors [12].

Parameter Name	Description	Value	Comments
λ_b	Base failure rate	0.00074	NPN transistor
π_T	Temperature factor	1.6	Operating temperature up to 45 Celsius
π_A	Application factor	1.5	Linear amplification
π_R	Power rating factor	1.0	For rated power of 1 W
π_S	Voltage stress fracture	0.11	Applied V_{CE} 5.0V / Rated V_{CEO} 40V = .125 [5]
π_Q	Quality factors	6.0	Plastic
π_E	Environment factor	6.0	Ground fixed

λ_p and MTTF calculation for 2N3904:

$\lambda_{p4} = \lambda_b \cdot \pi_T \cdot \pi_A \cdot \pi_R \cdot \pi_S \cdot \pi_Q \cdot \pi_E = \mathbf{0.007}$ failures per 10^6 hours

$MTTF = \frac{1}{\lambda_{p4}} = \mathbf{143,000,000}$ hours

λ_p and MTTF calculation for entire circuit (note λ_{p3} is included twice because there are two voltage regulators in the circuit):

$\lambda_p = \lambda_{p1} + \lambda_{p2} + 2 \cdot \lambda_{p3} + \lambda_{p4} = \mathbf{2.21}$ failures per 10^6 hours

$MTTF = \frac{1}{\lambda_p} = \mathbf{452,000}$ hours

According to the calculations, the least reliable component is the microcontroller. This is reasonable since it is the most complex component of the circuit, it has the most number of pins (twice as many as the next highest component), and it also will operate somewhat above room temperature due to its higher power dissipation. The second-most complex device based on design and pin count, the 74LCD8T245, is also the second least reliable. The LM340T5/LF33CV is only slightly more reliable. Although less complex, the heat generated by its operation would decrease its lifespan. The 2N3904 is significantly more reliable than the rest, nearly achieving the probability of "never" failing (defined as 10^{-9} failures per hour of operation) [15].

With the λ_p of the entire circuit being 2.21 failures per 10^6 hours, if there were one million units in use, a product failure would occur approximately every 27 minutes. Since the DHS is intended to warn users of imminent dangers such as an intruder or a fire, this level of failure could lead to many lives being jeopardized. Based on the current design and analysis, DHS is an unsafe product. It would therefore be important to pursue means of reducing the failure rate.

There are several analysis refinements that would realistically improve the predicted reliability of the design. One would be to choose a lower maximum operating temperature. Since DHS is intended for indoor use, it does not generate too much heat itself, and the product has numerous ventilation holes in the enclosure, the chosen maximum temperature of 45 Celsius could reasonably be decreased to 30 Celsius. Since decreasing operating temperature lowers all the individual λ_p values, the overall λ_p would decrease significantly. Second, when choosing the package failure rate parameter for the MC9S12, the value chosen was for an IC with 64 pins (the closest value available), whereas the microcontroller only has 48 pins. Using a more accurate value would increase the reliability prediction since a lower pin count yields higher reliability. Third, for the 2N3904, a conservative power rating factor of 1W was chosen (again, the closest value available), while the transistor is actually rated for .625W [16]. The lower power rating factor would yield a higher reliability calculation. Fourth, some components are subject to a duty cycle factor due to the fact that they are not always enabled (for example, the speaker amplifier). The application of a duty cycle factor would decrease the amount of time the component is in use and therefore increase its predicted lifespan. Fifth, a quality factor of ten should be reevaluated because it is an overly-harsh value based on legacy manufacturing variances.

For design modifications that would improve reliability, a new microcontroller would have to be chosen. The current model is much too far from the necessary failure rate. A replacement model should have fewer pins since the design does not use all the pins on the current microcontroller. It should also have an 8-bit core to reduce the die complexity failure rate factor. Also, redundant systems and internal fault detection mechanisms could drastically improve the reliability of the design. A final design option would be to remove the function of detecting smoke from the microcontroller itself (which is possible) so that this high-criticality function is not impacted by the microcontroller's higher failure rate.

5.3 Failure Mode, Effects, and Criticality Analysis (FMECA)

For FMECA analysis, the design is divided into functional blocks and then the individual blocks are analyzed for their various failure modes. The propagation of this failure throughout the rest of the system is examined, and the effect on the operation of the system is studied. This technique helps identify weaknesses of the design and can potentially suggest changes that will eliminate the weaknesses [15].

There are four functional blocks that have been identified in DHS: the microcontroller circuitry, the power circuitry, the peripheral circuitry, and the wireless circuitry (see schematic in Appendix A). In Appendix B, there is a detailed FMECA analysis of the possible failure conditions of each functional block as well as the causes and effects of each of the failures. They are also assigned a criticality level based on their impact on the function of the overall system. Three different criticality levels have been identified: high, medium, and low. High criticality is defined as a failure that causes loss of local smoke detection functionality. If the unit loses the ability to warn the user about the presence of smoke, the user is placed in a potentially life-threatening situation. Because of the severity of this scenario, the acceptable failure rate, λ, must be "never", i.e. $\lambda < 10^9$. Medium criticality is defined as a failure that causes a loss or reduction in effectiveness of detecting a break-in. As a result of such a failure, the user would not be able to arm the alarm when he or she leaves the house. Because this scenario is still dangerous, an acceptable failure rate must be below $\lambda < 10^7$. A low criticality failure is one that causes inconvenience to the user, but does not present any degree of danger (i.e. temperature reading being incorrect). Since this scenario is inconvenient yet not harmful, an acceptable failure rate must be below $\lambda < 10^5$.

5.4 Summary

Both analysis techniques have shown that in its current state, the design is not reliable enough. This is a result of having parts with a relatively high failure rate and a design that lacks system redundancy. These deficiencies would need to be eliminated in order to increase the reliability of DHS to acceptable levels. Although it does benefit from being able to instantly notify the user of certain failures via e-mail and SMS, this is a less-than-ideal solution. Furthermore, there are several high-criticality failure modes that are unable to be detected by any means other than direct observation by the user. For these reasons, further design iterations would need to be undertaken in order for DHS to be qualified for use in its intended capacity.

6.0 Ethical and Environmental Impact Analysis

6.1 Introduction

The Digijock Home Security (DHS) system is a wireless network of remote sensor units (RSU) that communicate with a central monitoring station (CMS) to provide security and peace of mind to the user. In order to bring peace of mind, the user needs to know how he/she is actually being protected by the DHS. One of the problems with one of the security aspects is that in order to alert the customer as soon as possible, the customer must enter some personal information such as a phone number. Since this information is contained within a web server, this may leave their information vulnerable. Another concern of the customer would be the environmental impact of the device. While the customer may have concerns with the manufacturing and ultimate disposal of the device, the main concern of the customer will be how much power the device consumes and how often the battery will need to be replaced. These ethical and environmental concerns must be addressed before this product can go to market.

6.2 Environmental Impact Analysis

From its manufacturing, lifetime, and to its inevitable disposal, every device of the DHS will have an impact on the environment. This report will focus on three components that every device shares: the plastic covering, the liquid crystal display (LCD), and the printed circuit board (PCB). The RSU focus will expand to include a battery. These four components will have the most significant impact on the environment.

The DHS plastic coverings are made of ABS plastic. This plastic is flame retardant [17] which will allow our devices to survive a long time in the event of a fire emergency. It is also very durable allowing it to take concussive blows [17]. In addition to these favorable qualities, ABS plastic is also recyclable [17]. Despite these great properties, the manufacturing of plastic consists of melting and molding of hydrocarbons [18] which will release greenhouse gases.

The only thing that can be done about the manufacturing of our plastic cases is to trap the emitted greenhouse gases. There exist bacteria that actually can absorb greenhouse gases [19]. Utilizing these in manufacturing would reduce greenhouse gas submission substantially. In regards to disposal, it would be wise to mention the recyclability of the plastic casing in a user manual. If the user does not recycle the plastic, its strength and durability actually make it very resistant to decomposing [18].

The LCD and the PCB both contain hazardous materials that have an impact on the environment. The LCD has a PCB as well. PCB's contain recoverable quantities of precious metals and base metals [20] which mean they can be recycled and scrapped. This also means that improper disposal could be very poisonous to the environment. Over its lifecycle, the LCD itself also can contribute to ozone depletion and human health toxicity as well as a host of several other problems [21].

Little can be done to solve the manufacturing and disposal environmental impacts of the PCB and LCD. The impact from manufacturing can be helped by looking into more environmentally viable PCB's. Finding a way to reduce the amount of natural gas used in the manufacturing of LCD's is the best way to dramatically reduce its effect on global warming [21]. Disposal entirely depends on the customer. The most we can do is put a label on the device indicating proper disposal. If economically feasible, it would probably be wise to have the customer send the to-be-disposed device to us, so that we can recycle and scrap it properly.

Lastly, the RSU contains a 9V battery in the event there is a power outage it is able to operate for a few hours. Almost all disposable batteries contain a lead-acid solution [22] which is very harmful to the environment. The battery will not be rechargeable. A rechargeable battery would increase its longevity, but since it is ideally never going to be used, this is an unnecessary cost. The DHS actually monitors the life of the battery and will warn the user when the battery is running low. This means that the user will not have to replace the battery after a certain length of time, but instead only when necessary. When the time does come for the battery to be disposed, there will be a warning label near the battery reminding the user to recycle the battery and how to recycle it. The simplest way for the user to figure out where to recycle the battery is by calling 1-800-8-BATTERY [22]. The phone number will be referenced on the warning label, and all of these instructions will be referenced in the user manual.

6.3 Ethical Challenges

There are two main ethical challenges with our design: making sure the customer knows how they are being protected and to make sure that their personal information is secure. Making sure that the customer knows how they are being protected is definitely the highest priority. Customers will depend on this device for safety and security. If the customer actually believes that DHS will protect them from all threats, then not only are we possibly legally responsible for any security breaches but also morally responsible. In addition to its protection features, the DHS must also store personal information. While a phone number and an e-mail address would be the only personal information stored, having that stolen can be a great annoyance.

Making sure the customer knows how they are being protected actually means two things. The customer needs to be aware of what security threats the DHS protects him against and also what features are actually working. The former aspect can be solved by advertising on the packaging what the RSU's will be able to detect. A sticker can also be placed upon each device indicating what all they monitor. The second aspect is more complex. There is no real way to test that a circuit component is working properly other than to simulate a scenario such as smoke or noise; however, the CMS will have a function which will test the alarm system to make sure that if a situation is detected, the owner will know about it. Store-bought smoke detectors are tested by checking the alarm; it would be unreasonable to expect the customer to actually perform a smoke test on a smoke detector. When someone buys a product, they intend for it to work. A simple way around this is to place a sticker on the device or have it clearly marked on the package that the RSU's will need to be replaced after a certain amount of time. Smoke detectors have to be replaced every ten years. Unfortunately, according to our reliability report [23], our device could theoretically fail after twenty-seven minutes. This is unacceptable. The report has some suggestions, but time will be needed in order to research ways of reducing the failure rate.

Closely related to making sure the customer knows how they are being protected is making sure they know how to make our system most effective. It would seem obvious to many people that remote sensor units should be located near doors, windows, and potential fire hazards. This may not be obvious to some. Having an entry in the user manual that describes the best strategic locations for the devices would alleviate responsibility from us in the event that someone's home is compromised and our system fails to notify the customer because they put the RSU's in an ineffective location.

The second ethical challenge is about ensuring the confidentiality of information contained within the CMS. There won't be any information that would directly lead to identity theft, but if a hacker were to get a hold of the customer's phone number and e-mail address, then the customer could be spammed or –even worse – subjected to a malicious attack. Another issue is that many people use the same password for everything. While there is definitely nothing we can do about this other than a simple warning, it is imperative that we maintain its secrecy. Another important reason to keep the password a secret is because an intended function with the website is for it to be able not only monitor security parameters but to also set them.

Fortunately, MySQL will encrypt passwords [24] although it is recommended that a hashing function be used to protect passwords from especially clever hackers. All other information is sent as plaintext which can be read by packet sniffers. Recommended ways of handling this are by connecting to the database via SSH or some other secure connection which will encrypt transmissions. Another protection against hackers is to make sure that the web server never runs as root. MySQL will actually throw an error if the web server is ran as root unless a specific option is set. In addition, the user should never have "super" privileges since they should only use the website and peripherals provided. All of these methods of protection will be implemented by the manufacturer, so the user will be oblivious to this. It would be wise to mention some of these precautions within a product or user manual in case the customer wants to know.

6.4 Summary

The Digijock Home Security system is a wireless network of remote sensor units that communicate with a central monitoring station to provide security and peace of mind to the user. Ensuring this peace of mind is a necessary ethical challenge that DHS handles by making sure the user knows how they are being protected. This is accomplished by proper labels on both the packaging and the devices themselves. In addition the DHS must protect the personal information of the customer. Fortunately, this is handled by the software using various hashing and encrypting functions which will protect the customer's information from even the most seasoned hacker. Another ethical concern is the environmental impact of the device. The PCB, the LCD, the plastic case, and the battery impact the environment more than the other components in the DHS. Utilizing proper warning labels and using cutting edge technology, most of impact can be reduced. The DHS will have to depend on the user for ultimate execution of these concerns, but the effort put behind the DHS alleviates a lot of burden off the user. All of these considerations should make the DHS an environmentally sound device that not only will protect the customer but also the planet.

7.0 Packaging Design Considerations

7.1 Introduction

Digijock Home Security (DHS) is a security and monitoring system that is designed for use in residential applications. It features a sensing system that is capable of detecting motion, smoke, noise, and measuring temperature. The information is relayed back to a Central Monitoring Station (CMS) that stores the data and provides a web interface to access the data logs. The alarm is capable of being managed by a control unit that is connected to the CMS via USB. The divided nature of the various components of the overall system means that packaging analysis requires additional consideration.

Special care must be taken to ensure that the packaging design does not interfere with the operation of the different sensors. The motion sensor will require a direct line of sight to the outside environment without being blocked by the enclosure. Both the smoke and temperature sensors must have uninhibited exposure to air from the room. Additionally, the reading from the temperature sensor should not be impacted by the surrounding circuitry. The noise sensor should be able to detect sound without it being affected by damping. All of these requirements must be met in order for the final product to function satisfactorily and according to specification.

Finally, DHS is targeted towards cost-conscious consumers who wish to have a full-featured security and monitoring system at a minimal price.

7.2 Commercial Product Packaging

7.2.1 Product #1

Figure 7.2.1: DSC Wireless Ready Alarm System Kit

The DSC Wireless Ready Alarm System Kit is a mass-market product similar to our design. This model includes a LCD control panel with built-in wireless receiver and keypad, a wired motion sensor, a four amp-hour backup battery, a 15 watt siren, a telephone jack, and a 16-zone wired alarm control panel. Noteworthy features include combined wired/wireless networking, a 500-event buffer, control unit battery backup, standalone siren, wall-powered sensors, and landline telephone connectivity [25]. Positive aspects of these design and packaging choices include flexibility in placing sensors by choosing wired or wireless connections, long-duration backup battery, and no need to replace or recharge numerous batteries. Drawbacks to this design include bulky and heavy design due to dual wired/wireless connectivity, more complex system configuration caused by dual wired/wireless, more difficult installation of wired sensors, cumbersome interface with no remote management capability, basic two-line LCD screen, requirement to have landline phone service and additional monitoring subscription, sensors require wall power and do not have battery backup, and the user must purchase many separate and expensive sensors.

Packaging and design features that we wish to incorporate into our project include event logging capability, a straight-forward keypad interface, and battery-free sensors that do not require replacement or recharging. Unique features that our product will offer are simplified lightweight plastic packaging without bulky batteries, integrated wireless sensors for simplified installation, easy local system configuration with a more advanced LCD display, web-based event log viewing and system management, and no need to have landline phone service or an alarm monitoring subscription.

7.2.2 Product #2

Figure 7.2.2: 2GIG Go! Control Panel Wireless Alarm Kit with AT&T GSM

The 2GIG Go! Control Panel Wireless Alarm Kit with AT&T GSM is a second product similar to the security system we are designing. It features a wall-mounted control unit along with wireless motion sensors, door/window sensors, and a keychain controller [26]. Noteworthy features are battery-powered wireless peripherals, a touch screen interface, and GSM cellular connectivity allowing the alarm to be managed with a smart phone. The positive aspects of these features include the advanced user interface afforded by a touch screen, the ability to control the system even while away from home, and its dependability during power failures.

The specific combination of features that the manufacturer chose to include results in a system that is very compact and lightweight. Packaging is simple, elegant, and aesthetically pleasing. Also, installation is simplified due to the absence of wired connections to the central unit. On the other hand, drawbacks include a lack of event logging, susceptibility to dead batteries, expensive add-on peripherals, requirement to be located in an area with reliable cellular signal, and the necessity to pay for a monthly AT&T cellular plan for the GSM connectivity.

Features we wish to incorporate include a simplified and lightweight design with attractive coloring if possible, easy installation, remote system management, wireless peripheral connectivity, and an advanced user interface. Unique features that our product will offer are lower price, no recurring costs, event logging, and no susceptibility to dead batteries.

2.0 Project Packaging Specifications

Because of the nature of our security system, the packaging is separated into two distinct units based on function. These units include the control unit and the wireless peripheral units. There are several features that are common to both types of units. First, they are designed to be hung on a wall. For this reason, the packaging should be lightweight, maintain a low profile, and must incorporate mounting hardware. Second, both require components to be able to protrude through and be mounted to the front of the enclosure, so the material chosen must be conducive to this design. Third, for aesthetic reasons, a light-colored package is preferable to a dark-colored one. This will help the units be less conspicuous when installed.

Specifically for the control unit, there are several additional design aspects that must be considered. The three components included in the control unit are a keypad, speakers, and an LCD screen. All together, these parts take up a decent amount of surface area. Also, the speakers themselves are fairly bulky in order to make a loud sound, so the enclosure must be of a large enough volume to contain all the parts.

The peripheral units will hold the printed circuit boards, which include a microcontroller, temperature, smoke, motion, and noise detectors, an LCD screen, an LED, and a wireless module. As mentioned in the introduction, the sensors must have uninhibited exposure to the surrounding environment in order to provide accurate readings. Therefore, ventilation openings should be incorporated into the enclosure. It is important that the enclosure be able to easily accommodate a PCB to simplify assembly.

The ideal packaging solution would satisfy all of these above criteria while being as small and visually appealing as possible. The two enclosures that are best suited are Hammond Manufacturing 1591EFLBK cases for the sensor units and a Polycase DC-96F for the control unit. Both are plastic which is lightweight and easy to drill for wires and ventilation holes. They both feature PCB mounts inside for convenient mounting of the PCB. They are as slim as possible while still fitting all the components. The 1591EFLBK measures 190 x 110 x 60.6 mm [27], while the DC-96F measures 254 x 152.4 x 76.2 mm [28]. Both are large enough to accommodate the necessary parts. Additional product specifications can be found in Appendix B, and three dimensional CAD models are located in Appendix A.

The Atom board itself will not be placed inside an enclosure since it is already housed in a mini-ITX case. All components will run on wall electricity to avoid the weight and bulk of batteries. Also, battery life would not be satisfactory due to the constant power requirement of maintaining a wireless network. It would be very impractical to have an alarm system that required all the distributed sensors to be recharged or fitted with new batteries on a regular basis. Finally, avoiding batteries helps reduce the overall cost of the system.

3.0 PCB Footprint Layout

The three components previously identified as major elements of the project include the microcontroller, the computing platform, and the wireless module. Their importance to the success of the project merits special consideration in their final layout on the printed circuit board.

It should be noted that the final selection for the computing platform, an Intel Atom board (D945GSEJT), is a standalone unit that will not be attached to a PCB. Therefore, it will not be included in the layout. The wireless module, an Xbee 1mW Chip Antenna, is only available as a 20-pin DIP, so that is what we will use. The microcontroller that was chosen, the MC9S12C32, is available as a 48-pin LQFP [29]. It is also available on a 32-pin DIP module (NC12C32SP-SB) that incorporates an on-board RS232 transceiver, a voltage regulator, and a crystal with associated PLL support circuitry [30]. Although the DIP module is significantly larger, it includes additional circuitry that our design requires, and we have several models immediately at our disposal. Therefore, we have chosen the DIP module.

Because we are making two peripheral units, our PCB area will have to be split in half, and the design will be duplicated on both halves of the PCB. The two DIP modules will occupy a significant amount of space. The Xbee will occupy 673 mm^2 [31], and the microcontroller module will occupy 823 mm^2 [30]. The motion sensor, LED, and LCD will be attached via headers since they have to be incorporated into the packaging face. The smoke detector circuit, microphone, and speaker circuits all require several passive components, which will occupy approximately 1000 mm^2 per sensor. The temperature sensor is small and only requires 100 mm^2. Additional circuitry will be required for voltage regulation and level translators, which will occupy an estimated 2000 mm^2. The total area thus far is approximately 6600 mm^2. Taking into considering space for extra components and routing traces, an estimate of 10,000 mm^2 is likely closer to the true area requirement. Since our circuit layout has to be duplicated, the area requirement is double to 20,000 mm^2. Considering our area allowance is approximately 38,700 mm^2, we will be within the limit.

4.0 Summary

Packaging is an important element in the design and ultimate success of our project. The product must be small, lightweight, easy to install, and simple to use, all without making sacrifices in the overall performance and utility of the system. Comparisons to off-the-shelf products helped determine what features are desirable to incorporate in a security system and which ones should be avoided. Packaging choices were dictated by the features that were included in the product and the desire to minimize cost. The ultimate packaging solution is an ideal fit to the desired outcome and the predetermined success criteria for the project.

8.0 Schematic Design Considerations

8.1 Introduction

Digijock Home Security (DHS) is a home security system that implements the standard lines of protection from fire and burglary. With this system in place, it will monitor several aspects of common fire and burglary scenarios and relay the information to the Central Monitoring Station (CMS), which runs a web server. This functionality will allow the user to login to the web server and view information and statistics. The user may also choose to communicate directly with the CMS with a keypad and LCD interface. This will allow the user to set the security system into multiple modes of operation. The remote sensor units will be controlled by a microcontroller, which will send updates via Xbee wireless to the CMS. The CMS stores the information in a database, which will be accessed by a .NET web application.

8.2 Theory of Operation

The CMS allows users to interact with the security system. The CMS will consist of five components: an Intel Atom board, a keypad, an LCD screen, a speaker, and an Xbee wireless module. A standard AC adapter will power the CMS. It will be a stationary device that will be on at all times running the web server and communicating with the remote sensors. The heart of the CMS is the D945GSEJT Atom board running Windows XP. It controls the web server and the user interface on the LCD screen. The user will interact via a USB keypad and LCD to change the modes of operation: 1) Change password, 2) Activate in-home mode (disable the motion and noise detection), 3) Activate out-of-home mode (all the sensors are on), 4) Get status condition from a selected unit (temperature of the room), 5) Stop an active alarm or test the alarm. Each USB component will be directly powered by its USB connection.

The Atom board will host the web server, which will be used for remote access from any computer connected to the Internet. This will give our user the flexibility to check in on his/her house when away on vacation or at work. The framework of our web server will run Apache Web Server 2.2, a well-known open source HTTP Server project that has a lot of documentation and forums for ease of use. Our .NET Web Application is not going to encounter heavy usage; it will not need to handle several thousand hits per second. Our design will be able to manage minimal data traffic and is setup to handle only a few sessions at a time. To hold and keep track of the information coming in from the remote sensors, we will setup a database using SQL Server 2005. The web application will be populated from information that is present in the database. A table in the database will be set up to handle both remote sensors and track temperature change, smoke detection, motion detection, and noise. Another key feature of the web application is that the user will have the ability to activate or deactivate the alarm via the Internet. Also, once the alarm is tripped and the CMS is notified it will send an email to each member of the family. This is a key feature for users who are on the go and want peace of mind that there are no problems at home.

The remote sensor units are stand-alone components separate from the CMS that communicate wirelessly with each other. The remote sensors will be powered by an incoming 9-volt power source connected directly to a standard wall outlet, which will be regulated. Using rechargeable batteries is a possibility, but we decided against it for our project. These units are going to be stationary in a room—they are not meant for portability. Also, since the units will be constantly communicating with the CMS using a wireless connection, the power required would quickly discharge the battery. For this reason, a standard wall outlet will power the remote sensor units.

Each remote sensor will contain a Freescale 9S12C32 microcontroller that will operate at 24MHz. This microcontroller operates at 5-volts regulated and will need a DC to DC step down voltage regulator circuit [32]. The remote sensor units will track different conditions within a house: smoke detection, motion detection, temperature, and noise detection. Also provided on each unit is an LCD screen and speaker that allows for a limited user interface.

In order for the remote sensor unit to detect the presence of smoke, it will feature an RE46C140 CMOS photoelectric dedicated IC that operates on a 9-volt regulated power source [33]. It will detect the presence of smoke by having a smoke chamber. The smoke chamber has an infrared emitter shine into the chamber with a photo diode sensor not directly in the path. When smoke enters the smoke chamber, the infrared light will bounce off smoke particles into the photo diode sensor. If the amount of light detected by the photo diode is enough to set off a smoke condition, it will relay that information to the 9S12 microcontroller. This IC allows for a speaker to be hooked up directly to it, but for our project the microcontroller is going to control the speaker. Therefore this functionality will not be utilized.

In order for the remote sensor unit to detect motion, it will feature an AMN34112 MP Motion Sensor Module. This module provides 10 meters of detection area, which is equivalent to a standard room size. It will require a 5-volt regulated voltage along with a transistor switching circuit [34].

In order for the remote sensor unit to detect noise, it will feature a CMA-6542PF electret microphone. It will require an audio preamplifier circuit, with a high gain of about 50. The reason an audio preamplifier circuit is require is that the microphone output needs to be amplified for the microcontroller's ATD converter. At this time we are considering adding a high pass filter to filter out any noise below the 4kHz frequency. We believe this will take away many factors that might cause a false alarm.

In order for the remote sensor unit to detect the temperature in the room, it will feature a LM35 Precision temperature sensor that will use a Fahrenheit circuit provided by the manufacturer. It will be powered by a 9-volt regulated voltage source. It will utilize an analog to digital converter. Every 1.0mV step corresponds to a change of 1 degree Fahrenheit [35].

The remote sensor unit will also feature a limited user interface. It will be equipped with an LCD screen, two LEDs, and a speaker. The LCD screen will display several messages depending on which state the security system is in. For normal activity, the LCD screen will display the current temperature in the room. When an alarm is tripped, the LCD screen will display the root cause in case the user is not near the CMS. Also, two LEDs (red and green) supply the user with visual information. The green LED will be lit when no alarm has been tripped, and the red LED will turn on when it goes into an alarm state. Once the alarm is tripped, a speaker will sound to notify the home occupants and to scare off any potential burglars. The speaker is controlled by the PWM subsystem of the microcontroller. It will fluctuate in frequency to imitate a siren. We are still working with the circuit configuration. We are trying to improve the gain using an amplifier circuit, but so far we have not had success. Given more time for research and prototyping, we will design a functional circuit.

The remote sensor units will feature wireless communication with the CMS using Xbee wireless modules. These modules run on 2.4GHz operating frequency, and run off 3.3-volt regulated voltage source [36]. It will utilize the SCI subsystem of the 9S12 microcontroller. It will digitally transmit and receive information to and from the CMS.

8.3 Hardware Design Narrative

8.3.1 SCI Subsystem

The SCI subsystem on the 9S12 microcontroller will be utilized for the Xbee wireless communication. Port pin 1 on the micro is specifically used for Tx, which is the data out pin that will be connected to the Xbee module. Port pin 2 is specifically used for Rx, which is the data in pin, and that too will be connected to the Xbee module. The SCI subsystem will run at the normal 9600-baud rate and it will be run in a program-driven operation.

8.3.2 SPI Subsystem

The SPI subsystem on the 9S12 microcontroller will be utilized for the LCD screen. We are only interested in sending data out and not receiving data. We will only utilize MOSI and SCK hand shaking. Port pin 14 (PM4) will be used for MOSI and port pin 15 (PM5) will be used as the clock to the shift register. The SPI will use a 6.25Mhz baud rate and it will transmit the most significant bit first.

8.3.3 PWM Subsystem

The PWM subsystem on the 9S12 microcontroller will be utilized for the speaker. We plan on adjusting the frequency to emulate a siren. We will use port pin 24 (PT5) for the PWM. The configurations have not yet been discussed as of now.

8.3.4 ATD Subsystem

The temperature sensor and the microphone circuit will utilize the ATD subsystem on the 9S12 microcontroller. The temperature sensor will utilize the port pin 6 (AN1) and the microphone will utilize port pin 5 (AN0). The ATD will be set to do two conversions and run at 8-bit resolution. For the temperature sensor, every 1mV sensed by the ATD accounts for one degree Fahrenheit. In software we will measure the level of sensitivity of the microphone and depending on testing we will set a cap on how much noise we will tolerate before the alarm is tripped.

Pin #	Pin Name	Input/Output	Use in Design	Special Notes
1	Tx	Output	Data Out (Xbee Wireless)	

2	Rx	Input	Data In (Xbee Wireless)	
4	VSS	Input	Ground	
5	AN0	Input	Microphone (ATD)	
6	AN1	Input	Temperature (ATD)	
11	AN6	Input	CTS (Xbee Wireless)	
12	AN7	Output	RTS (Xbee Wireless)	
13	PM5	Output	SCK (LCD)	
14	PM4	Output	MOSI (LCD)	
19	PT0	Input	Smoke Detector (I/O pin)	
20	PT1	Input	Motion Sensor (I/O pin)	
21	PT2	Output	RS (LCD)	
22	PT3	Output	LCDCLK (LCD)	
23	PT4	Output	RW (LCD)	
24	PT5	Output	Speaker (PWM)	
25	PT6	Output	Alarm Status (LED)	
26	PT7	Output	Ok Status (LED)	

Table 8.3.1 – Port Pin Assignments

8.4 Summary

This report summarizes all the operating components and subsystems of different peripheral circuits in the home security system. Described in section 8.2.0 is the Theory of Operation of how our CMS functions and interacts with the remote sensor units. Also described is how our remote sensor units operate along with operating frequencies and voltages. Section 8.3.0 deals with the subsystem of the microcontroller and how they are used in our circuit. All the port pins have been assigned depending on which subsystem they use on the microcontroller.

9.0 PCB Layout Design Considerations

9.1 Introduction

Digijock Home Security is a home security system based on a Central Monitoring Station (CMS) and two remote sensor units (RSU). The two sensor units perform the same operations, so they will be built in the same way. The RSUs incorporate a microcontroller, so our analysis will focus on the design of the accompanying PCB. Each unit will have a smoke detector, a motion detector, a temperature sensor, a noise detector, an LCD, and a wireless module (for communication with the CMS). Some of the peripherals will require voltage level translators and amplifier circuitry in order to interface with the microcontroller.

All these elements will be taken into consideration in the following analysis in terms of placement of analog and digital components, increasing capacity to withstand noise, and minimizing the size of the layout. Special attention will also be paid to EMI problems, which we will try to solve by decreasing potential emissions and increasing circuitry immunity.

9.2 PCB Layout Design Considerations – Overall

There are several aspects that have to be taken into consideration in our PCB layout. First of all we need to consider the type of signals used by each component, how to place the components in order not to create interference, and the area requirement that we are trying to meet with the circuit. The PCB will be divided in three major areas: analog, digital, and high-power. Since analog signals are generally more vulnerable to interference and the power circuitry is a consistent source of EMI, there will be a clear division between the two areas [37]. The microcontroller will occupy a central position. This location will give us two advantages: keeping the path between microcontroller ports and peripherals as short as possible and dividing the major areas identified above (Figure 2).

The analog area will be located in the lower left corner, and the microphone will probably be the component most sensitive to noise interference. For this reason it will be located as far as possible from the power circuitry, which will be in the upper right side of the PCB. Moreover we have identified the speaker circuitry as a source of EMI, so it will be located on the other side of the PCB as well (lower right side). In addition, special attention will be given to the Xbee module. Since it is an intentional RF transmitter, it must be positioned in such a way as to minimize interference [38]. For this reason it will be locate in the upper left side.

Conductors carrying changing current are the primary source of coupling noise. As a result, trace width, location of vias, and trace angles are important considerations in the layout. The traces that are identified as the most critical ones will be addressed first (power and ground). Acute angles need to be avoided because they can cause acid traps. Also, 90^{o} angles could cause problems in terms of EMI noise. Moreover adequate space needs to be left for mounting holes.

Most of the sensors will be connected to the PCB via headers, so the header pins will be located at the bottom of the PCB for convenient access and to reduce the clutter caused by overhead wires.

In terms of traces, it's important to remember that length and width affect their impedance. Nonetheless, we have not identified any source of high current since all the components use current between 70 μA and 80 mA. For this reason the traces will be around 10-12 mils.

Finally another EMI concern that we need to take into consideration is the ground for analog and digital signals. The ground paths for digital and analog signals will be separate and will only be connected together at a singled point on the PCB.

9.3 PCB Layout Design Considerations – Microcontroller

The microcontroller is going to be placed in the lower middle part of the PCB. For our project we are going to use the 9S12C module placed directly on the PCB. Since we already have several modules available, this will save us money. Furthermore, it will save us space on the bottom layer of our PCB since the components we would have had to place on the bottom of the PCB are instead located on the bottom of the module. The crystal for the microcontroller is an RF emitter is extremely vulnerable to noise. Therefore its traces are filtered with an RC filter [39]. Also, decoupling capacitors are places in close proximity to the microcontroller.

Some important considerations need to be taken into account regarding the pin usage in the microcontroller. Since we are not going to use all the pins available for each protocol, it would be a good idea to spread the pin usage in order to avoid a crowded layout (Figure 1). Moreover the placement of the different areas (analog and digital) in the PCB is designed to reduce the path between the microcontroller pins and the related peripherals.

Some signals are more critical than others, so they need to be addressed first in our PCB design. On the left side (analog area) we will have: the smoke detector, the thermometer, the microphone, and the LCD (it actually uses the SPI pins located at the very bottom of the 9S12C module, making the path between these pins and the headers on the edge of the PCB very short). The microphone is the most sensitive device so it will be placed as far as possible from the Xbee module which uses TX and RX for the SCI protocol and AN1 and AN2 for the control signals. In fact as a radio frequency transmission device, the Xbee module can be a source of EMI, so it has to be isolated (in the upper left corner) from the rest of the circuit.

Another important note on the ATD connections is related to the reference voltage pins. They are going to be directly routed to ground and power, and an RC circuit consisting of a 1kΩ resistor and a 1uF capacitor will be connected to filter noise.

On the right side (digital area) we will have: the speaker, the motion sensor, and the LEDs. The speaker will likely be a critical device. As a possible source of EMI, it will be connected to PT0, the pin farthest from the power circuitry. This design choice will help to avoid mutual interference.

9.4 PCB Layout Design Considerations - Power Supply

The power circuitry represents the most important design in terms of noise reduction. The devices that we are going to use in our design work with different supply voltages, ranging from 3.3V to 9V. For this reason our power supply area will have two voltage regulators: one from 9V to 5V (used for example by the motion sensor) and one from 5V to 3.3V (used by the Xbee module) [40].

The power design will also include circuitry for a backup battery system, the latest addition to our project. A 9V battery will be used in case of power failure. According to our calculations of the average current (220mA in alarm mode, 100mA in idle mode) used by the peripheral units, a 9V battery will last between 4 and 8 hours, giving the user plenty of time address the cause of the problem after receiving an alert email regarding the loss of power.

Two bulks capacitors will be placed as close as possible to the voltage regulators. The purpose of these capacitors is to recharge the IC decoupling capacitors upon depletion caused by current glitches and spikes (most often caused by logic transitions in digital circuitry). Along with the bulk capacitors, there will be a 0.1uF capacitor, used to decouple high frequency noise at the power input [37]. The value of 0.1uF was chosen since our system clock speed is below 15 MHz.

The battery circuitry will have two signals connected to the microcontroller. The digital one will inform about wall power failure, while the analog one will tell the level of the battery. Although they originate from the same area of the PCB, the two signals need to be placed as far as possible from each other to avoid mutual interference. Moreover the analog signal will be connected to AN0 (the highest of the analog pins on the left side) to give as much space as possible between this signal and the other analog signals. For the same reason the digital signal for power failure will be connected to PT7, the pin farthest from the speaker. Both the analog and the digital signals from the power circuitry do not carry significant current, so the trace width will be around 10-12mils. The power supply and ground traces will be much wider, with an estimated width of 40-60mils.

Also, the ground system is a very important feature in the PCB layout. The goal is to minimize the voltage drop caused by current flowing through impedance in the ground traces. Although a ground plane would be the ideal solution for minimizing EMI, the cost of adding an additional layer for ground would not be economical for our project. Our best option is a single-point grounding layout with as many parallel paths to ground as possible. Also, ground and power traces will run parallel to each other wherever possible.

9.5 Summary

This report justifies the design choices that we made for our PCB layout. Elements we have taken into account for our design were explained, including logistic area placement, pin usage, and trace width evaluation. The critical points that we addressed were preserving the integrity of our signals from interference, reducing potential sources of EMI, and designing the most effective power circuitry for our PCB.

10.0 Software Design Considerations

10.1 Introduction

The Digijock Home Security (DHS) system consists of remote detector units wirelessly relaying updates to a web server on the Central Monitoring Station (CMS) which was built entirely on an Atom board with peripherals connected via USB. A program written in C# will read the updates from the Xbee wireless module and format it into the MySQL database. The web server will allow users to login to a .NET web application (written in C#) and remotely monitor the status of whichever room(s) the detector units are located. In addition, the web server will also send alerts to the user through a text message and an email. The CMS also has a local interface consisting of an LCD and a keypad to allow security level customization and other controls. Together these components will provide a security system that will alert the user to most threats.

The remote detector units utilize the Freescale 9S12C32 microcontroller module used from ECE362. This provides us with familiarity which makes programming much easier. The application code is an interrupt-driven, polling loop. The ATD module will support the noise detection, smoke detection, and temperature measuring. The SPI module will handle the LCD. For our wireless system, an Xbee wireless module will communicate with the SCI module of the microcontroller. The speaker (audio alarm), the LED (indicating armed/disarmed mode), and the motion detection will be simple inputs and outputs. These modules will allow the DHS to monitor several aspects of common fire and intruder scenarios through its remote detector units.

10.2 Software Design Considerations

10.2.1.1 Digital I/O Module

The digital input/output module is actually the peripheral interface module (PIM). The reason why it is referred to as such is that PIM controls all ports and digital I/O is the default [41].

Since the LED's and the inputs from the motion detector, the power failure detector, and the alarm are simple digital logic, the digital I/O module is more than sufficient to handle these devices. The register DDRT [41] controls whether the ports PT0-7 are input or output. Setting the bits high indicates that the ports are outputs; low means they are inputs. The register PTT [41] actually contains the information from the inputs where each bit corresponds to the respective port.

10.2.1.2 Analog-to-Digital Module

Several devices actually output analog signals to indicate more information through one port. Because of this reality the analog-to-digital converter is needed in order to handle it. The noise and smoke detector both output analog signals indication how much noise [42] and smoke [43] they are receiving respectively. The temperature device and the battery level measuring also output analog signals [44]. It should be noted that the battery doesn't output any intelligent information; we are able to ascertain the charge level by simply connecting to the battery and measuring its output. The register ATDDIEN [41] controls whether the ATD ports are inputs or not. Setting the bits high indicates they are inputs. ATDCTL2 [41] turns on the ATD so that it will actually work. The other two control registers ATDCTL3, 4 [41] handle the sample time and the conversion sequence length. These were the familiar settings from ECE362, so that we knew how to get the calculations.

10.2.1.3 Serial Communications Interface Module

Since the data packets we want to send and receive consist of multiple bytes and then need to be handled as fast as possible, we wanted the serial communications interface to handle the communication with the Xbee wireless module. Ports Tx and Rx are used to send and receive from the Xbee respectively. The Xbee module communicates at a baud rate of 9600 therefore the registers SCIBDH and SCIBDL [41] have been initialized with the appropriate values to set the baud rate of the SCI to match it. The register SCISR1 [41] controls whether it is transmitting or receiving. SCISR2 [41] initializes the SCI for program-driven operation. Setting the second bit high in DDRB [41] sets PB4 for output mode, and doing the same for PORTB [41] asserts the DRT on the COM port. These configurations are necessary to allow ease and simple communication with the Xbee module.

10.2.1.4 Serial Peripheral Interface Module

Since the SCI was being used by the Xbee wireless module, the serial peripheral interface (SPI) was chosen to output data onto the LCD. The LCD operated at 6.25MHz, so the baud rate for the SPI had to be set to match it which was done with SPIBR [41]. DDRM [41] had to have the two least significant bits set high so that PM0 and PM1 could be used as outputs. PM1 controls the read/write operations while PM0 determines whether the output is an instruction or a character. Registers SPICR1 and SPICR2 [41] were configured so that the most significant bit was sent first and that it operated in the normal mode. This was done for familiarity from ECE362.

10.2.1.5 Real Time Interrupt

The real time interrupt (RTI) is used to decide when the update packet to the CMS should be sent. It subsequently decides when the flags are set low. The register CRGINT [41] is used to enable the interrupt. This is accomplished by setting bit four high. RTICTL [41] controls the interrupt rate. The rate will determine how fast the updates are sent.

10.2.2 Application Code Organization

Our code for the remote detector units is written in Embedded C using the Freescale CodeWarrior IDE. A fairly simple feature - user-defined security levels - has actually had the most impact on why the overall structure of the software is an interrupt-driven polling loop. As seen in Appendix A, the detector units never actually activate their local alarms. The CMS controls whether the alarm goes off or not which is why the various detection apparatuses merely set flags through a polling loop. This was done since the CMS has the responsibility of what events are considered threats by the user. In order to control congestion and prevent packet loss, a timed interrupt triggers the actual sending of the packets which takes place every yet-to-be-determined time interval. These factors contribute to why an interrupt-driven polling loop works best given our desired functionality.

10.2.3 Debugging Provisions

The only debugging capability available to the customer is the CMS can test the alarm system. Beyond that the only other debugging method available is to actually simulate threat scenarios. However we (the DHS Company) can attach a computer monitor to the CMS which will allow us total insight into the CMS in case we need to check anything ranging from processes running to checking the packets from the detector units.

10.2.4 Memory Map

Address	**Purpose**	**Address**	**Purpose**
Start – 0x0000	Registers	Start – 0x8000	Flash Memory
End – 0x03FF		End – 0xF7FF	
Start – 0x3800	Variables, stack	Start – 0xFF00	Interrupt Vectors
End – 0x3FFF		End – 0xFFFF	

10.3 Software Design Narrative

10.3.1.1 Main

The main() function serves as the controller for the detection unit. This is the first program to be booted, so it handles the initializations of the registers. Afterwards it goes into an infinite loop where it begins to poll all of the peripherals. Starting with the SCI, it checks the

SCIDRL to see whether it should activate the alarm system or not. Then it checks for a low battery, power failure, temperature, noise detection, smoke detection, and motion detection which all will set flags to ‘1’ if any are triggered. The battery and temperature measured will regardless be printed onto the LCD. After the polling is complete, it returns to the top of the loop.

Status: All code has been written and tested.

Hot Link: Main module code

10.3.1.2 Analog-to-Digital Converter

The analog-to-digital converter (ATD) retrieves the analog inputs from the battery (for charge), noise, smoke, and temperature components. The battery charge, smoke, and temperature components don’t possess any special algorithm other than just a conversion from the ATD. They simply read what their device sends and set a flag or store a value into a register. On the other hand, the noise detection has a special algorithm. Since we were encountering problems with the variations in noise, we decided to have a running average. The average consists of three numbers where one the third number is new while the other two are the past two sampled values. Once an average value has been obtained, we check to see if it is greater than 35 which we found to be the ATD converted value for noise at 90 dB.

Status: All code has been written and tested.

Hot Link: ATD module code

10.3.1.3 Serial Communications Interface

The Serial Communications Interface (SCI) is responsible for sending and receiving data via the wireless Xbee modules. There are two functions OutSCI() and InSCI(). OutSCI() is responsible for transmitting data whereas InSCI() will read incoming data. With these two functions, the detector will be able to read packets from the CMS to see whether alarms need to be set and send status updates to the CMS indicating possible threats and the temperature.

Status: All code has been written and tested.

Hot Link: SCI module code

10.3.1.5 Serial Peripheral Interface

The serial peripheral interface (SPI) communicates with the LCD in order to display system statuses locally. The LCD will display the area around the detector unit's temperature as well as the status of the battery. This is done through the two functions: print_batterylevel() and print_temp(), but these simply format the data. Both of these functions rely on send_char() and send_instr() to actually send data to the LCD which in turn depend on OutSPI(). We never read from the LCD, so an InSPI() is not necessary. OutSPI() does the direct interfacing with the LCD while send_char() and send_instr() change the appropriate register values to indicate whether they are sending a new character or an instruction to the LCD. In addition to data local to the detector unit, the alerts sent from the CMS will also indicate what kind of emergency or emergencies are caught by the system, and these will be displayed on the LCD too in case the user happens to be in the area of a detector and no other means of communicating. If there are no emergencies it will display nothing more than the temperature and the battery status.

Status: All code has been written and tested.

Hot Link: SPI module code

10.3.1.6 Digital I/O

The digital input/output ports control outputs to the LED's and accept inputs from the power failure indicator and the motion detector. Technically this is controlled by the port integration module (PIM), but since PIM controls all of the ports and all of the ports are general purpose I/O by default, this is a moot point. There is nothing truly unique, but the functions are designed to create more readability for the code. Obviously the functions redLED_on(), redLED_off(), greenLED_on(), and greenLED_off() control the output of the LED's which is simply the manipulation of a bit in the PTT register. The functions speaker_on(), spearker_off(), power_failure() and motion_sensor() are also very straightforward. Since they produce digital outputs, if the input sees an event, the power failure and motion sensor flags respectively will be set.

Status: All code has been written and tested.

Hot Link: Digital I/O module code

10.3.1.7 Real Time Interrupt

The real time interrupt (RTI) serves primarily as the trigger to begin transmission of the detector's current status to the CMS. The interrupt is used to prevent congestion and lost packets in the system. There is no TCP protocol since there aren't many packets being sent in the system, but packet loss can still occur and that would be devastating to the system. To avoid this and still keep the system simple, the updates are sent every yet-to-be-determined time interval instead of near instantaneity.

Status: All code has been written and tested.

Hot Link: RTI module code

10.3.2.1 LCD Handler

The program is written in C# and essentially converts a JPEG file into a byte stream which can be displayed on the LCD screen. It grabs these images from the database every half second.

Status: All code has been written and tested.

Hot Link: LCD Handler code

10.3.2.2 Web Application

The .NET web application written in C# contains the code for the website and how it interacts with the MySQL database. The website is how the user will be able to actively remote monitor the status of the room(s) the detector units are located and control the CMS, and the database is responsible for storing the information. The website has three noteworthy pages. The first page is the login screen which is how the user will login and access his unique DHS. The registration page is where the user can enter the information corresponding to his unique DHS and online preferences such as username, password, and email address. Uniqueness will be determined by the associated serial number with every DHS (only one valid serial number since this is the prototype). The database will store the information.

Status: All code has been written and tested.

Hot Link: Web Application code

10.3.2.3 Xbee Communication

Written in C#, this program is responsible for obtaining and sending data to the detectors via the Xbee wireless module connected via USB. It will determine what raised flags are considered security threats and will send an alarm signal to the detectors if there is a valid security threat. The current temperature as well as valid security threats will be logged into the MySQL database. The temperature values will be replaced, but valid security threats will be time logged.

Status: All code has been written and tested.

Hot Link: Xbee COM code

10.3.2.2 Keypad Handler

The Keypad handler is able to read input from the CMS keypad and based upon that command inputs a new image into the database for the LCD Handler to display. This program is written in C#.

Status: All code has been written and tested.

Hot Link: Keypad Handler code

10.4 Summary

The Digijock Home Security system is a network of detection units that communicate with a Central Monitoring Station to provide security and peace of mind to the user. The detectors are built around the Freescale 9S12C32 microcontroller module whose peripherals (SPI, SCI, ATD, PIM, and PWM) and modules (RTI) allow the units to detect threats and respond with the appropriate response. The CMS being built within an Atom board gives it an incredible range of abilities that permit it to host a web server, run MySQL and .NET applications, and have USB connected peripherals. These enable the user to interact with the system locally and anywhere in the world.

11.0 Version 2 Changes

Version 2 of the Digijock Home Security system would only change a few aspects from the original design. The most fundamental change would be the CMS. Version 2 of the CMS would actually make use of a microcontroller and transmit its information to a central server (instead of having its own unique server) which would be located at the DHS Company. That way there would only have to be one dedicated IP instead of presumably thousands (if it ever became that popular). The other bonus of using the microcontroller is that the entire CMS could fit inside the peripheral box instead of just the peripherals. For the RSU's, the main change would be making the PCB smaller. While the spread out version made it easier to prototype, the DHS would be much more marketable if the RSU's were considerably smaller.

If we had access to better resources, a few minor details and extra features would be included in version 2. We are now aware that there exist more sophisticated motion sensors which can differentiate between movements of intruders and pets. Version 2 would also include extra security features like sensors that detect the opening and closing of windows and doors. This would involve an extra peripheral that would create a magnetic connection to the RSU (called a contact point) and would indicate to the RSU when a door or window is opened. Aside from that the only other changes would be purely aesthetics. For example, a better website design with a more professional look would be done. Now that we know the functionality, more time could be spent on making everything look as neat and user-eye-pleasing as possible.

12.0 Summary and Conclusions

Throughout this semester we were able to successfully build our project in its entirety. We made three member units which are able to communicate wirelessly to one another, so that together they are able to serve as a home security system. The RSU's can detect all intended security threats, and the CMS is able to collect these security alerts and handle them in the intended manner. The CMS not only activates the local alarms but will also send an alert via email and text messaging. The website hosted by the CMS allows the user real-time monitoring and control of the system.

As the project was being made, a lot of knowledge was obtained. We learned how to design an actual printed circuit board. As far as security systems go, we learned the various constraints concerning security peripherals (like how to monitor noise above 90 dB and not below). When programming the microcontrollers, we learned about Embedded C and how to debug it. The biggest learning curve that we eventually mastered was writing programs in C# that interacted with an external peripheral and a MySQL database.

References

[1] Tech. CUI INC. Web. http://products.cui.com/getPDF.aspx?fileID=3085.

[2] *Precision Thermocouple Amplifiers with Cold Junction Compensation*. Tech. ANALOG DEVICES. Web. http://www.analog.com/static/imported-files/data_sheets/AD8494_8495_8496_8497.pdf.

[3] *Parallax Serial LCD*. Tech. PARALLAX. Web. http://www.parallax.com/Portals/0/Downloads/docs/prod/audiovis/27976-7-9-ParallaxSerialLCD-v2.1.pdf.

[4] *MP MOTION SENSOR*. Tech. PANASONIC. Web. http://pewa.panasonic.com/assets/pcsd/catalog/napion-catalog.pdf.

[5] *MC9S12C Family Device User Guide V01.10*. Tech. no. 9S12C128DGV1/D. MOTOROLA. Web. https://engineering.purdue.edu/ece362/Refs/9S12C_Refs/9S12C128DGV1.pdf.

[6] *PIC18(L)F2X/4XK22 Data Sheet*. Tech. MICROCHIP. Web. http://ww1.microchip.com/downloads/en/DeviceDoc/41412D.pdf.

[7] *Xbee™ ZNet 2.5/Xbee-PRO™ ZNet 2.5 OEM RF Modules*. Tech. Digi International. Web. http://ftp1.digi.com/support/documentation/90000866_C.pdf.

[8] Mitsuhiko Yukawa, "Home Security System", U.S. Patent Application 10,909,354, Feb 2, 2006. http://www.google.com/patents/about?id=YXaaAAAAEBAJ&dq=10909354

[9] Richard L. McMaster, "Photoelectric smoke detector with count based A/D and D/A converter", U.S. Patent 5,705,988, January 6, 1998. http://www.google.com/patents/about?id=lfgcAAAAEBAJ&dq=5705988

[10] Yen-hung and Cheng-huan, "Home security system integrating local wireless network and external communication networks", U.S. Patent Application 20,080,007,403, January 10, 2008. http://www.google.com/patents/about?id=_4mmAAAAEBAJ&dq=20080007403

[11] Toshiyuki Aritsuka, Shoji Suzuki, Hiroshi Hanyu, and Fumio Enmei, "Security System", U.S. Patent 7,755,480, July 13, 2010. http://www.freepatentsonline.com/ds.html

[12] U.S. Department of Defense. (1991, December 2). Military Handbook: Reliability Prediction of Electronic Equipment. MIL-HDBK-217F. [Online]. Available: https://engineering.purdue.edu/477grp7/nb/datasheets/Mil-Hdbk-217F.pdf

[13] Freescale Semiconductor, Inc. (2004, May 12). MC9S12C Family. [Online]. Available: https://engineering.purdue.edu/477grp7/nb/datasheets/mc9s12c32.pdf

[14] NXP Semiconductors. (2011, February 11). 74LVC8T245. [Online]. Available: https://engineering.purdue.edu/477grp7/nb/datasheets/74LVC8T245.pdf

[15] Novacek, George. Designing for Reliability, Maintainability, and Safety. Circuit Cellar, Issue 125. Dec. 2000. [Online]. Available: https://engineering.purdue.edu/ece477/Homework/CommonRefs/CC_reliability_and_safety_ref.pdf

[16] Fairchild Semiconductor. (2001, June 4). 2N3904 NPN General Purpose Amplifier. [Online]. Available: https://engineering.purdue.edu/477grp7/nb/datasheets/2N3904.pdf

[17] Express Waste Management Services Ltd. (2010) *ABS Bayblend (Acrylonile Butadiene Styrene)* [Online]. Available: http://www.ewms.ltd.uk/Acrylonitrile_Butadiene_Styrene.htm

[18] American Chemistry Council, Inc. (2010) *Life Cycle of a Plastic Product* [Online]. Available: http://www.americanchemistry.com/s_plastics/doc.asp?CID=1571&DID=5972

[19] A. Morris. (2010) *Good Bacteria Eat Bad Greenhouse Gas* [Online]. Available: http://www.livescience.com/9862-good-bacteria-eat-bad-greenhouse-gas.html

[20] U.S. Environmental Protection Agency. (2009) *Electronics Recycling (eCycling)* [Online]. Available: http://www.epa.gov/region2/ecycling/

[21] M. L. Socolof et al. "Environmental Life-Cycle Impacts of CRT and LCD Desktop Computer Displays," *Journal of Cleaner Production*, vol. 13, no. 13-14, p. 1281 – 1294, Nov.-Dec. 2005.

[22] Environment, Health, and Safety Online. (2011) *Battery Recycling and Disposal Guide for Households* [Online]. Available: http://www.ehso.com/ehshome/batteries.php

[23] S. Pulliam. (2011) *Reliability and Safety Analysis* [Online]. Available: https://engineering.purdue.edu/477grp7/Homeworks/hw11_group7.pdf

[24] Oracle. (2011) *MySQL 5.0 Reference Manual* [Online]. Available: http://dev.mysql.com/doc/refman/5.0/en/index.html

[25] 2GIG-CNTRL2KIT5 2GIG Go! Control Panel Wireless Alarm Kit with AT&T GSM. *Tech. The Home Security Store. Web. http://www.homesecuritystore.com/p-1743-2gig-cntrl2kit5-2gig-go-control-panel-wireless-alarm-kit-with-att-gsm.aspx?affiliateid=10054&zmam=55691497&zmas=1&zmac=4&zmap=2GIG-CNTRL2KIT5*.

[26] SecureLinc Wireless Home Security System. *Crutchfield. Web. http://www.crutchfield.com/p_72673903W/SecureLinc-Wireless-Home-Security-System.html?tp=8605*.

[27] 1591EFL Enclosure. *Tech. Hammond Manufacturing. Web. http://datasheet.octopart.com/1591EFLBK-Hammond-datasheet-17673.pdf*.

[28] DC-96F Product Detail Drawing. *Tech. Polycase. Web. http://www.polycase.com/uploads/14531129045666546.pdf*.

[29] *MC9S12C32*. Tech. Freescale Semiconductor. Web. http://us.element-14.com/jsp/search/productdetail.jsp?SKU=70K3229&CMP=AFC-GBE14.

[30] *NanoCore12: An Entire Family of 9S12 DIP Microcontroller Modules*. Technological Arts. Web. http://www.nanocore12.com.

[31] *Xbee®/Xbee-PRO® RF Modules*. Tech. Digi International. Web. http://www.sparkfun.com/datasheets/Wireless/Zigbee/XBee-Datasheet.pdf

[32] *MC9S12C Family Device User Guide V01.10*. Tech. no. 9S12C128DGV1/D. MOTOROLA. Web. https://engineering.purdue.edu/ece362/Refs/9S12_Refs/9S12C128DGV1.pdf.

[33] *RE46C140 CMOS Photoelectric Smoke Detector ASIC with Interconnect and Timer Mode*. Tech. R&E International. Web. http://ww1.microchip.com/downloads/en/DeviceDoc/22179b.pdf.

[34] *MP MOTION SENSOR*. Tech. PANASONIC. Web. http://pewa.panasonic.com/assets/pcsd/catalog/napion-catalog.pdf.

[35] LM35 Precision Centigrade Temperature Sensors. Tech. National Semiconductor. Web. http://www.national.com/ds/LM/LM35.pdf

[36] *Xbee™/Xbee-PRO™ OEM RF Modules*. Tech. MaxStream. Web. http://datasheet.octopart.com/XB24-ACI-001-MaxStream-datasheet-34843.pdf

[37] Glenewinkel, Mark. "The Target Is to Minimize the Voltage from Current Flowing through Ground Impedance." MOTOROLA. Web. https://engineering.purdue.edu/ece477/Homework/CommonRefs/AN1259.pdf.

[38] *Xbee™ ZNet 2.5/Xbee-PRO™ ZNet 2.5 OEM RF Modules*. Tech. Digi International. Web. http://ftp1.digi.com/support/documentation/90000866_C.pdf.

[39] *MC9S12C Family Device User Guide V01.10*. Tech. no. 9S12C128DGV1/D. MOTOROLA. Web. https://engineering.purdue.edu/ece362/Refs/9S12C_Refs/9S12C128DGV1.pdf.

[40] "1A Low Dropout Regulator for 5V to 3.3V Conversion.". National Semiconductor, May 1999. Web. http://pdf1.alldatasheet.com/datasheet-pdf/view/8903/NSC/LM3940IT-3.3.html.

[41] *MC9S12C Family Device User Guide V01.10*. Tech. no. 9S12C128DGV1/D. MOTOROLA. Web. https://engineering.purdue.edu/ece362/Refs/9S12C_Refs/9S12C128DGV1.pdf .

[42] Electret Condenser Microphone.Tech. CUI INC. Web. http://products.cui.com/getPDF.aspx?fileID=3085.

[43] *RE46C140 CMOS Photoelectric Smoke Detector ASIC with Interconnect and Timer Mode*. Tech. R&E International. Web. http://ww1.microchip.com/downloads/en/DeviceDoc/22179b.pdf.

[44] LM35 Precision Centigrade Temperature Sensors. Tech. National Semiconductor. Web. http://www.national.com/ds/LM/LM35.pdf

Appendix A: Individual Contributions

A.1 Contributions of Linda Stefanutti:

The Digijock Home Security (DHS) system is a project that was developed in several months. Many steps brought us to the successful completion of the design and I personally participate at different levels to many of these intermediate steps.

At the very beginning I participated to the design phase of the project, sharing my ideas and my knowledge to define the main features of our DHS. Several hours were spent researching material and documents online. In this step it was important to define the performances of our device, which modules and protocols we needed to get familiar with and how we would be able to reach our goals considering the deadlines in the semester.

The second step in which I took part was testing our circuits. I worked with Stuart in prototyping the circuits for all our sensors like motion, noise and speakers. Sometimes the work required to design our own circuits (amplifier or filters) while other times we just replicated the circuits provided in the datasheets. This step determined many changes in our design according to our successes and failures during these tests. The main work was to reproduce on the breadboard the sensors' circuits to verify if they were actually working and if the values obtained on the microcontroller were the required ones.

In the third step I collaborated again with Stuart in the PCB design. Since I was in charge of the related report, I spent several hours with Stuart to figure out the best location for all our components on the PCB to avoid EMI problems. This phase was particularly challenging considering that the entire team was made by Computer Engineers. For this reason I spent some time getting familiar with EE concepts needed to design the PCB.

Probably the most important step that I was involved in was the fourth step, the software design for the microcontroller. Since I was deeply involved in the prototyping phase of the RSU circuits, I had a clear idea about how each RSU sensor was supposed to work and how these sensors would interact with each other. For this reason I wrote the entire code for the microcontroller while I was finishing testing with Stuart the different sensors. The code was written in embedded C for ease to read and debug. This step of the work required also further considerations in our design. In fact a crucial point of our project was the wireless communication between the CMS and the RSUs. At that point in time we still had issues with the

Xbee module used for this interaction, so the work was suffering a moment of stall. I used the time required to fix our hardware problems to define with Stuart how the wireless communication would have worked in our project. This means that we defined how many packets were sent among the devices, which information each packet was containing and how the packets were processed on both the sides of the communication.

The fifth and last step that I took part in was the final prototyping of the entire system. This step required a close collaboration with Zach, who worked on the software side of the CMS. In fact the major problems that we met were related on how the Xbee module was working between the microcontroller and the Atom Board and how the information was processed on both sides.

As the team leader of the group I also tried during the entire semester to be aware of the work of all the other team members. For this reason I got involved on the packaging development of our final product and I learned from Zach how to test the code for the CMS. Especially at the beginning of the project I also tried to organize the work of the entire team, scheduling meetings and splitting the work among the team members. After this initial phase, almost everyone had a defined role in the group so my supervision wasn’t necessary anymore.

A.2 Contributions of Stuart Pulliam:

In the initial phases of the project, I helped with defining the parameters and scope of our project. Once we knew that we were going to build a wireless home security system, the next step was to select parts and design the circuitry in our RSUs. I selected and purchased the majority of our parts. I designed and prototyped the circuits for detecting smoke, detecting noise, sensing motion, measuring temperature, and sounding a siren. I also designed the power circuitry, which included two voltage regulators, a battery backup, power failure detection, and low battery detection. Finally, I designed our wireless communication circuitry using Xbee modules and a voltage translator.

Once all the circuits were prototyped, the PCB layout had to be designed. I learned how to use PADS Logic, PADS Layout, and PADS Router. I created the circuit schematic in PADS Logic, including creating numerous custom parts that were not included in the provided libraries. At that time I picked out the enclosure for our project so that I could design the PCB layout specifically for the enclosure. Once everything was laid out and routed, I corrected the design so that it had an error-free evaluation by the FreeDFM design checker.

Once we began using the microcontroller to integrate all of our separate circuits, we encountered several difficulties. Several of the sensor sub-circuits did not work well (for example the microphone and thermometer), and I helped with getting those to work with the analog to digital converter. Once the circuits were working with the microcontroller, I helped with testing to make sure that our alarm did not have false alarms and did actually detect the presence of alarm triggers. One of the biggest obstacles we encountered was the Xbee wireless communication failing to work correctly. After much debugging of the circuit and consultation of the documentation, I was able to get bidirectional communication working between the RSUs and the CMS.

Once the PCBs arrived, I helped with portions of the soldering as well as designing the fly-wire modifications that had to be made to the PCB. Also, we had three separate packaging enclosures that had to be measured, cut, painted, and assembled. I helped throughout this process.

There were several software details that remained to be figured out. We had a USB LCD screen for the CMS that needed to display a menu as well as status information. The software that was included with the LCD was written in unmanaged Visual C++. None of us had worked with Visual C++ before, so I spent time learning the language and studying the code in order to be able to incorporate the LCD into our project. It was one of the most difficult aspects of the project that I worked on, and it was rewarding to see it finally work.

Another software challenge was being able to play a sound file (for a siren) on the CMS from within our code. Initially the code would halt upon playing the sound, but I was able to create a function that allowed us to play and stop the siren without interrupting the flow of the rest of the program.

Overall, I contributed to numerous aspects of the project and gained valuable experience in product design, debugging, and assembly.

A.3 Contributions of William Granger:

My first major contribution was coming up with the team name: Digijock Home Security. I also participated in the final deliberations concerning the Project-Specific Success Criteria. Due to my impeccable language skills acquired through my years in Liberal Arts, I was in charge of writing the early homework and TCSP's. Throughout the rest of the semester, I would be responsible for proofreading my teammates various papers and documents. In addition to helping proofread my partners' papers, I also wrote Homework 9 and 12. Towards the end of the semester, I was largely responsible for the final documentation of our project.

Aside from my language abilities, I wasn't able to shine in other areas. Thanks to my years of experience with software and hardware, I was able to play more of the role as a support player. I assisted my teammates in various tasks such as researching parts, helping with soldering, and debugging.

However, I did play a major role in designing the software for the remote sensor units. I first had to familiarize myself with Embedded C and bit-wise operators. I then created the main flowchart which is what the main program is currently based upon. This compelled me to actually write the preliminary main function for the remote sensor unit. In order to make the main function much more readable, I created some functions for changing the values of registers in the microcontroller. To test my code, I made another major contribution to the remote sensor unit by designing and testing the motion sensor circuit.

For the central monitoring station, my input was fairly minimal. My main contribution was the design of the registration page for our website. To do this, I had to look up some information on how to interface C# with MySQL. I made some edits to the main page as well which was just manipulation of the code already there.

I did play a fairly major role in the packaging of our product. The design layout of one of the remote sensor units and the central monitoring station is based off of my design layouts. Drawing inspiration from the Ethical and Environmental Homework, I also created labels for the products that display warnings and recycling information. There were also labels that displayed our product's name and logo.

Lastly, towards the later third of the semester, I made significant contributions to the website. I organized the website into a tighter, more insightful one. All of our final contributions to the project were injected into the website for easy look-up.

A.4 Contributions of Zach Smith:

For our senior design project, we decided to build and implement a wireless home security system with an Internet application. This project took 16 weeks to design and build into a working product. I had several responsibilities throughout the course of this project to ensure that there would be a successful completion of the project.

To kick-start our project we needed to get our website up and running in order to have a centralized place where documentation, homework, and lap notebooks could go. I searched online and went through hundreds of website layout templates that would be appropriate for our needs. I also assisted my teammates in search for specific parts and sensors that we could use in our circuit designs.

Next, I started working on our web application that would let the user login and see status updates of their home. I chose to write it in Visual Studio using ASPX and C# because I had done some previous work with this setup and it worked out well. For database I also chose to use SQL Server because I had previous experience with it. This took quite a bit of time at the beginning of the semester; within the 4^{th} week I had already got the majority of the web application done. I then helped out in other areas of the project and later came back to finish up the web server once we had the remote sensors prototyped.

My next responsibility for this project was to configure and establish our wireless network using 3 Xbee modules. This was by far the most challenging and frustrating part of this project. I was able to configure the wireless modules to have one module act as the main receiver hub and the other two modules act as transmitters for the remote sensors. I had an issue with the Xbee modules working together with the Tx and Rx pins of the microcontroller. After many days and hours of debugging with Stuart we found a solution and ultimately got the wireless working as expected.

Next, I worked with packaging and the PCB. I was in charge of soldering the components to both PCB boards. With the help of all team members, both PCB boards were soldered without any significant issues or problems. I also worked on packaging up the final project of both remote sensor units. With the assistance of all team members we were able to package everything up together without too many issues.

My final responsibility for this project was the software for the central monitoring station. I chose to use visual C# because again I had past experience with this language and felt that this language supported everything we needed it to do. It took awhile to establish the framework of how it was going to communicate with the remote sensor units, but after careful consideration my teammates and I ironed out all the problems I saw and got a working main program for the CMS.

Over all for this project, I felt I contributed in many parts to make this a successful project for my team and me. I have gained valuable experience in many different areas including product and circuit design, debugging and product packaging.

Appendix B: Packaging

Note: All measurements are in millimeters.

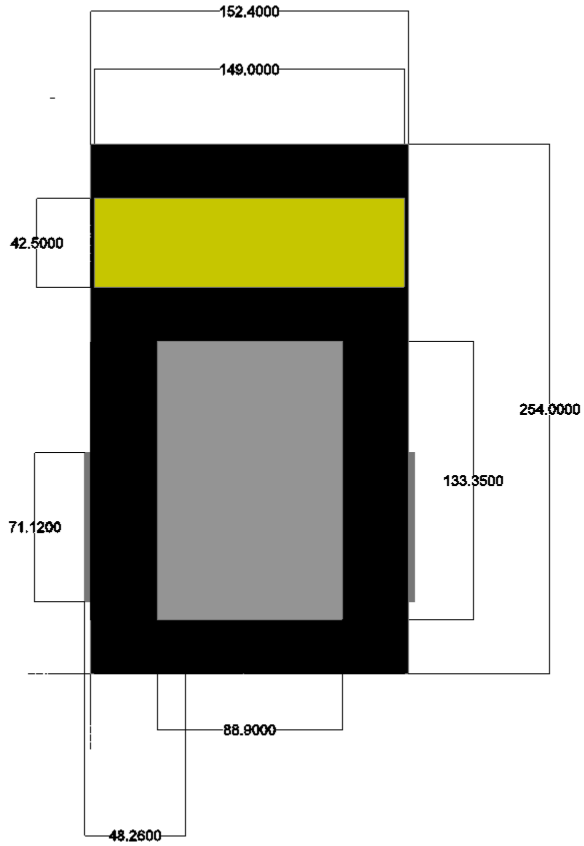

Figure B-3: Front view of control unit featuring LCD screen, keypad, and speakers on the sides.

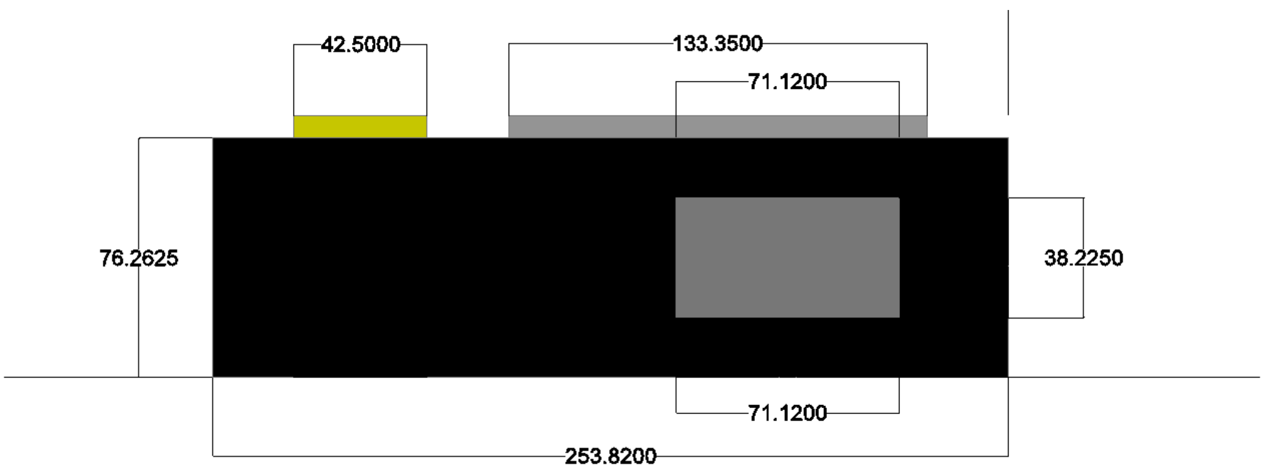

Figure B-4: Left side view of control unit featuring speaker with LCD and keypad visible on top.

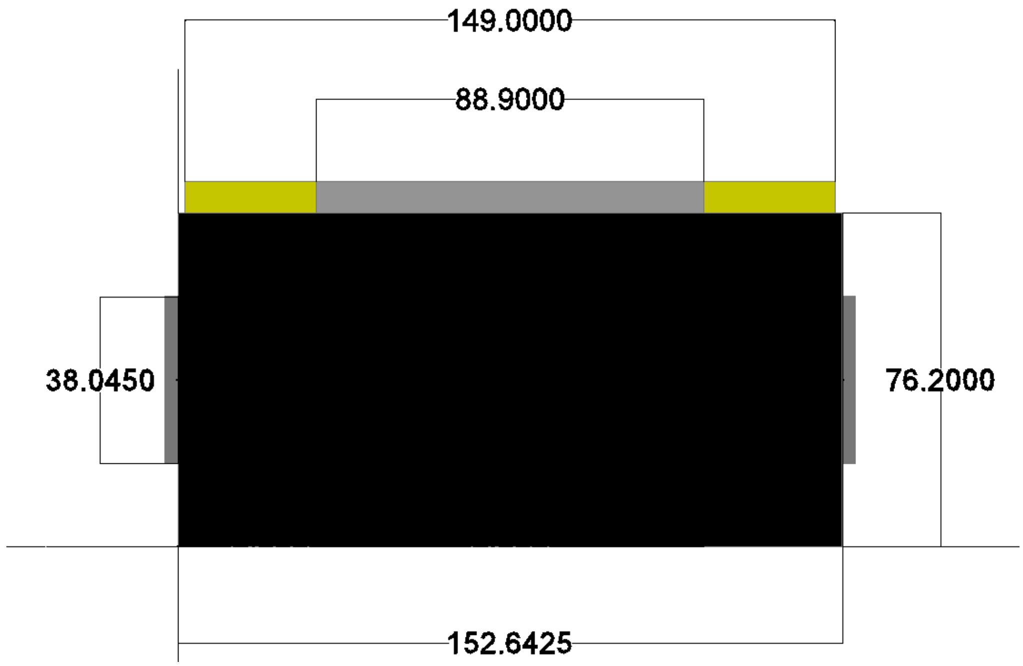

Figure B-5: Bottom-side view of control unit with speakers visible on sides and LCD and keypad visible on top.

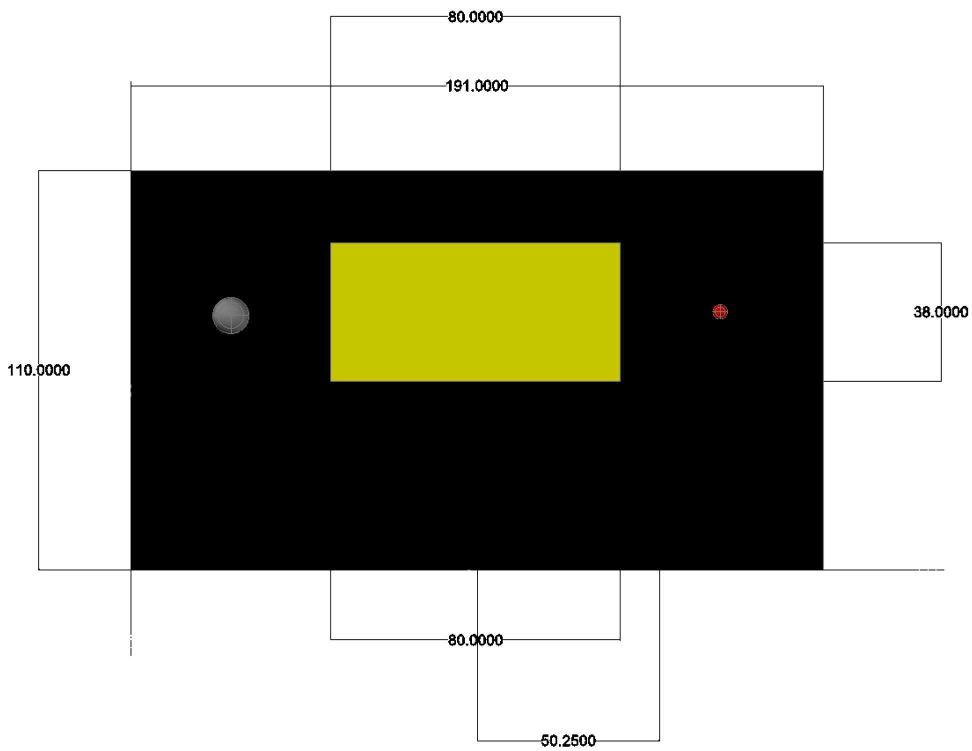

Figure B-6: Front view of sensor unit featuring the motion sensor, LCD, and LED.

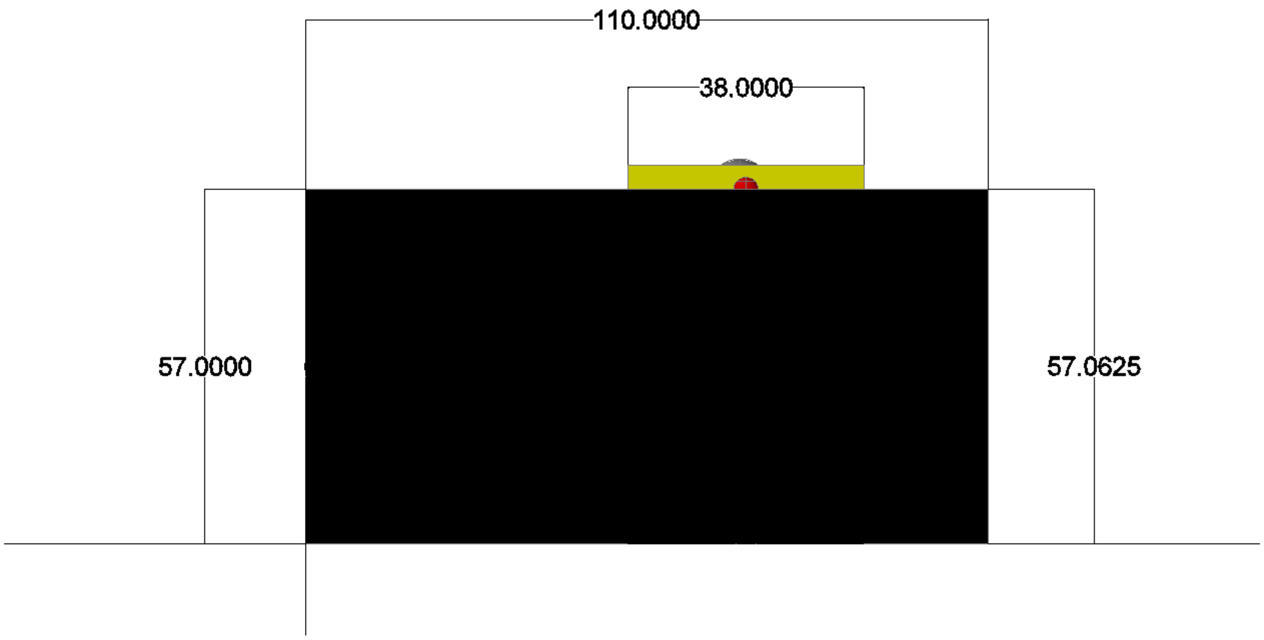

Figure B-7: Right side view of sensor unit with LED, LCD, and motion sensor visible on top.

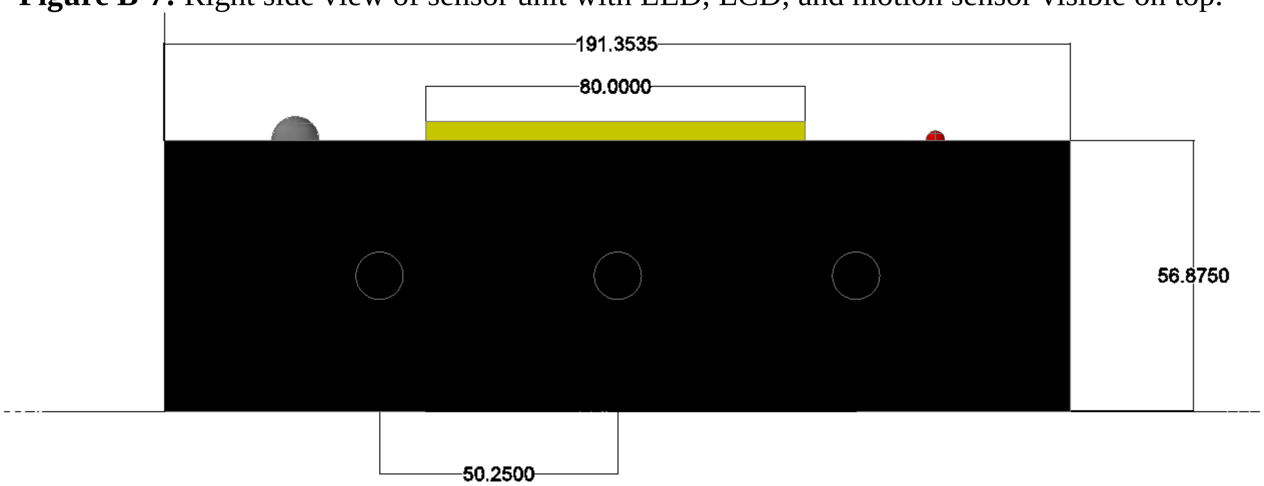

Figure B-8: Bottom-side view of sensor unit featuring ventilation holes with the motion sensor, LCD, and LED visible on top.

Appendix C: Schematic

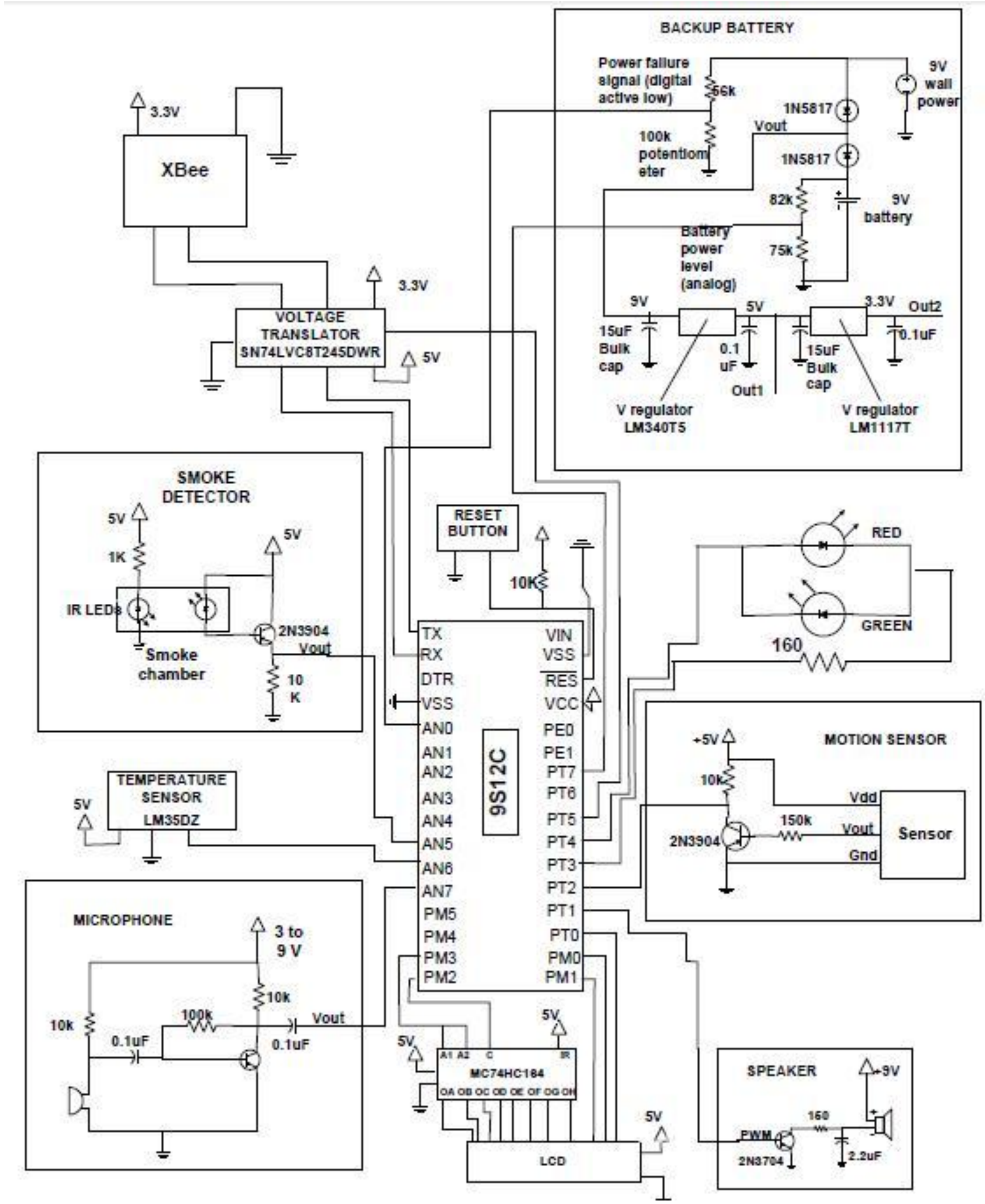

Figure C-1: RSU Schematic

Appendix D: PCB Layout Top and Bottom Copper

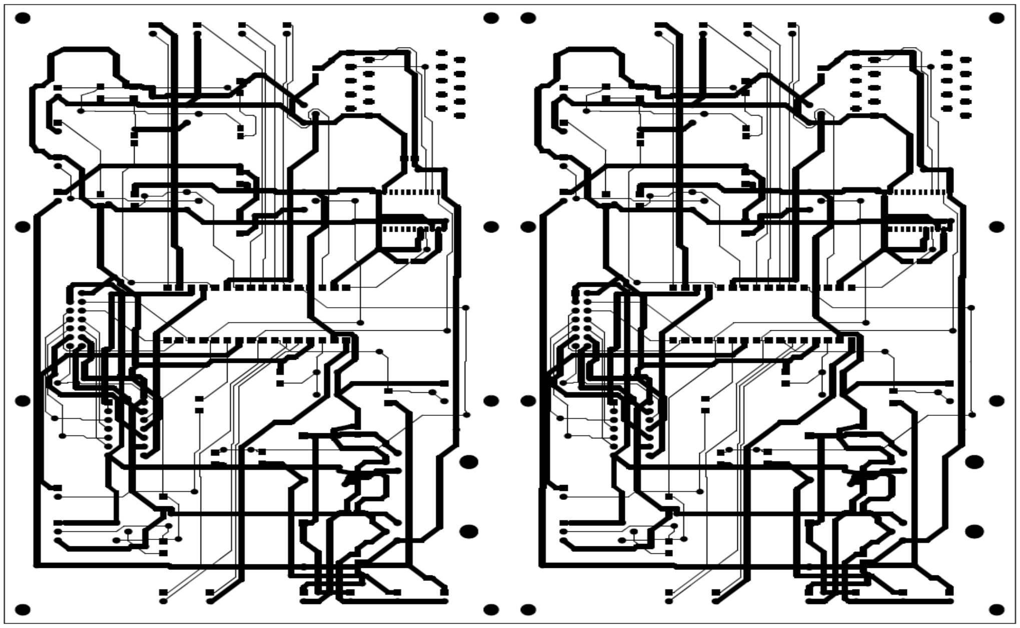

Figure D-1: Top and Bottom Copper

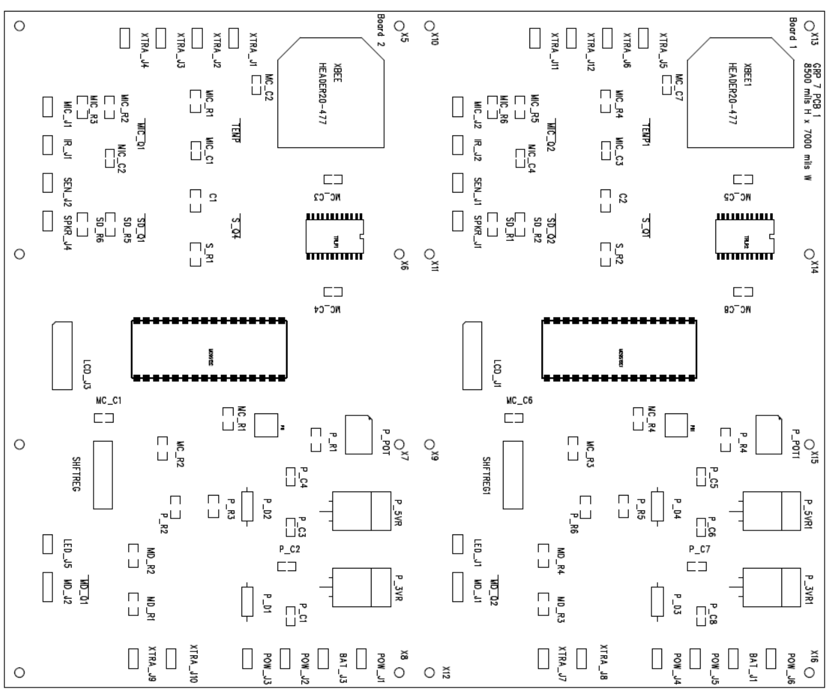

Figure D-2: With Silkscreen

Appendix E: Parts List Spreadsheet

Appendix A: Parts List Spreadsheet						
Vendor	*Manufacturer*	*Part No.*	*Description*	*Unit Cost*	**Qty**	*Total Cost*
RobotShop.com	Freescale	M68DKIT912C32	32-bit microcontroller	21.00	2	$42.00
Digi-Key	Analog Devices Inc	AD8494ARMZ-ND	THERMOCOUPLE AMPLIFIER IC	4.30	2	$8.60
Digi-Key	Microchip Technology	RE46C140E16F-ND	IC SMOKE DETECTOR CMOS 16-DIP	0.96	2	$1.92
Digi-Key	Panasonic Electric Works	255-2649-ND	SENSOR MOTION 10M DETECT BLK LEN	14.31	2	$28.62
Digi-key	Parallax Inc	27977	LCD MODULE 16x2 BASIC STAMP	29.99	2	$59.98
Digi-key	PUI Audio, Inc.	668-1136-ND	SPEAKER 8OHM .15W 72DB 30MMPC MT	3.20	2	$6.40
Digi-key	CUI Inc	102-1720-ND	MIC CONDENSER ELECT OMNI -42DB	1.03	2	$2.06
Mini-Box	Mini-Box	Not Listed	PICO LCD 256X64 SLIDESHOW	59.85	1	$59.95
Digi-key	DigiInternational/ Maxstream	XB24-BUIT-004-ND	MODULE 802.15.4 SER 2 U.FL CONN	21	3	$63
Digi-key	DigiInternational/ Maxstream	**XB24-ACI-001-ND**	MODULE 802.15.4 1MW W/CHIP ANT	19	1	$19
Amazon	Targus	Not Listed	Targus PAUK10U Ultra Mini USB Keypad	3.36	1	$3.36
Amazon	Altec Lansing	iML237	PORTABLE USB-POWERED SPEAKER	20.61	1	$20.61
PriceGigs	Intel	D945GSEJT	DESKTOP MOTHERBOARD	97.65	1	$97.65
Logic Supply	Morex	T1610	MINI-ITX CASE	65.00	1	$65.00
				TOTAL		**$478.15**

Appendix F: FMECA Worksheet

Table F-1. Block A, Microcontroller functional block FMECA analysis

Failure no.	Failure mode	Possible cause	Failure effects	Method of detection	Criticality	Remarks
A1	Output continuously '1'	MC9S12, PB, MC_R1, TRLR_R1, TRLR_R2, MC_R2, MC74HC164, software	Loss of LCD display, wireless connection, and status LED, siren activated, loss of all detection	Loss of wireless connectivity	High	E-mail/SMS notification sent
A2	Output continuously '0'	MC9S12, PB, MC_R1, TRLR_R1, TRLR_R2, MC_R2, MC74HC164, software	Loss of LCD display, wireless connection, and status LED, siren disabled, loss of all detection	Loss of wireless connectivity	High	A1, A2: Microcontroller block is non-functional. Output could be stuck in either state. E-mail/SMS sent
A3	Output erratic values	MC9S12, PB, software	Random letters on LCD, random packets sent, random LED glow, erratic siren, loss of all detection	Invalid packets transmitted by RSU to CMS	High	E-mail/SMS notification sent
A4	Fail to detect correct voltage level of inputs	MC9S12, PB, software	Erratic reading on sensors, inability to receive packets	Invalid packets transmitted by RSU to CMS	High	E-mail/SMS notification sent

Table F-2. Block B, Power circuitry functional block FMECA analysis

Failure no.	Failure mode	Possible cause	Failure effects	Method of detection	Criticality	Remarks
B1	5V Output = 0V	Can be caused by a failure of any component within functional block B or an external short	Loss of smoke and intruder detection, no power to any of circuit	Loss of wireless connectivity	High	E-mail/SMS notification sent
B2	3.3V Output = 0V	Can be caused by a failure of any component within functional block B or an external short	Loss of intruder detection, no wireless connectivity	Loss of wireless connectivity	Medium	E-mail/SMS notification sent
B3	Output above 5V or 3.3V	Failure of P_5VR or P_33VR	Potential for system damage and loss of intruder detection	Loss of wireless connectivity	High	E-mail/SMS notification sent
B4	BAT_LVL signal stuck high	P_R2, P_R3, P_D2	Invalid battery level measurement	Observation	Low	If P_D2 fails, the MCU could be damaged
B5	BAT_LVL signal stuck low	P_R2, P_R3	Invalid battery level measurement	Observation	Low	Battery reading will be zero despite fresh batteries
B6	IS_PWR signal stuck high	P_D1, P_R1, P_POT	RSU always reports wall power is present even if on battery	Observation, MCU measures that battery begins discharging	Medium	The battery will eventually die and the CMS will send an E-mail/SMS notice
B7	IS_PWR signal stuck low	P_POT, P_R1	RSU reports that there is no wall power	Observation	Low	Errant E-mail/SMS will be sent out

Table F-3. Block C, Peripheral circuitry functional block FMECA analysis

Failure no.	Failure mode	Possible cause	Failure effects	Method of detection	Criticality	Remarks
C1	Temperature sensor outputs logic high	Temp	Inability to measure temperature	Unrealistic temperature reading	Low	e-mail sent
C2	Temperature sensor outputs logic low	Temp	Inability to measure temperature	Unrealistic temperature reading	Low	e-mail sent
C3	Temperature sensor erratic	Temp	Inability to accurately measure temperature	Observation	Low	
C4	Noise sensor outputs logic high	MIC_R2, MIC_R3, MIC_Q1, Microphone	Inability to detect sound, siren turns on without cause	Unexpected value observed from sound reading	Medium	RSU can send notice to CMS, e-mail/SMS notification sent
C5	Noise sensor outputs logic low	MIC_C2, MIC_Q1, MIC_R1, MIC_R2, Microphone	Inability to detect sound	Observation	Medium	
C6	Noise sensor erratic	Can be caused by failure of any component within noise sensor circuit	Inability to accurately detect sound	Observation	Medium	
C7	Speaker never turns on	S_C1, S_R1, S_Q4, Speaker	Inability to alert user of danger	Observation	High	
C8	Speaker never turns off	S_C1, S_R1, S_Q4	Inability to accurately alert user of danger, annoyance of user, decreased battery life	Observation	High	
C9	Erratic speaker operation	S_Q4, Speaker	Inability to accurately alert user of danger, decreased battery life	Observation	High	

C10	Smoke sensor outputs logic high	D1, SD_Q1	Inability to detect smoke, siren turns on without cause	Unrealistic smoke reading	High	RSU can send notice to CMS, e-mail/SMS notification sent
C11	Smoke sensor outputs logic low	SD_R5, SD_Q1, D1, LED, SD_R6	Inability to detect smoke	Observation	High	
C12	Smoke sensor erratic	SD_R5, SD_Q1, D1, LED, SD_R6	Inability to accurately detect smoke	Possible unrealistic smoke reading	High	RSU can send notice to CMS if detected, Possible e-mail/SMS notification sent
C13	Motion sensor outputs logic high	Can be caused by failure of any component within motion sensor circuit	Inability to detect motion, siren turns on without cause	Observation	Medium	
C14	Motion sensor outputs logic low	Can be caused by failure of any component within motion sensor circuit	Inability to detect motion	Observation	Medium	
C15	Motion sensor erratic	Can be caused by failure of any component within motion sensor circuit	Inability to accurately detect motion	Observation	Medium	

Table F-4. Block D, Wireless circuitry functional block FMECA analysis

Failure no.	Failure mode	Possible cause	Failure effects	Method of detection	Criticality	Remarks
D1	RX line always low	TRLR1, XBEE, MC_C2, MC_C3, MC_C4	Unable to receive packets, siren won't sound in case of non-fire trigger	Observation	Medium	
D2	RX line always high	TRLR1, XBEE, MC_C2, MC_C3, MC_C4	Unable to receive valid packets, siren won't sound in case of non-fire trigger	RSU receives invalid packets	Medium	RSU can send notice to CMS, E-mail/SMS notification sent
D3	RX line erratic	TRLR1, XBEE, MC_C2, MC_C3, MC_C4	Invalid packets received, siren won't sound in case of non-fire trigger	RSU receives invalid packets	Medium	RSU can send notice to CMS, E-mail/SMS notification sent
D4	TX line always low	TRLR1, MC_C4	Unable to send packets, siren won't sound in case of non-fire trigger, database not updated	Atom board stops receiving packets	Medium	E-mail/SMS notification sent
D5	TX line always high	TRLR1, MC_C4	RSU sends invalid packets, siren won't sound in case of non-fire trigger, database not updated	Atom board receives invalid packets	Medium	E-mail/SMS notification sent
D6	TX line erratic	TRLR1, MC_C4	RSU sends some invalid packets, siren won't sound in case of non-fire trigger, database not updated	Atom board receives invalid packets	Medium	E-mail/SMS notification sent