

MACHINE TO MACHINE COMMUNICATION
FOR PHYSICAL SECURITY

By

Mark Bryan Goff

Approved:

Ahmed H. Eltom
Professor of Electrical Engineering
(Director of Thesis)

Abdul R. Ofoli
Assistant Professor of Electrical Engineering
(Committee Member)

Stephen Craven
Adjunct Professor of Electrical Engineering
(Committee Member)

William H. Sutton
Dean of the College of Engineering and
Computer Science

A. Jerald Ainsworth
Dean of the Graduate School

MACHINE TO MACHINE COMMUNICATION
FOR PHYSICAL SECURITY

By

Mark Bryan Goff

A Thesis Submitted to the Faculty of the University
of Tennessee at Chattanooga in Partial
Fulfillment of the Requirements of the
Degree of Master's of Science
in Electrical Engineering

The University of Tennessee at Chattanooga
Chattanooga, Tennessee

May 2013

UMI Number: 1537079

All rights reserved

INFORMATION TO ALL USERS

The quality of this reproduction is dependent upon the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript and there are missing pages, these will be noted. Also, if material had to be removed, a note will indicate the deletion.



UMI 1537079

Published by ProQuest LLC (2013). Copyright in the Dissertation held by the Author.

Microform Edition © ProQuest LLC.

All rights reserved. This work is protected against unauthorized copying under Title 17, United States Code



ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 - 1346

ABSTRACT

The objective of this study was to research the core principles of Machine to Machine (M2M) communications methodology and create a framework that can be used to lower the total cost of ownership for a system. The second objective was to demonstrate an M2M communications application for physical security using an array of interacting machines. This study also demonstrates that M2M communication framework can be used to bring cost savings to the consumer.

In the designed application, the individual machines were stitched together to coordinate with the subscribers by using wired and wireless sensors, wireless personal area networking (WPAN), and complex coding for Programmable Logic Controllers (PLC), for delivering data to a central controller and the internet. Based on the processed data, information was generated and passed to the subscribers. The demonstration of the M2M communication system followed the developed framework to illustrate the technical steps and provided the cost justification to replace an older system.

TABLE OF CONTENTS

LIST OF TABLES.....	vi
LIST OF FIGURES.....	vii
LIST OF ABBREVIATIONS.....	ix
CHAPTER	
1. INTRODUCTION.....	1
Principles of Machine to Machine Communications.....	1
Data Collection.....	2
Data Transmission.....	3
Data Assessment.....	4
Action Generation.....	5
Applications of M2M Communications.....	5
2. PHYSICAL SECURITY USING MACHINE TO MACHINE COMMUNICATIONS ..	6
Research Task.....	6
Requirements.....	6
Prior Art.....	7
3. WIRED SENSORS	10
Sensors for Status.....	10
Sensors for Counters	11
4. WIRELESS SMART SENSORS.....	16
Fundamentals for Using ZigBee for Wireless Sensors.....	16
Garage Door Open / Close / Moving / Stopped Wireless Sensors.....	18
Garage Door Range Wireless Sensors.....	19
Motion Detector Wireless Sensors.....	20
Wireless Gas Sensors	21
Microprocessors to Make Sensors Smart	26
A Microprocessor to Aggregate the Wireless Data.....	31

5. MAIN CONTROL UNIT	33
Cubloc CT1721C PLC / Microprocessor	33
Wired Inputs and Outputs to the MCU	34
Wireless Inputs and Outputs to the MCU	37
6. HMI, WEB SERVER AND TEXT MESSAGING	40
Output to the User	40
HMI Interface	40
Web Server Interface	42
SMS Messaging Interface	44
7. CONCLUSIONS	47
M2M for Physical Security	47
Summary	47
REFERENCES	48
VITA	50

LIST OF TABLES

4.1 Figaro Gas Sensors.....	23
4.2 Protocol for Garage Door Sensor & Control Board.....	28
4.3 Protocol for Motion Detectors.....	29
4.4 Protocol for Gas Detectors.....	30

LIST OF FIGURES

3.1	Using a Reed Switch for Status Data Input.....	11
3.2	The Hall Effect Principle.....	12
3.3	Hall Effect Switch.....	13
3.4	Pictorial of the Water Flow Sensor.....	13
3.5	Water Piping Before the Installation.....	14
3.6	Items Needed for the Water Meter and Electric Shut-Off Valve Installation.....	15
3.7	Installation of the Water Meter, Pressure Regulator, and Shut-off Valve.....	15
4.1	XBee Pro Module and Pin Outs.....	17
4.2	Garage Door Block Diagram for Sensors.....	18
4.3	Maxbotix MB1010 Sonar Range Finder Sensor.....	19
4.4	Parallax PIR Sensor (Revision B).....	21
4.5	Typical MQ Series Gas Sensor.....	23
4.6	Sensor Output as Heater Voltage Varies and Gas Concentration Varies.....	24
4.7	Circuit Diagram for MQ - X Figaro Gas Sensors.....	25
4.8	Calculating the Voltage Output from a Gas Sensor.....	25
4.9	CB320 Microprocessor and PLC on a Chip.....	26
4.10	Garage Door Sensor & Control Board PCB.....	27
4.11	Garage Door Sensor and Control Board Block Diagram.....	27
4.12	Motion Detector Board Block Diagram.....	29

4.13 Gas Detector Board Block Diagram.....	30
4.14 CB380 Microprocessor and PLC on a Cubloc Header Board.....	31
4.15 Wireless Transceiver Board.....	32
4.16 Transceiver Board to Master Control Unit Interface.....	32
5.1 Cubloc CT1721C.....	33
5.2 Wired Sensor Machine to Master Control Unit Interface.....	34
5.3 PLC Ladder Logic for One Wired Sensor Machine Input.....	35
5.4 LED Color Based on Status of the Door or Window.....	36
5.5 PLC Logic to Drive One of the 16 LEDs.....	36
5.6 PLC Logic for Car in the Garage Status.....	37
5.7 PLC Logic for Wireless Motion Detectors.....	38
5.8 The Master Control Unit.....	39
6.1 The HMI Touch Screen Interface.....	42
6.2 The Web Server Hardware Interface.....	43
6.3 The Web Server Web Page Display.....	43
6.4 Example of Code to Send an Email Message.....	44
6.5 The Display of a iPhone Receiving a SMS.....	45
6.6 The Overall View for M2M Communications for Physical Security.....	46

LIST OF ABBREVIATIONS

A/D, Analog to Digital Converter

ASCII, American Standard Code for Information Interchange

DC, Direct Current

DIP, Dual Inline Pin

HTML, Hypertext Markup Language

IEEE, Institute of Electrical and Electronics Engineers

ISM, Industrial, Scientific and Medical

ISP, Internet Service Provider

KHz, Kilo Hertz

LAN, Local Area Network

LPG, Liquid Propane Gas

LTE, Long Term Evolution

M2M, Machine to Machine

MCU, Master Control Unit

mA, Milliamps

mW, Milliwatt

PAN, Personal Area Network

PCB, Printed Circuit Board

PIR, Passive Infra Red

PLC, Programmable Logic Controller

ROI, Return on Investment

RTC, Real Time Clock

SCADA, Supervisory Control and Data Acquisition

SMTP, Simple Mail Transfer Protocol

SMS, Short Message Service

V, Volts

WAN, Wide Area Network

WiMAX, Long Term Evolution (4G/LTE)

WLAN, Wireless Local Area Network

WPAN, Wireless Personal Area Network

WSN, Wireless Sensor Network

CHAPTER 1

INTRODUCTION

Principles of Machine to Machine Communications

Machine to Machine (M2M) communications is transforming the world of individuals, businesses, industries, and governments. It allows the sharing of data, information and actions at the speed of light from across the room to around the globe. It provides monitoring and control in real time from remote locations.

M2M communications is the flow of data (uplink and/or downlink) from one machine to another machine without human intervention for the purpose of producing better information to the user. An overall simple view can be illustrated by a sensor converting a physical quantity into data. The sensor communicates the data over a communication link to another machine where the data is processed. It may take many exchanges of data between machines to properly assemble the data. Once the data has been assimilated, it is presented to the user. The user may be a person or another machine. The user acts upon the processed data and creates an action. This action may be in the form of data input from a machine or an action from a person such as a key stroke or a click of the mouse. The data input flows to the processing machine. The processing machine packages the data and sends it in the form of a command through a communication link to a receiving machine. The receiving machine takes the data and converts it into a real life physical action. This cycle acts as a feedback loop to control and manage the overall system.

Even though every installation is unique and with varying levels of complexity, there is a common theme with the following four core principles throughout any M2M deployment. They are the following: [1]

- Data Collection (Sensor Machine)
- Data Transmission (Communication Network)
- Data Assessment (Processing Machines)
- Action Generation (User Response)

Data Collection

Data can be as simple as status of a switch or as complex as multiple links to a super computer on the internet. The process starts with a sensor or a sensing machine for the purpose of gathering the data from its environment. Here a physical property such as a status (off / on), pulse count, temperature, content level of a tank, weight of an object, video image, etc. is converted to an electrical signal and packaged such that it can be communicated.

The data can be collected by a Slave machine or a Master machine. A Slave machine has only the basic ability to gather data and must be instructed by a Master machine on when and what type of data to collect. The simplest Slave machine is a switch which is used as a status indicator. A Master machine is more complex because it has a built in processing unit. A Master machine could take the same input of status and use its processing power to count the number of status changes or measure the time between status changes. There are advantages to the Master machine since data can be processed nearer to the collection point. The processing allows for a local display of the data or an alarm. But, this can be a disadvantage because of a higher cost and the requirement for a power source nearer to the sensor.

Data collection has greatly improved in recent history due to advancements in sensor technology, battery technology and microprocessor technology which has allowed many more devices to become a Master machine. These technology advancements have taken the previous generation of Supervisory Control and Data Acquisition (SCADA) which used mostly Slave machines, into today's world of M2M communication using mostly Master machines.

Data Transmission

Next the data is packaged into a form such that it can be communicated across a network. This mainly takes place in a Master Machine since it has the processing power to package or format the data into what is known as a data protocol. Data protocols come in various forms. The designer of a protocol must balance data integrity, data speed and data transmission cost.

Data transmission options have become much more available in hard-to-reach places due to improvement in wireless communication. In the past few years the world has been introduced to a wide variety of new radio technologies and standards. These technologies include ZigBee for wireless personal area network (WPAN) [2], Wi-Fi for wireless local area network (WLAN) [3] and 4th Generation wireless such as LTE for wide area network (WAN) [4]. Also, the advances in telecommunications have made better use of the spectrum, lower costs, expanded interoperability, increased security, reduced hardware size and increased data rates.

As the communication infrastructure has grown, gateways have been added to allow more systems to interact. Gateways receive data from one system and pass it to another system. Gateways play a vital role in the transportation of data because they allow a point for routing, security and isolation between communication systems. The gateways can convert data rates and protocols to keep the communication flowing smoothly across multiple networks.

Gateways provide a good place to divide the system between the users and providers. One example is where a Telecom Company provider can sell its back haul or middle mile services to end users. This allows the users to be part of the network without installing a large infrastructure. The Telecom Company can provide a huge infrastructure since it has many subscribers to share the cost.

Data Assessment

Data Assessment can be as simple as standalone system or managed across the enterprise system. A standalone system is the state of the art for smaller users because M2M communications is monitoring and controlling a specific process. The smaller users need to have a return on investment (ROI) [5] before moving forward to an enterprise system. Larger users have seen the business case and have moved their most critical processes to an enterprise system approach.

Southwest Airlines offers a good example of an enterprise system. They offer a unique M2M communication system for tracking and monitoring critical air cargo. [6] As of December 2012, they offer services to 73 cities while operating more than 3,300 flights a day. This M2M communication solution offers six real-time metrics including location, shock, vibration, temperature, pressure, and humidity of the cargo during transit. The customer receives updates via email or by the Southwest Cargo website. This approach has a great value add for their customers who are shipping critical cargo that needs special attention.

M2M communication for Physical Security offers an opportunity of improvement for the consumer. Today, Security Company's system acts more like the previous generation of SCADA rather M2M communication. As processing power and communication infrastructure improves M2M communication at home will begin to reach the consumer at an affordable price.

This is because the consumer can purchase the desired sensing machines and data processing machines. Then using M2M communication, the information can be forwarded directly to them without going through a third party provider thus lowering the total cost of ownership.

Action Generation

The final element for M2M communications is to alert the user to take some action. The first three elements are virtual elements, but they all culminate into requiring a response by the user. Continue to monitor may also be considered an action.

The overall purpose for M2M communications is to gather, communicate, and process data to keep a system running smoothly. Before M2M, only a few sensor points of a system were known. Now, with multiple machines with sensors interacting with other machines, complex sensor arrays can be installed to allow better and faster decisions by the user.

Applications of M2M Communications

M2M communications touches or has the capability of touching almost every aspect of life [7]. They include but not limited to:

Physical Security - Surveillance systems, Alarm systems, Access control

Tracking / Navigation - Fleet management, Toll road pass and pay, Traffic flow

Infrastructure Justification - Traffic flow, Bridge usage

Electric Power System - Smart Grid, Power flow and usage

Financial System - Stock market analysis and trends, Inventory, Sales

Health Care - Medical monitors, Remote diagnosis,

Auto Insurance - Monitoring driving behaviors, In-vehicle accident recorders

Government - Military surveillance, Advance weapons, Satellites

CHAPTER 2

PHYSICAL SECURITY USING MACHINE TO MACHINE COMMUNICATIONS

Research Task

The objective of this study was to research the core principles of Machine to Machine (M2M) communications methodology and create a framework that can be used to justify M2M communication for other applications by giving a ROI in less than 36 months. The second objective was to demonstrate an M2M communications application for physical security using an array of interacting machines. This framework explained how the use of M2M communication will lower total cost of ownership for physical security. Also, the framework can be applied to a variety of older systems.

The demonstration involved building wired and wireless sensor machines for inputs that can ultimately alert the user by the following three methods without relying on a third party company that charges an ongoing monthly fee:

- 1) Local indicator on the human machine interface (HMI) unit
- 2) Text message/short message service (SMS)
- 3) Web page update

Requirements

Since the project for this demonstration was designed from the ground up, it required custom printed circuit boards (PCB) to be designed, etched and drilled. It also required removing of the old plumbing (water pressure regulator and piping) and soldering in a new water

meter, pressure regulator, electric water shut-off valve, and water pressure gauge. Special sensors had to be researched, designed and installed. The most complex sensors built were those for measuring/controlling the water flow and sensing the presence (or not) of a vehicle in the garage. Other sensors were much simpler and only consisted of a magnetic reed switch that reports the status (open or closed) of a door or window. The communication system links required hardware and software solutions. These solutions incorporate hardwire, ZigBee for WPAN, Comcast for the ISP, and 4th Generation wireless for WAN. The processing of the data required programming of a microprocessor and programmable logic controller (PLC) on some of the sensors. The web server required coding using hypertext markup language (HTML) code. But the most complex programming (over 2,500 lines of code) took place on the Master Controller Unit (MCU) which contains the human machine interface (HMI). Testing at each step was paramount to guarantee the smooth operation between each of the four core principles of M2M communications.

Prior Art

Supervisory Control and Data Acquisition (SCADA) was the forerunner to M2M Communication. SCADA was developed for the power industry for operating the major assets of the power grid. Each major high voltage substation was equipped with a communication link such as a private leased telephone line, optical fiber or microwave tower. SCADA gave the power grid operators the ability to read analog points such as the station voltages, the line currents and power flow across the power grid. SCADA also gave the status points of each breaker, switch and alarm. The operators could control the power grid as needed by sending a control signal to manipulate the equipment on the remote end. Since most of these points

required little or no processing power, slave machines were mostly used. Mobility was not a requirement because everything being monitored or controlled was stationary.

As needs and technology evolved, M2M communication emerged to replace SCADA. M2M uses more Master machines and has the flexibility of connecting fixed or mobile assets. OnStar[8] was one of the first and best known M2M communication companies. It was introduced by General Motors in 1996. Due to the popularity of OnStar, M2M communication became a goal for all industries. However, M2M communication was held back from most industries because of the high cost of communication links between machines. This was improved by the early 2000's when high speed internet became wide spread. However, M2M communication for mobile machines was still expensive. Cell phone technology opened the door for mobile communication links as the cell phone technology made major steps to lower cost and increase data rates. The 3th Generation of cellular technology was deployed in several markets by 2005 [9]. However, it did not become main stream until early 2008. Shortly thereafter, the smart phone market exploded with the introduction of the iPhone 3G in July 2008[10]. The growth potential of M2M communications was opened up due to the advancements in high speed, mobile and wide area communication technology,

Running parallel in time, Personal Area Network (PAN) technology was being developed. When cell phones became an accessory many user desired. A wireless "Hands Free" head set was the largest application for Bluetooth. However, sensors were not able to take advantage of Bluetooth because it was expensive, complex and lacked network topology flexibility. The ZigBee Alliance [11] was formed and set out to construct another PAN for wireless sensor networks (WSN) to address the shortcomings of Bluetooth. In 2003, the ZigBee Alliance ratified the ZigBee stack that operates on the IEEE 802.15.4 specification. ZigBee has multiple network topologies like: 1) Point to Point, 2) Point to Multipoint, and 3)

Mesh Network which was one of the key components needed for WSN. [12] ZigBee also included the security, simplicity, and low power requirements which made it the PAN of choice for any WSN. M2M communications has taken off since 2009 because all the infrastructure pieces were in place for a robust M2M communication system. According to M2M magazine, 90 million homes are expected to employ home automation by 2017 [13]. Most of the work for the home looks to be focused on the Home Automation applications but not Home Security [13].

Engineering research comprises nearly half of the papers and articles that drills deep into the wireless infrastructure options and standards because communication is the hub of the M2M communications infrastructure [14][15]. Most of the remaining papers and articles are geared toward a high level view for the commercial infrastructure systems. These articles give little detail how a system works, but typically focus on models for the future. [16][17]. Only a few papers look at an M2M communication applications for the consumer [13]. However, these few are for home automation, not physical security. This is because physical security still relies on the previous generation approach using the SCADA model.

The technological pieces are in place but a paradigm shift is needed. This shift can take place by building a framework that uses M2M communication principles for a consumer market application for physical security and to construct the hardware to demonstrate the feasibility. The upfront cost can be capitalized since it is a one time upfront cost to replace the old SCADA type system. A SCADA type system requires a central control center hosted by a security company. Depending on the security company the monthly charges range from \$35.99/mo to \$46.99/mo.[18]. This is an operational expense that never ends.

The M2M communication application of this study illustrates how more features can be added while having a ROI in less than 3 years. This approach is a road map such that other applications can be upgraded using the same framework of principles for M2M communication.

CHAPTER 3

WIRED SENSORS

Sensors for Status

The sensor to indicate the status of a door or window is as simple as a switch. The switch is connected to the Master Control Unit by two wires. The advantage to using a switch as a sensor is because the power is supplied from a remote location and no local power source is needed. The switch sensor uses a #22 gauge wire which is very small. This size wire will work for switches up to 500 feet from the source because the current requirements are less than 10mA and the voltage is only 12 VDC.

The status can be one of two ways. A closed door / window status can either be represented by an open or closed switch. It is best to use a closed switch to represent a closed door / window. This gives two advantages. First, multiple switches can be put in series to create a zone. If any door or window in the series loop is opened then the status will change to open for the zone. Second, if someone wanted to break in they may cut a sensor wire thinking they have disconnected the sensor from the system. This would not work because cutting a wire would be the same as opening a door or window in the zone of protection because it would open up the circuit which is interpreted by the Master Control Unit as an open status.

A reed switch and magnetic combination is commonly used in this type of application because it is a hermetically sealed unit and easy to install. The reed switch is constructed of two small wires with a ferric coating inside a glass hermetically sealed tube. These two wires do

not touch but when a magnet approaches these two wires, they make contact. This works great for a door or window. The magnet is embedded in the movable section and the reed switch is in the stationary section. When a door or window is closed, the magnet is in very close proximity to the reed switch and the wires make a good connection. See Figure 3.1. When the door or window opens the magnet moves away from the reed switch and the contacts open.

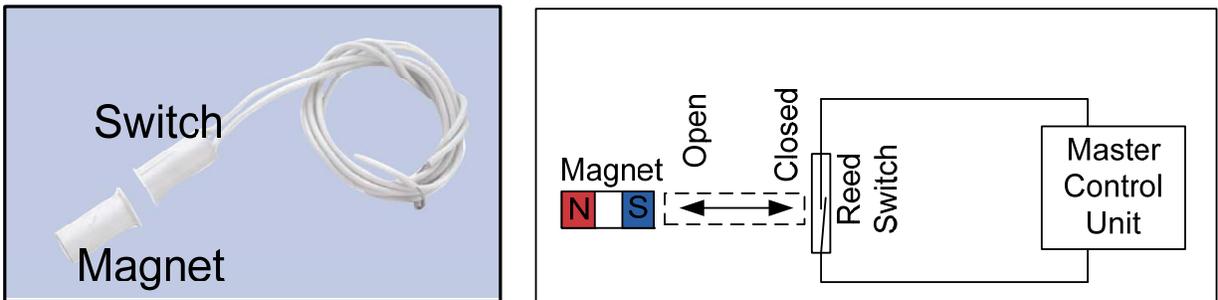


Figure 3.1 Using a Reed Switch for Status Data Input

Sensor for Counters

A counter sensor is similar to a status sensor because it detects opens and closes. But instead of reporting an open or close status, a counter sensor needs keep track of a sequence of opens and closes. In other words, a counter sensor counts the number of open-close-open or close-open-close (pulses).

If the pulses are moving slow, then a reed switch will work fine. But, in some cases such as a counting the number of revolutions of a rotating shaft on a motor, a solid state semiconductor switch is needed. This solid state switch is a Hall Effect Switch.

The Hall Effect occurs when a magnet approaches a thin piece of p-type semiconductor material that has a constant current flow across it. The magnetic flux lines exert a force on the P-type semiconductor that separates the charge carriers (electrons and holes). As the holes

and electrons separate a potential difference is produced. The potential difference called the Hall voltage is directly proportional to the strength of the magnetic field passing through the P-type material. See Figure 3.2. The Hall Effect Principle was discovered by Edwin H. Hall in 1879 [19].

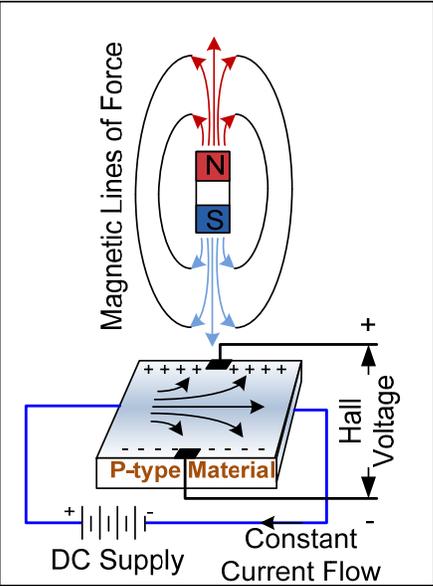


Figure 3.2 The Hall Effect Principle

The Hall Effect Switch is a small integrated circuit consisting of a Hall Effect sensor, amplifier, and a digital logic circuit to produce the solid state switching action (On / Off) in a chip by using a magnet's proximity. The digital logic converts the proportional voltage at a set point of magnetic strength to an "On" when the magnet is near and "Off" when the magnet is removed. A Hall Effect Switch requires from power source that can continuous deliver 6 to 10 mA continuously to power the chip and sensor. This requires an extra wire to be run from a power source compared to a reed switch. See Figure 3.3.

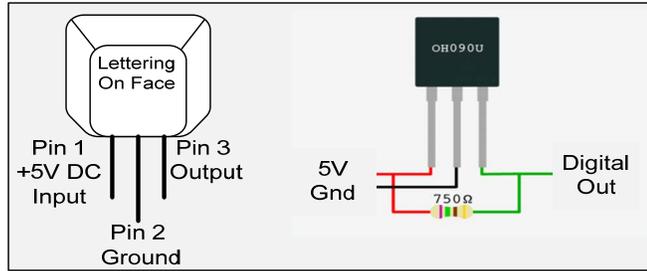


Figure 3.3 Hall Effect Switch

The Hall Effect Switch in this demonstration is used to count the number of revolutions made by a statistical water meter. As the water flows, it turns a paddle wheel in the meter. The shaft of the paddle wheel contains a magnet and rotates as the water flows. The amount of water that flows is proportional to the number of rotations of the magnet. By using a Hall Effect Switch, as shown in Figure 3.4, to count the rotations of the water wheel and by knowing how many tenths of a gallon is represented by one count, the amount of water flowing through the meter can be determined.

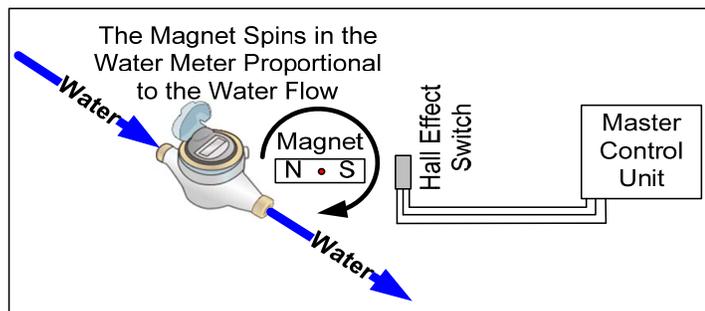


Figure 3.4 Pictorial of the Water Flow Sensor

The multiplication factor between the tenths of gallons of water and counts can be easily determined by running a known amount of water based on the calibrated meter dial on the

meter and counting the number of pulses. Next divide the counts by the tenths of gallons of water. This multiplication is used in the Master Controller Unit to get an accurate count for the amount of water that flows through the meter.

By sensing the water flow amount, the Master Control Unit can be programmed for leak detection. For example, the Master Control unit would only allow a small amount of water to flow during times no one was home or during normal sleeping hours. If the water flow was more than a few gallons, a command would be sent to an electric valve to shut off the water supply.

The existing installation had a high pressure faucet, manual water shut- off valve and a pressure regulator seen in Figure 3.5. Installation of the new water meter required unsoldering the existing plumbing. Next, the new plumbing had to be designed to fit the existing space and the necessary components were purchased. See the layout of the design, tools and parts in Figure 3.6.

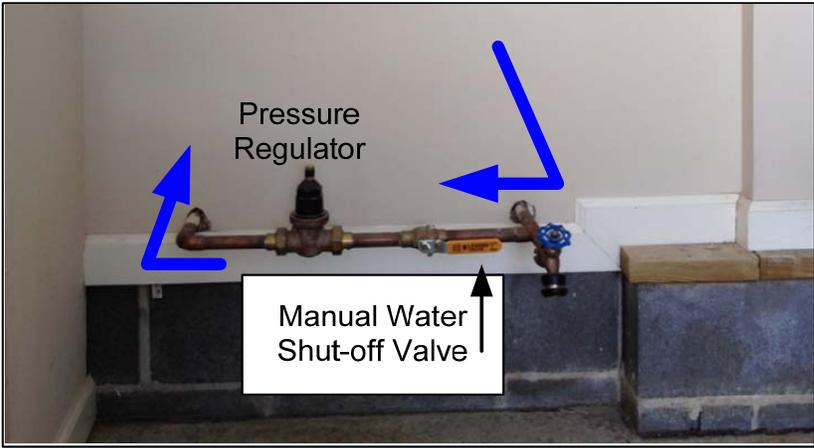


Figure 3.5 Water Piping Before the Installation



Figure 3.6 Items Needed for the Water Meter and Electric Shut-Off Valve Installation

A statistical water meter and an electrical shut-off valve were added. See Figure 3.7. At the same time the pressure regulator was replaced and a water pressure gauge was added. The water pressure gauge allowed the new pressure regulator to be set. The electric water shut-off valve is used to shut off the water in the case of a leak.

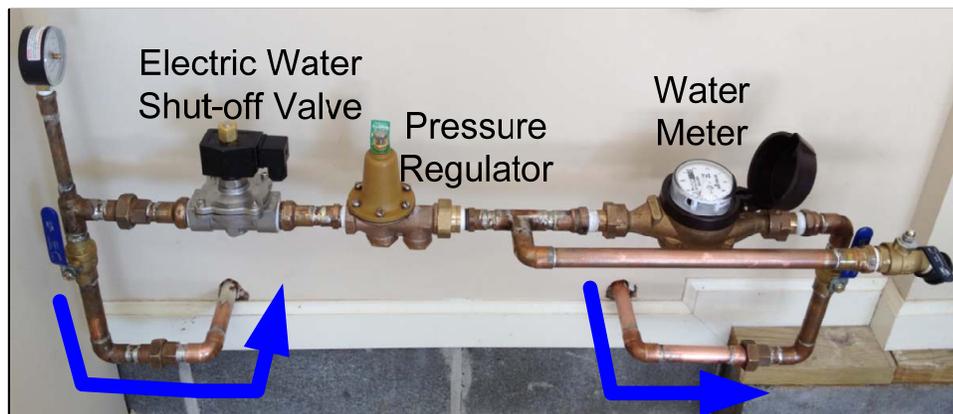


Figure 3.7 Installation of the Water Meter, Pressure Regulator, and Shut-off Valve

CHAPTER 4

WIRELESS SMART SENSORS

Fundamentals for Using ZigBee for Wireless Sensors

Zigbee is a low power spin off of Wi-Fi and is based on IEEE 802.15.4 - 2003. It was designed for WPAN which filled a need of a simple structure like those needed for wireless sensors and wireless sensor networks. The Zigbee Alliance developed Zigbee to be low cost, low power, energy efficient and cost effective. Unlike Bluetooth which is more complex and data rates in excess of 1 Mbps, Zigbee is slower at a maximum of 250kbps and lower cost. Zigbee has the defining features for networking large number of radios and for secure communications through the use of 128-bit cryptographic keys.

The XBee from Digi International was the brand name used for the Zigbee radios in this demonstration [20]. The XBees use a fully implemented protocol for a robust network in a WSN, that include addressing, acknowledgements, and retries to assist in the safe delivery of the data to the intended node.

The XBees in this demonstration operate in the 2.4 GHz Industrial, scientific and medical (ISM) radio band. They have two different power level models. The low-power (1 mW) model just called XBee and a high power (63 mW) model called XBee Pro. The low power model has an indoor range of 100 ft and an outdoor range of 200 ft. The high power model has an indoor range of 300 ft and an outdoor range of 1 mile.

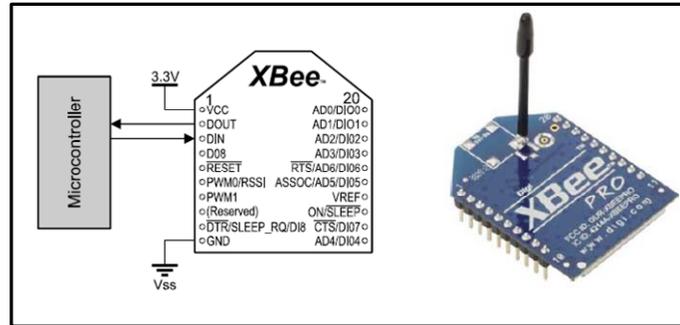


Figure 4.1 XBee Pro Module and Pin Outs

The XBee can exchange three types of data on the WSN. They are digital inputs and outputs, analog inputs with Pulse Width Modulation (PWM) outputs, and serial data (RS-232). Serial data was the one chosen in this demonstration because it offered the most flexibility. Serial data is a common way computers exchange data to an external peripheral device, but it usually involves a serial cable. The XBee allows the same serial data to be transferred wirelessly over several feet without a physical wire connection. See Figure 4.1. All is needed is an XBee on each end.

The sensor network is setup using the X-CTU configuration program by Digi International. In the X-CTU program, each XBee in the WSN must be set to the same channel and PAN identification number. This increases security, reduces interference and allows multiple WSNs to operate in the same physical area. Also, each XBee must have its own address which can be any hexadecimal address from 0000 to FFFE. FFFF is reserved for multicast.

The XBee can be set up to talk to each other by directly addressing another unit on the network or it can multicast. Broadcast is not used because each XBee must subscribe to the WSN Channel and have the same PAN in order to be able to send and receive data in the

WSN. When using less than 20 XBees, multicast will not overload the WSN and it allows interaction between sensors.

Garage Door Open / Close / Moving / Stopped Wireless Sensors

Although a garage door sensor has already been installed using a wired sensor, that sensor only has one point of reference. Once the garage door starts to open the reed switch opens up. There is no way to tell if the door is fully up, fully down, or somewhere in the middle. This special sensor is a Master machine type sensor that knows when the door is fully up, fully down, or in the middle. It also knows if the door is moving or stopped in the middle due to measuring the current being pulled by the motor.

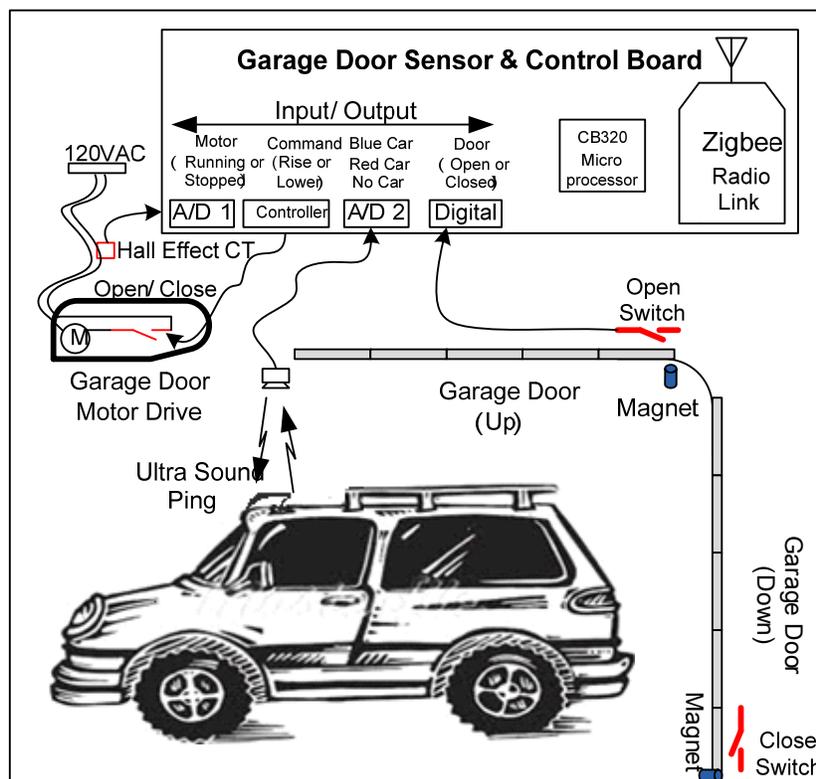


Figure 4.2 Garage Door Block Diagram for Sensors

The Garage Door Sensor and Control Board have two magnetic reed switches that sense when the door is fully open or fully closed. See Figure 4.2. A Hall Effect sensor sends a voltage proportional to the motor current to the analog to digital converter label as A/D 1. The motor current becomes digitized and enters into the microprocessor. The microprocessor looks at a set point and will send out the status of the door to the Master Control Unit.

Garage Door Range Wireless Sensors

Figure 4.3 also shows a Sonar Range Finder sensor made by Maxbotix, Model number MB1010 [21]. This sensor is very small (0.870" x 0.785" x 0.645) and its purpose is to measure the distance from itself to the nearest object. To accomplish this, the sensor sends out a 42 KHz burst. The onboard microprocessor starts timing and stops timing when the echo from the pulse is detected. This repeats 20 times per second. The sensor accuracy measures from 6 inches to 254 inches with 1 inch resolution. This sensor has three ways to interface. 1) Serial output, 2) Voltage output, and 3) Pulse width. The voltage output was used in the demonstration.



Figure 4.3 Maxbotix MB1010 Sonar Range Finder Sensor

A voltage from this sensor goes to the second analog to digital converter labeled as A/D 2 and is seen in Figure 4.2. Here the microprocessor compares the value to a look up table. If

the distance is greater than 8 feet, then the sensor is detecting the garage floor. In this case, the microprocessor sends out a status indicating “No Car” is in the garage. Two known vehicle distances were measured and programmed in to the microprocessor. If the value is equal to the known value for the “Toyota 4 Runner” the microprocessor sends out a status indicating the “4 Runner” is in the garage. The same process happens if the value is equal to the known value for the “Tacoma Truck”. But, if the sensor sees a value not equal to the above conditions and an object is in the garage, then the status of “Unknown” is sent.

Motion Detector Wireless Sensors

The motion detector unit used was made by Parallax Inc [22]. The PIR (Passive Infra Red) sensor is a pyroelectric unit that detects motion using a detector under a Fresnel Dome lens. Infrared (radiant heat) levels emitted by surrounding objects that hit the sensor is measured. The motion is sensed when the detector measures a sudden change in infrared energy striking the sensor. The infrared energy emitted by an object is a function of its temperature and its ability to emit infrared energy (emissivity). In simple terms, the moving object must have a different temperature than the background or else no motion will be detected. But when the object that is moving is different in temperature than the background, motion is detected and the internal logic causes the output to change from logic 0 to logic 1. After a short delay of inactivity, the logic returns to 0.

The Parallax PIR unit has a short range setting and a long range setting. The short range is effective up to 15 feet and the long range setting is effective up to 30 feet. As seen in Figure 4.4, the range is set by the jumper on the front (S to G or L to G). By increasing the sensitivity of the sensor in the long range setting, more false triggers may be observed. The sensor has an onboard LED to give visual feedback when motion is detected.

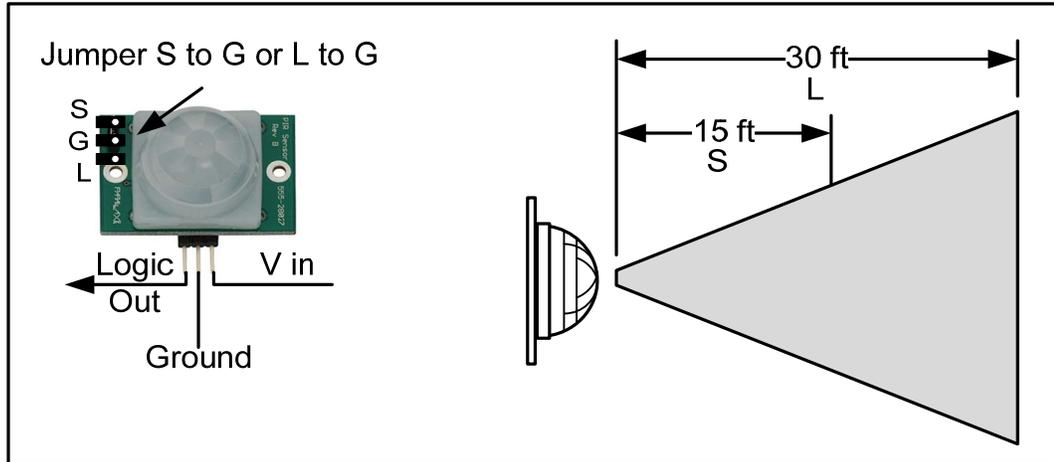


Figure 4.4 Parallax PIR Sensor (Revision B)

Wireless Gas Sensors

Gas Sensors can detect a wide variety of gases using various sensors. Most often they fall into two broad categories which are combustible and poisonous. Both categories are hazardous to human health and safety. These sensors are different from a smoke detector sensor and a smoke detector cannot detect either combustible or poisonous gases. However, certain gas sensors are also sensitive to smoke due to the unburned fuel that is present in the smoke.

Combustible or poisonous gasses may be found in various places but the most likely place is in a garage or utility room because they usually contain such items as a gas hot water heater, lawn mower, batteries, gas grill, etc. These items all contain one form or another of a fuel which when vaporized becomes a combustible gas. Many times gases used for fuel either have an odor or an odor that is added to alert someone of a leak. But, in an isolated area such as a detached garage, a small gas leak may go unnoticed until someone opens the door and flips on a light switch. The small arc created in the light switch when it is flipped on may ignite

the gas and cause an explosion. Therefore an array of various gas sensors is needed to warn of such a leak before it becomes a major problem.

Also, in the case of a gas hot water heater, the exhaust vent for the burned gas may become blocked which would prevent the carbon monoxide from escaping. Carbon Monoxide is a poisonous gas that is odorless and tasteless. Therefore it requires a special sensor to detect it.

Most detectors are for smoke and a few newer monitors detect smoke and carbon monoxide. A detector for multi types of combustible gases is needed to have the best security. The most common combustible gases include methane (natural gas), Liquid Propane Gas (LPG), butane (from a lighter), hydrogen (by produce of charging a battery), gasoline (vapors) and alcohol (vapors).

Figaro is a company that manufactures a wide variety of combustible gas sensors. See Table 4.1. [23] These sensors typically use tin oxide (SnO_2). The Tin Oxide sensitive layer, measuring electrode and heater element are formed into a crust and placed on a stainless steel net. Using a set voltage applied to the heater, the Tin oxide crystal is heated to a set high temperature. The oxygen is absorbed from the atmosphere on to the surface of the crystal and causes a negative charge to form thus causing the resistance to increase across the crystal. In the presence of a deoxidizing gas, the negative charge dissipates and the resistance is reduces in proportion to the gas concentration. Each sensor type has some sensitivity to all combustible gases but typically one gas dominates because the Tin Oxide crystal and the heater voltage are optimized for a particular deoxidizing gas. The MQ - 3 sensors are also sensitive to Smoke. The sensor designs heater voltages typically range from 1.4 to 5 volts but some sensors not listed go as high as 6 volts. See Tab 4.1 for the sensor sensitivity details.

Table 4.1 Figaro Gas Sensors

Figaro Sensor	High Sensitivity	Heater Voltage
MQ - 2	Methane, Butane, Propane, Smoke	5V
MQ - 3	Alcohol, Ethanol, Smoke	5V
MQ - 4	Methane	5V
MQ - 5	Natural Gas, Propane	5V
MQ - 6	Propane, Butane	5V
MQ - 7	Carbon Monoxide	5V and 1.4 alternating
MQ - 8	Hydrogen	5V
MQ - 9	Carbon Monoxide	5V and 1.4 alternating

All of the MQ series sensors are similar in physical appearance. Their foot print is a little smaller than a quarter. See Figure 4.5. The temperature set point is achieved by applying 5 volts to the heater element of the sensor. The MQ - 7 and MQ - 9 also have a low temperature set point (1.4 volts).



Figure 4.5 Typical MQ Series Gas Sensors

The Carbon Monoxide sensor (MQ-7 and MQ-9) circuit is a little more complex because it takes a reading at the low temperature set point to detect the Carbon Monoxide then raises

the temperature to the higher set point. The higher temperature resets the sensor by cleaning the gases that were absorbed at the low temperature.

The cycle pattern is 60 seconds at 5 volts then 90 seconds at 1.4 volts. In order to use a microprocessor a voltage divider circuit must be used to switch the voltage from 5 volts to 1.4 volts. This can be accomplished by triggering a transistor. When a logic 0 (0 Volts) is applied to the heater control it turns on the transistor. This allows the transistor to pass the 5 volts to the heater element. When a logic 1 (5 volts) is applied to the heater control point, the transistor turns off and voltage supplied to the heater drops to 1.4 volts. See the left schematic in Figure 4.6.

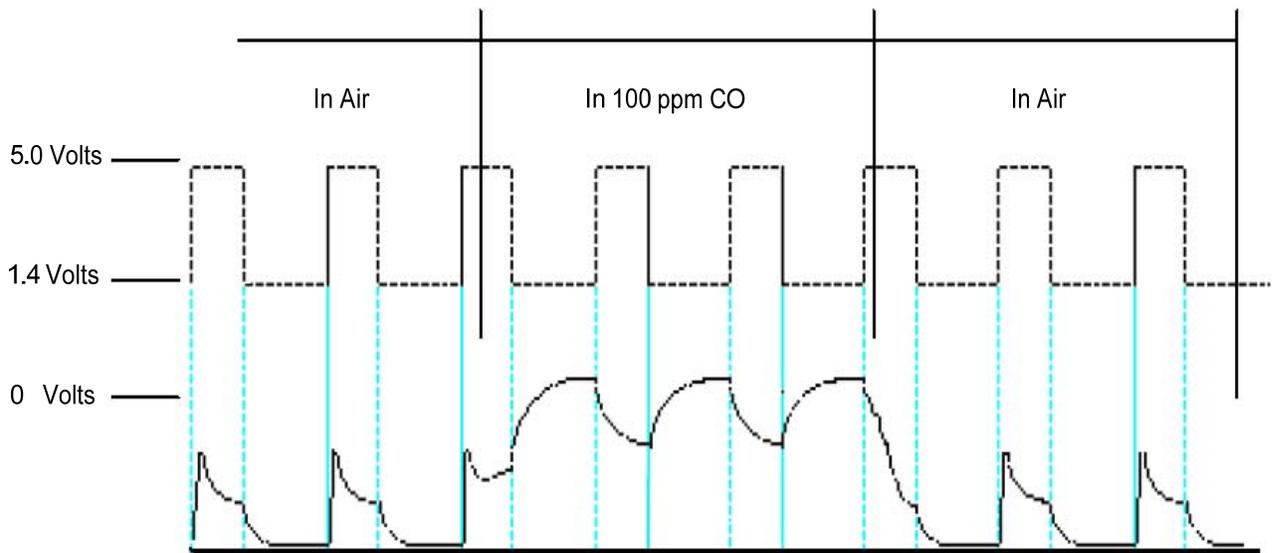


Figure 4.6 Sensor Output as Heater Voltage Varies and Gas Concentration Varies

The other sensors (Smoke/Gas Combination MQ-2, Alcohol MQ-3, Methane MQ-4, Methane/Propane MQ-5, Propane MQ-6 and Hydrogen MQ-8) do not require a cycling of the heater element. Only a constant 5 volts is needed to power the heater. The constant voltage

keeps the heater from fluctuating and helps prevent false triggering. See the right schematic in Figure 4.7.

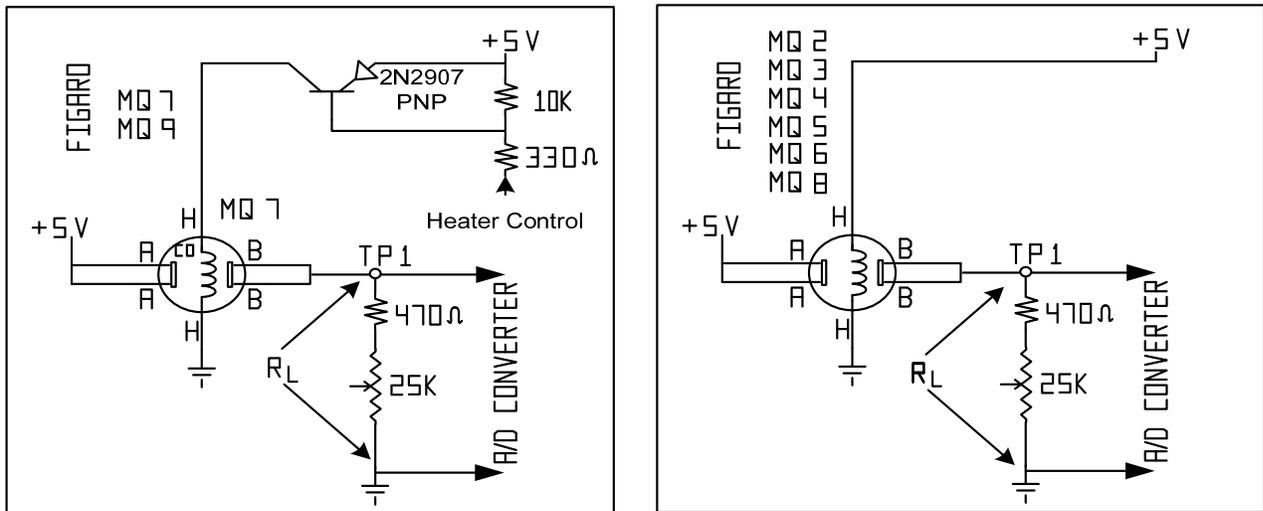


Figure 4.7 Circuit Diagram for MQ - X Figaro Gas Sensors

The voltage output is a typical voltage divider formula Figure 4.8. This voltage feeds a A/D converter on a microprocessor.

$$V_{\text{out}} = 5 \text{ volts} \frac{R_L}{(R_L + R_{\text{sensor}})}$$

Figure 4.8 Calculating the Voltage Output from a Gas Sensor

Microprocessors to Make Sensors Smart

The microprocessor ties digital and analog data together to turn raw data into smart data. This project uses the low cost CB320 and CB380 microprocessors / PLCs from Comfile Technology for this task [24].

The CB320 is a microprocessor and PLC on a 24 pin dual inline pin (DIP). See Figure 4.9. The microprocessor and PLC function in parallel while still able to exchange data with each other. The CB320 has 22 general input/output (I/O) lines for digital logic. These pins can be changed from general I/O to other configurable features such as: 8 Channels for A/D converter (10 bits resolution each), 4 lines for interrupts, 2 high speed counters or 1 serial port. This chip draws only 40 mA and can be powered from a power supply ranging from 5 volts to 12 volts.



Figure 4.9 CB320 Microprocessor and PLC on a Chip

The Garage Door Sensor and Control Board printed circuit board (PCB) was designed and made for garage door 1 and 2. See Figure 4.10. The image is from the PCB layout. Before etching, the image must be mirrored and transferred to a blank copper board. See Figure 4.10. A CB320 was programmed to use two digital inputs from the two reed switches for open and close status, one digital output for raising and lowering the door by remote, one analog input to monitor the motor current of the garage door drive motor and another analog

input to measure the distance from the sonar detector to the nearest object. The CB320 also communicated through the serial port to the Zigbee radio back to the Master Controller Unit. See the block diagram in Figure 4.11.

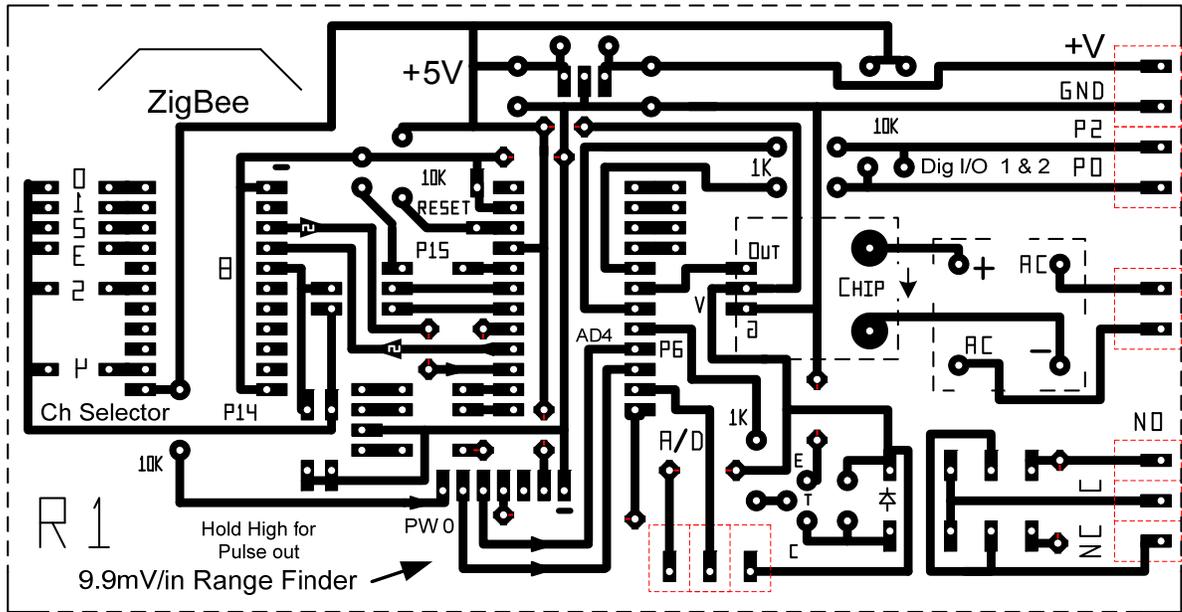


Figure 4.10 Garage Door Sensor & Control Board PCB

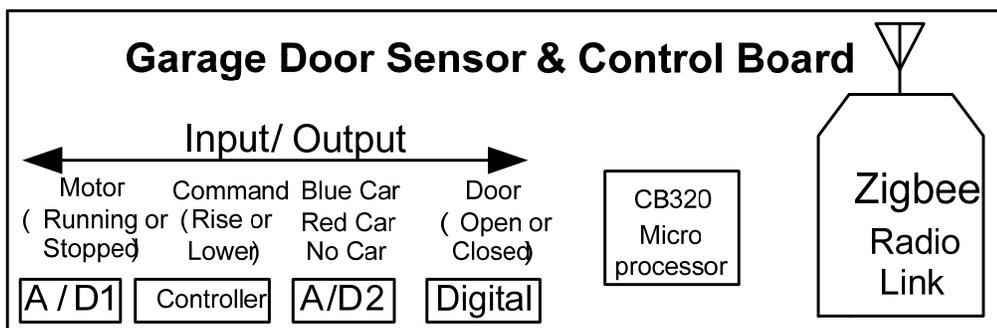


Figure 4.11 Garage Door Sensor and Control Board Block Diagram

The communication system between the Garage Door Sensor & Control Board and the Master Control Unit uses multicast. A protocol was defined as using a different ASCII character for each function or event. Table 4.2 shows the ASCII character and its function.

Table 4.2 Protocol for Garage Door Sensor & Control Board

Wireless ZigBee		Xbee code
Garage Door 1 UP	00 XX	a
Garage Door 1 Moving	01 XX	b
Garage Door 1 Stopped	10 XX	c
Garage Door 1 DOWN	11 XX	d
Garage 1 No Car	XX 00	e
Garage 1 Unknown Car	XX 01	f
Garage 1 Red Car	XX 10	g
Garage 1 Blue Car (4 Runner)	XX 11	h
Garage Door 2 UP	00 XX	i
Garage Door 2 Moving	01 XX	j
Garage Door 2 Stopped	10 XX	k
Garage Door 2 DOWN	11 XX	l
Garage 2 No Car	XX 00	m
Garage 2 Unknown Car	XX 01	n
Garage 2 Red Car	XX 10	o
Garage 2 Blue Car (Truck)	XX 11	p
Sends a UP Cmd to Garage Door 1		q
Sends a DN Cmd to Garage Door 1		r
Sends a UP Cmd to Garage Door 2		s
Sends a DN Cmd to Garage Door 2		t

The Motion Detector Sensor also uses the CB320 to gather the status from the PIR motion detector. A microprocessor helps coordinate the timing to minimize false triggers. See Figure 4.12. Using the same approach, a third party detector of any type can be placed in the system. This system has been setup for four motion detectors and four third party detectors.

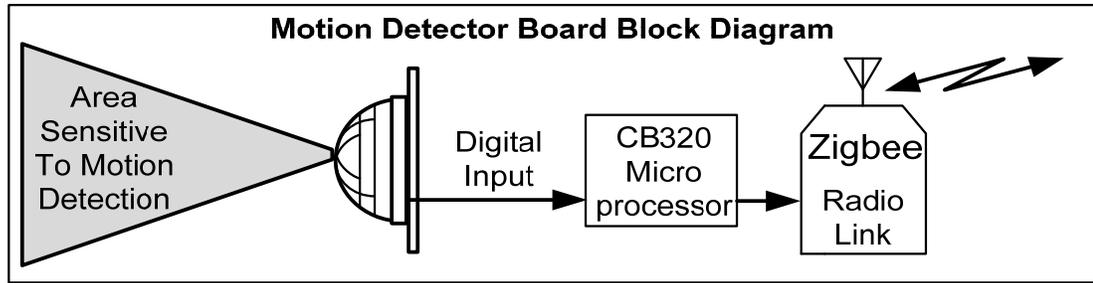


Figure 4.12 Motion Detector Board Block Diagram

The same protocol was used for the motion detector sensors as was used by the previous sensors. The first four are custom designed motion detectors and the last four are for adding third party sensors. This demonstration used Voice Alert motion detectors by System 6. Table 4.3 shows the ASCII characters and its function for the motion detectors.

Table 4.3 Protocol for Motion Detectors

Wireless ZigBee	Xbee code
Motion Detector Side Door	u
Motion Detector Front Door	v
Motion Detector Back Door	w
Motion Detector Driveway	x
Voice Alert (Motion Detector 1)	y
Voice Alert (Motion Detector 2)	z
Voice Alert (Motion Detector 3)	A
Voice Alert (Mail Box)	B

The Gas Detector Sensors also uses the CB320. The each gas sensor voltage output varies according to the gas concentration it observes. The voltages are feed into the A/D ports of the CB320 where they are compared to set values. If a value exceeds its set point, the

corresponding Xbee code is sent out the serial port. This code is transmitted by the Xbee radio to the Wireless Receiver Board. See Figure 4.13.

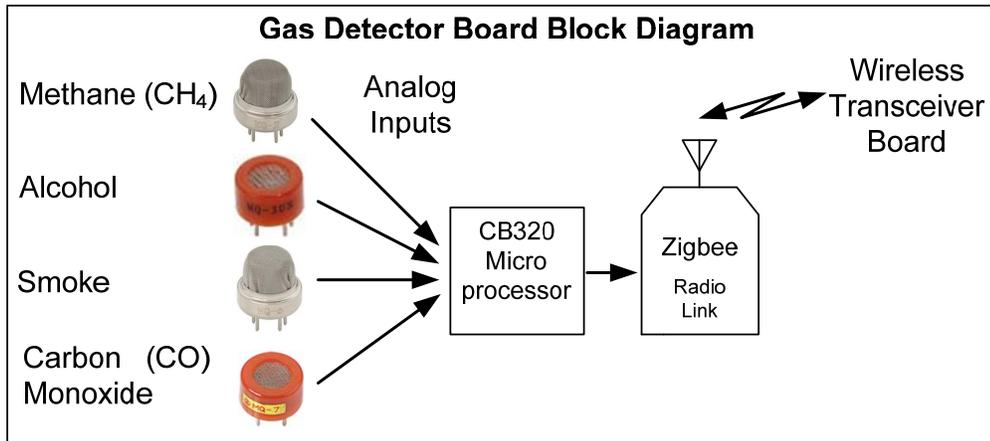


Figure 4.13 Gas Detector Board Block Diagram

The same protocol was used for the gas sensors as was used for the motion detector sensors. This demonstration used Methane (CH₄), Carbon Monoxide (CO), Smoke, and Alcohol sensors. Future sensors can be added. Table 4.4 shows the ASCII characters and its functions for the gas sensors.

Table 4.4 Protocol for Gas Detectors

Wireless ZigBee	Xbee code
Methane (CH4)	C
Carbon Monoxide (CO)	D
Smoke	E
Alcohol	F
Smoke/Gas Detector 5	G
Smoke/Gas Detector 6	H
Smoke/Gas Detector 7	I
Smoke/Gas Detector 8	J

A Microprocessor to Aggregate the Wireless Data

The CB380 is a microprocessor and PLC like the CB320. Due to the narrow pin spacing of the chip, a Cubloc header board was used. See Figure 4.14. The microprocessor and PLC function in parallel while still able to exchange data with each other. The CB380 has 49 general input/output (I/O) lines for digital logic. These pins can be changed from general I/O to other configurable features such as: 8 Channels for A/D converter (10 bits resolution each), 4 lines for interrupts, 2 high speed counters and 1 serial port. The header board can accept from 9 to 16 volts. The voltage passes through an onboard regulator to drop the voltage down to 5 volts for the CB380.

The data is sent and received by the XBee radio located on the Wireless Transceiver Board. See Figure 4.15. The XBee radio's serial port is tied to serial port on the header board via a MAX233 level convertor.

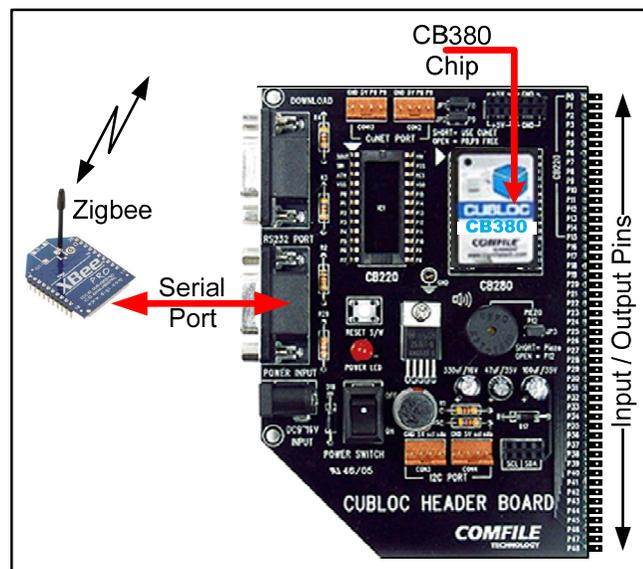


Figure 4.14 CB380 Microprocessor and PLC on a Cubloc Header Board

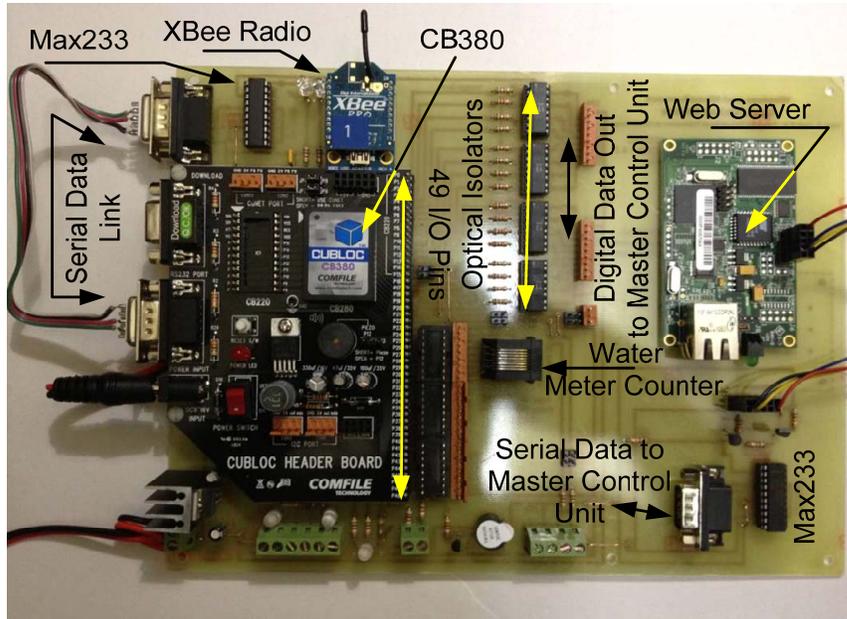


Figure 4.15 Wireless Transceiver Board

The Wireless Receiver Board receives the input from the wireless sensors and processes the data. Once the data is processed it is converted to a status of a logic 1 or logic 0 and placed on the output pins for the CB380 header board. There are 16 channels or status points. Each of the 16 output channels are conditioned through optical isolator and sent to the Master Control Unit as shown in Figure 4.16.

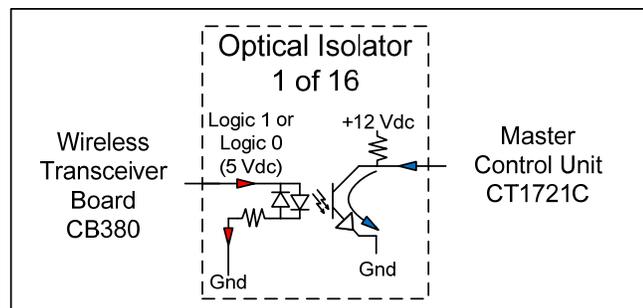


Figure 4.16 Wireless Transceiver Board to Master Control Unit Interface

CHAPTER 5
MAIN CONTROL UNIT

Cubloc CT1721C PLC / Microprocessor

The Main Control Unit is the HMI and it is built on the Cubloc CT1721C platform [24]. This unit is low cost and can be programmed with custom graphics along with a touch screen input. This makes this unit a practical choice. The CT1721C features dual Atmega128 processors. One processor is dedicated to the graphics and the touch screen input while the second processor is dedicated to user's program.



Figure 5.1 Cubloc CT1721C

Wired Inputs and Outputs to the MCU

The MCU senses the slave machines which are the door and window sensor machines. A common 12VDC source flows from the terminal block through the common voltage wire to the input on the CT 1721C MCU. The MCU has 32 optical isolated inputs and furnishes 16 of these for individual paths to each sensor point. These paths go to the door or window reed switches. Each sensor can be either open or closed. The common end of each sensor point is tied to ground to complete the loop. When a sensor is open or the loop is broken, current ceases to flow and the LED in the optical isolator of the MCU turns off. This indicated a change in status in the MCU. The circuit can be followed in Figure 5.2.

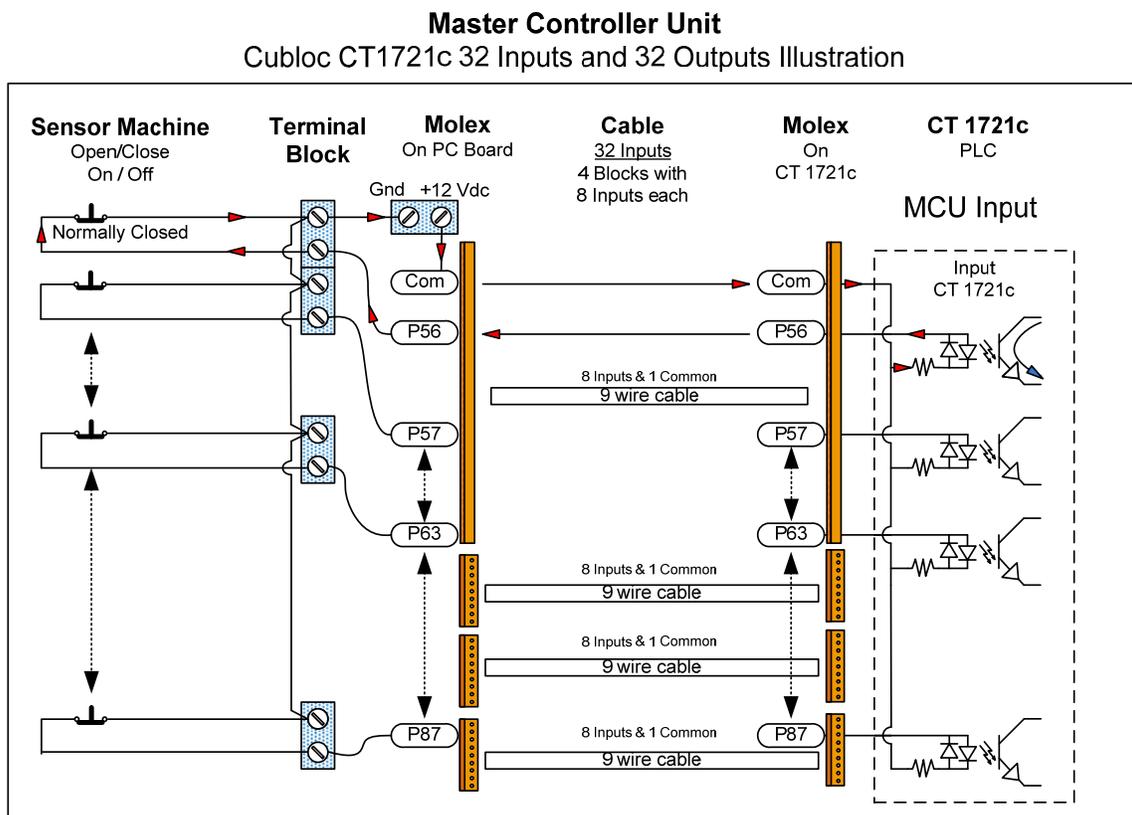


Figure 5.2 Wired Sensor Machine to Master Control Unit Interface

The MCU receives 16 inputs P56 through P71. The inputs feed the PLC ladder logic. The PLC allows for virtual inputs or soft inputs. The soft input is a screen touch and is used to be in parallel with the real sensor. This configuration will allow for a sensor to be bypassed or in other words taken out of service. Figure 5.3 show the input for wire sensor machine. P56 can be bypassed using a virtual input M156 controlled by a press of on the HMI on the Side Door indicator.

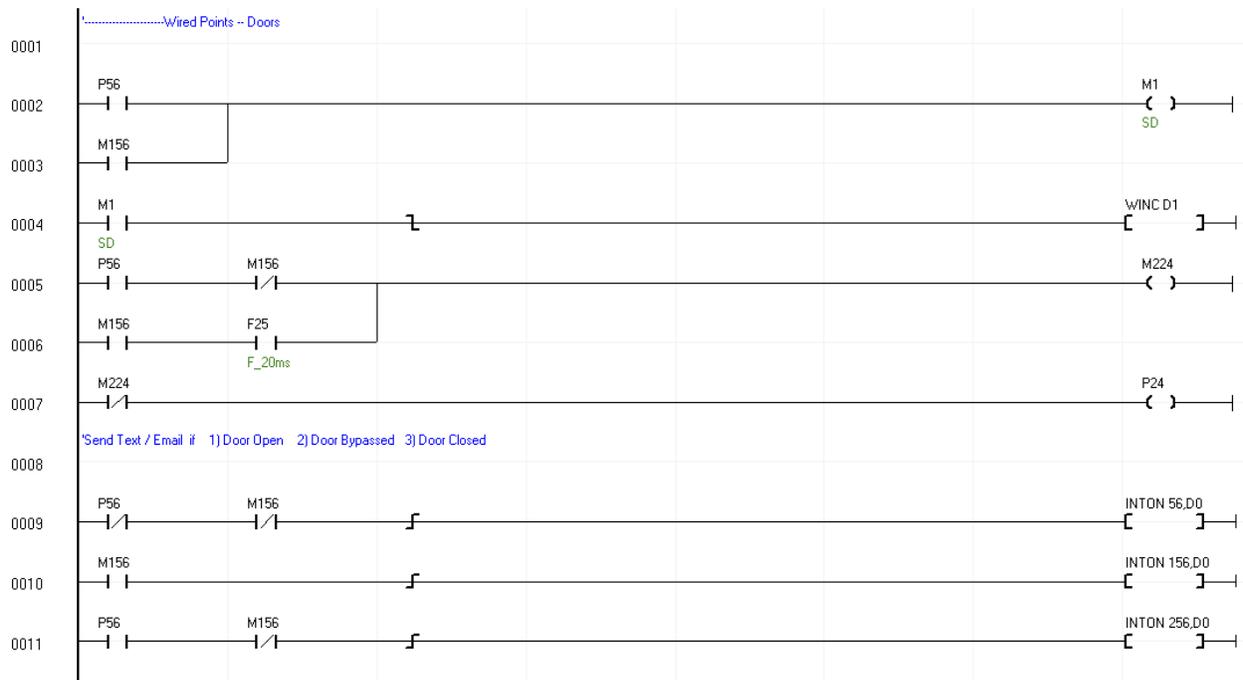


Figure 5.3 PLC Ladder Logic for One Wired Sensor Machine Input

If either P56 or M156 is closed the virtual contact M1 is closed. Each time M1 transitions from Closed to Open the variable *D1* is incremented. This keeps count of the number of times of times the door has been opened. If M156 is in the normal state (not bypassed) and P56 is closed (door closed), the logic keeps the output P24 off.

The point P24 is a real world output that goes to an input of a CB320 microprocessor chip. Each CB320 microprocessor chip has 4 inputs and drives 4 LEDs. These are special LEDs. These LEDs are made up of three LEDs in one housing (Red LED, Green LED, and Blue LED). There are 4 CB320 microprocessor chips with 4 inputs each. This gives a way to monitor 16 status points with LEDs. Each LED can be any combination of Red, Green, and/or Blue. Blue indicates the sensor door has not been open since the last reset. Red indicates the door is open. Yellow (Green and Red) indicates the door has been opened but is now closed. If the status point is closed and opens for less than 0.5 seconds then closes, the point will reset. Flashing Purple (Blue and Red) indicates the point is bypassed. Figure 5.4 shows the layout how various colors are related to the door or window status. Figure 5.5 shows the PLC Logic.

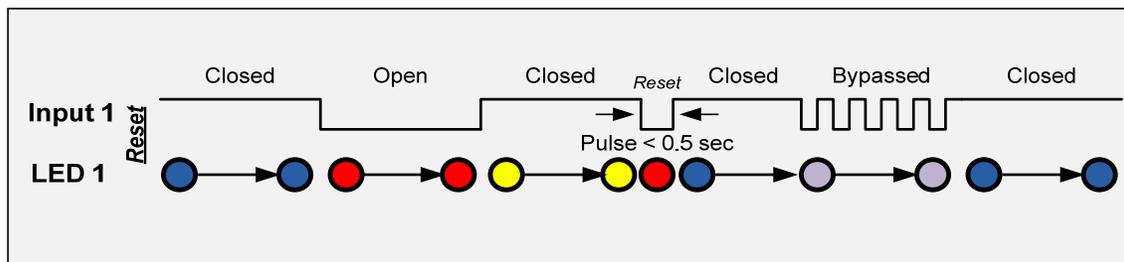


Figure 5.4 LED Color Based on Status of the Door or Window

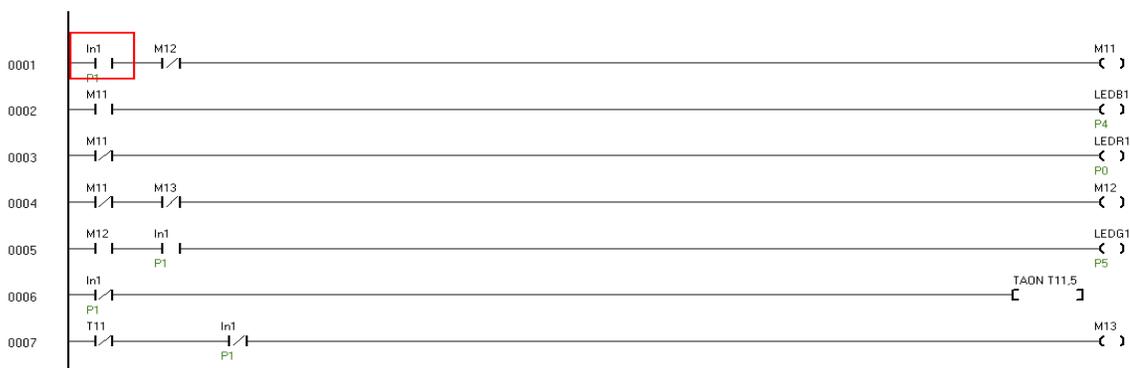


Figure 5.5 PLC Logic to Drive One of the 16 LEDs

Wireless Inputs and Outputs to the MCU

For the wireless sensors, most of the hardware complexity is in the remote sensor because it is a master machine with two onboard processors. One processor drives the ping distance sensor and Cubloc CB320 processor drives the analog to digital processor that interprets the distance and provides the communication protocol for the XBee radio. The wireless master machine sensor communicates with the Wireless Input Board which connects to the MCU. On the MCU, the PLC ladder logic is much simpler since there are no bypass points or status LEDs to drive, but these points require more complex calculations which is performed in the coding of the MCU. The inputs range is from P72 through P87. The outputs range is from M17 through M32. These are virtual outputs and drive the HMI, Web server, and the SMS server. See the PLC ladder logic in Figure 5.6 for one of the two garage parking slots and the more complex processor code in Appendix A.



Figure 5.6 PLC Logic for Car in the Garage Status

The wireless input for the motion detector and gas detectors are also simple for the PLC ladder logic but the complexity is in the sensor and the processing code. Figure 5.7 shows the Ladder logic for one Motion Detector.

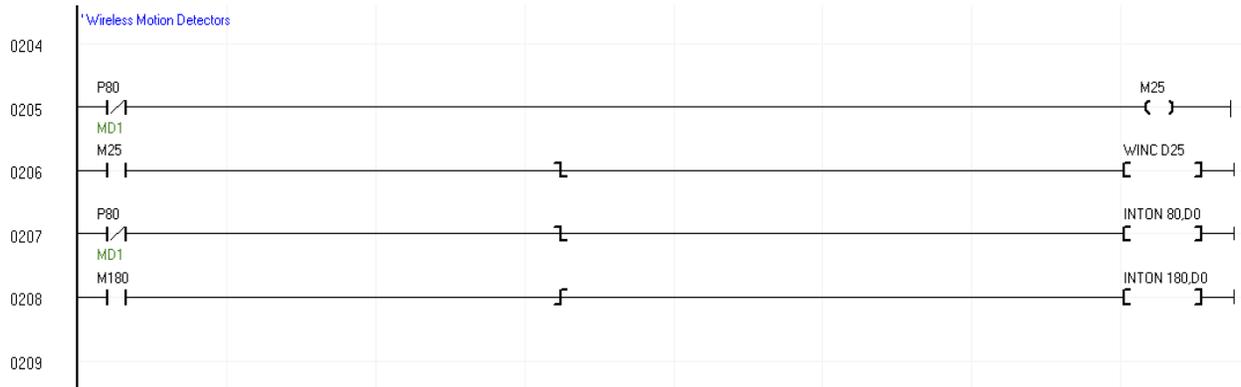


Figure 5.7 PLC Logic for Wireless Motion Detectors

The MCU which contains the HMI is mounted in an enclosure that also contains the wired input board and the wireless input board. See Figure 5.8. These three sections comprise the central part to the super machine that was built for this demonstration.

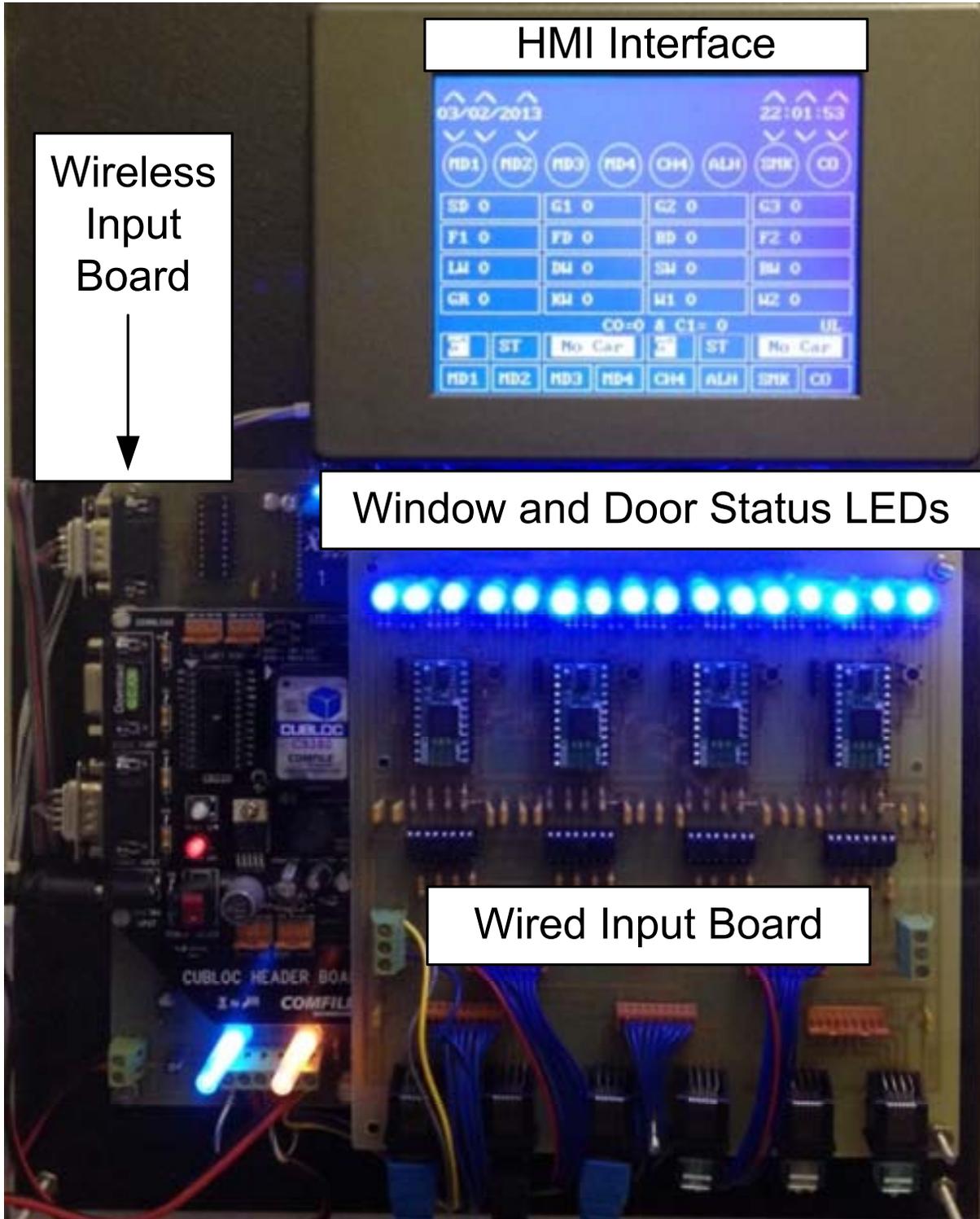


Figure 5.8 The Master Control Unit

CHAPTER 6

HMI, WEB SERVER AND TEXT MESSAGING

Output to the User

Once all of the data is received and digested by the MCU, the data needs to be communicated by an interface readily available to the user in such a way that an action can be taken if needed. The data in this demonstration is presented to the user by the local HMI and by two remote methods which are Web Page and SMS messaging. Security is applied to the SMS messaging by programming the PLC section of the HMI with the SMS address of the intended receiver or receivers. This is done through a local download port that is not accessible via the Web. The Web Server has an option of a requiring a password to access the web display page if more security is required.

HMI Interface

The HMI interface takes place on the Cubloc CT1721c. The top line of the HMI is reserved for the date and time from the real time clock (RTC). The 16 door and window points are given in a 4x4 matrix. Each box in the matrix has a two letter representation of the point and the number of times the point has been opened as seen in Figure 6.1. If the status of the point is open the background is white and if the status of the point is closed then the background is blue. If the user touches the box, the box toggles a virtual input to bypass the sensor point and

displays "****" in the box. If the user touches it again, the point returns to normal and resets the point. This also resets the counter to "0".

Below 4x4 matrix is the garage points statuses for the two garage bays that are normally used for parking. The left three blocks indicate the status of garage bay 1 and the right three blocks indicates the status of garage bay 2. Looking at the three blocks for each bay, the left most block indicates "G^" when the door is moving upward and "Gv" when the door is moving downward. If the door is moving the background is white and the next block indicates "Mv" for moving. If the door is stopped, the background is blue and the middle block indicates "ST" for stopped. The third block tells if a vehicle is in the bay and which vehicle it is. If no vehicle is in bay 1, the block indicates "No Car" and the block has a white background. If the 4 Runner is in bay 1 the third block says "4 Runner". The background is blue since this is the normal bay for the 4 Runner. If the truck is in bay 1, the block says "Truck" but the background is white which indicates this is not the normal position for the truck. The reverse is true for bay 2 since it is the normal bay for the truck. If another vehicle is in bay 1 or bay 2, the indicator will say "Unknown" for that block.

The motion detector points are along the bottom. There are indicators for 8 detectors. If no activity, the detector shows the detector's name. For example "MD1" would be in block 1 for motion detector 1. If motion was seen, the counter would increment by 1 every time motion was detected. There is a minimum time of 20 seconds between detection counts. This gives any motion in the zone time to move through the zone before being detected again. The motion detection points can be used for other points of interest. One example is the mail box and knowing if it has been opened. Figure 6.1 shows the interface.



Figure 6.1 The HMI Touch Screen Interface

Web Server Interface

The Web Server Interface is based on the Netburner SB70-100CR [25] hardware which is running a software embedded web server. The web server allows communication with a host microprocessor through a serial port. The microprocessor can read or write 100 variables through the serial communication port to allow for dynamic web page updates. The onboard 256K of memory allows for many pages of HTML code to display point statuses and web links.

Variables 01 - 16 are used to store the status of the doors and windows. Variables 51 - 66 are used to store the count for the number of openings of doors and windows. Variables 25 - 32 are used to store the status of the motion detectors. Variables 75 - 82 are used to store the count for the number of motions from the motion detectors. The status values are shown in colors that are the same format as the LED discussed earlier.

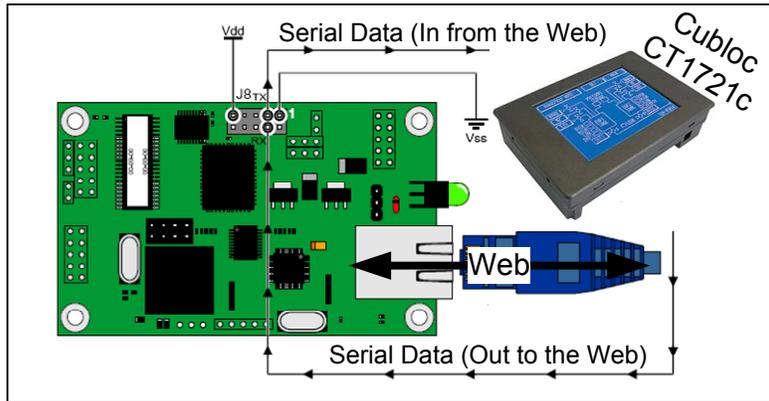


Figure 6.2 The Web Server Hardware Interface

ALARM -- Garage Door 1 Closed 1 02/13 09:48:37 PM

Doors and Windows	Motions Detectors
1. <input type="checkbox"/> 0 - Side Door	1. <input type="checkbox"/> 0 - Driveway
2. <input checked="" type="checkbox"/> 1 @ 09:48:37 - Garage Door 1	2. <input type="checkbox"/> 0 - Front Door
3. <input type="checkbox"/> 0 - Garage Door 2	3. <input type="checkbox"/> 0 - Side Door
4. <input type="checkbox"/> 0 - Garage Door 3	4. <input type="checkbox"/> 0 - Back Porch
5. <input type="checkbox"/> 0 - Future Door 1	5. <input type="checkbox"/> 0 - Voilce Alert 1
6. <input type="checkbox"/> 0 - Front Door	6. <input type="checkbox"/> 0 - Voilce Alert 2
7. <input type="checkbox"/> 0 - Back Door	7. <input type="checkbox"/> 0 - Voilce Alert 3
8. <input type="checkbox"/> 0 - Future Door 2	8. <input type="checkbox"/> 0 - Mail Box
9. <input type="checkbox"/> 0 - Laundry Room Window	9. 0 - Gallons of Water
10. <input type="checkbox"/> 0 - Dining Room Window	10. 0 - Inches of Rain
11. <input type="checkbox"/> 0 - Study Window	• Local Modify Variables
12. <input type="checkbox"/> 0 - Bed Room Window	• Modify Variables
13. <input type="checkbox"/> 0 - Great Room Window	• Local TMart Capture
14. <input type="checkbox"/> 0 - Kitchen Window	• Local TMart Cam
15. <input type="checkbox"/> 0 - Future Window 1	• Remote TMart Cam
16. <input type="checkbox"/> 0 - Future Window 2	• Reset Y/N ? <input type="text"/> <input type="button" value="Accept"/>

Figure 6.3 The Web Server Web Page Display

SMS Messaging Interface

The SMS Messaging Interface is also based on the Netburner SB70-100CR [24] hardware which is running a software mail server and communicates with a host microprocessor through a serial port. SMS messages can be sent using a mail server. The Email address has the following format: '10 digit phone number' @ 'cell phone company gateway suffix'. For example to send to a person at ATT a SMS Message with the phone number "(423)555-5555" use the following "4235555555@mms.att.com" as the email address. If the cell phone carrier is Verizon then use "4235555555@vtext.com" as the email address. All carriers provide this option for SMS and text messaging [26]. Figure 6.4 shows an example how to instruct a microprocessor send an Email message. Figure 6.5 shows the SMS output on an iPhone.

```
Putstr 1, "!NBOWET:4235551234@mms.att.net", 0 'TO Email Address
Delay Pause01
Putstr 1, "!NBOWEF:Alert@Alarm.net", 0 'FROM Email Address
Delay Pause01
Putstr 1, "!NBOWES:Reset ",DDis," ",TDis, 0 'Subject Line
Delay Pause01
Putstr 1, "!NBOWEC:", "Subject Line Here", 0 'Content
Delay Pause01
Putstr 1, "!NBOWEV:smtp.gmail.net", 0 'SMTP for Comcast
Delay Pause01
Putstr 1, "!NBOWEU:username@gmail.com", 0 'Login Email
Delay Pause01
'Putstr 1, "!NBOWEP:W11", 0 'Login Password
'Delay Pause01
'Putstr 1, "!NBOWEA:S", 0 'Turn Authentication On (Optional)
'Delay Pause01
'Putstr 1, "!NBOWEW:465", 0 'Turn Authentication On (Optional)
'Delay Pause01
Putstr 1, "!NBOSM" 'The command to send a email
```

Figure 6.4 Example of Code to Send an Email Message

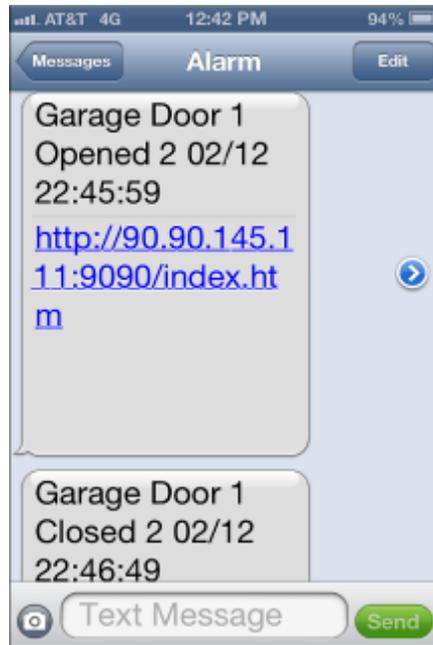


Figure 6.5 The Display of a iPhone Receiving a SMS

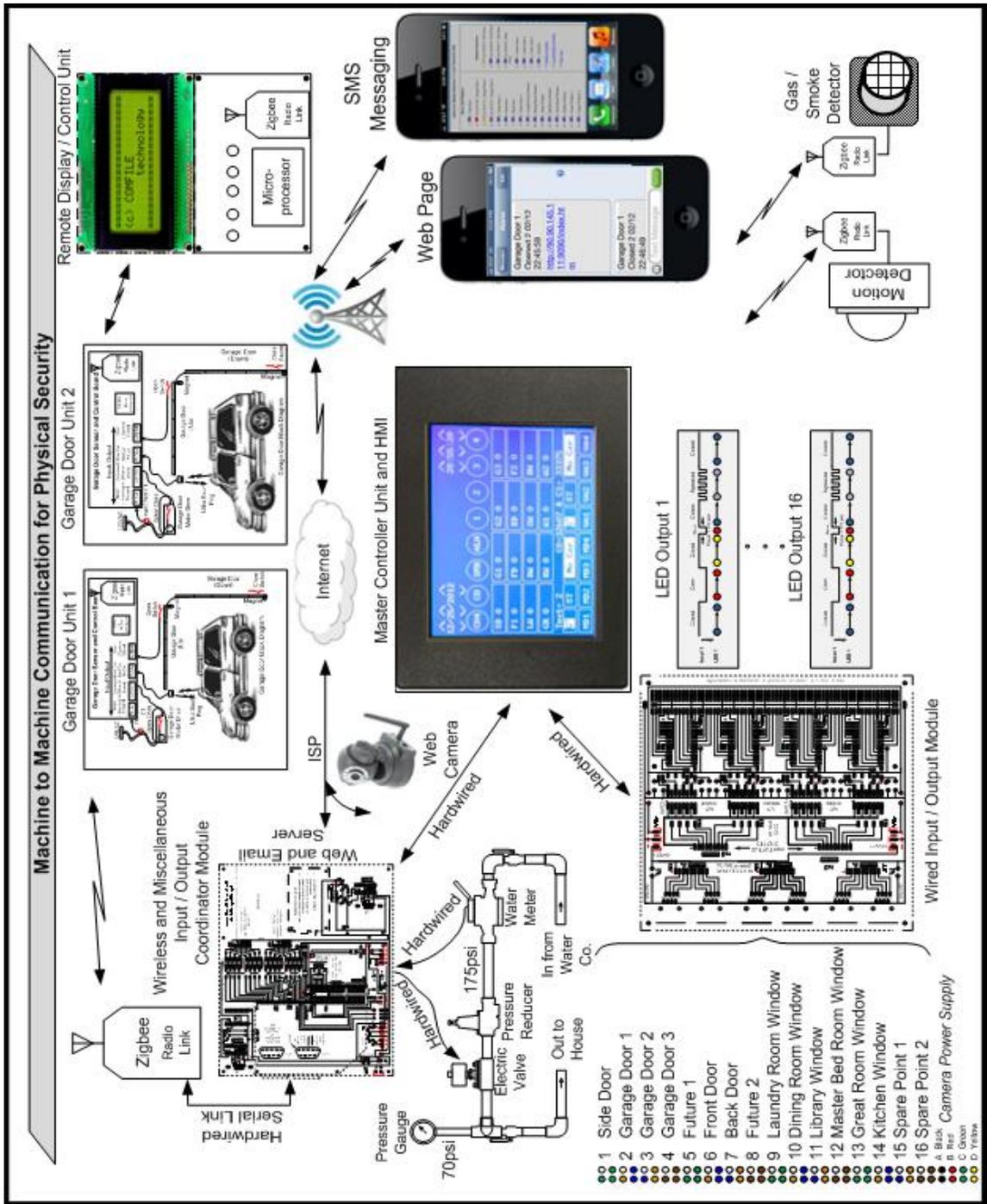


Figure 6.6 The Overall View for M2M Communications for Physical Security

CHAPTER 7

CONCLUSION

M2M for Physical Security

Physical quantities were measured with an array of sensors. Communication between local components were handled by hardwire connections and XBee radios. The system has made allowance for addition sensors from a third party such as security cameras. All of the data culminates into a PLC driving the HMI for local display and control. The real key is the communication of the processed data that can be received anywhere in the world via the internet and SMS messaging events that can be pushed to the users cell phone alerting the user of a recent event. All of this is done through M2M communications which eliminates the cost of a third party monitoring service. The overall big picture is shown in Figure 7.1

Summary

This thesis focused on stitching the four core principles of M2M communication of Data Collection, Data Transmission, Data Assessment, and Action Generation together with an array of real world physical machines. This required writing using the latest ZigBee radio hardware and writing hundreds of lines of code for processing the data. The overall result was the development and building of a super machine that gives the user a better and more cost effective method to provide physical security. Using the frame work of the four core principles, other systems can be upgraded to a M2M communication system using capital investment money. This demonstration showed an ROI in less than 30 months.

REFERENCES

- [1] EnerNOC Company, (2008, October 19). "What is M2M Communications". Web: <http://www.m2mcomm.com/about/what-is-m2m/index.html>
- [2] Gislason, Drew, (2010, July 23), "ZigBee applications - Part 3: ZigBee PANs". Web: <http://eetimes.com/design/embedded-internet-design/4204872/ZigBee-applications---Part-3--ZigBee-PANs>
- [3] Frenzel, Lou, (2012, February 23), "Wireless Module Brings Wi-Fi to M2M". Web:<http://electronicdesign.com/communications/wireless-module-brings-wi-fi-m2m>
- [4] Paxol, Steve, (2011, March 22), "M2M and the promise of LTE/4G". Web:<http://www.networkworld.com/news/tech/2011/032211-m2m-4g-lte.html?page=2>
- [5] Dan-Ari, Kfir (2012, March 8). "ROI Potential of M2M Services Rises with Sector Specific OSS". Web: <http://www.screenplaysmag.com/2012/03/12/>
- [6] Hilton, Steve, (2012, December 7). "M2M Tracking and Monitoring Solutions: An Industry Benchmark". Web: <http://www.analysismason.com/About-Us/News/Insight/M2M-tracking-and-monitoring-Dec2012/>
- [7] Kiani, Naveed, (2012, November 14). "Machine to Machine Communication - Not a Fiction anymore". Web: <http://teletimesinternational.com/articles/11269/machine-to-machine-communication-not-a-fiction-anymore?lang=fa, 12/27/2012>
- [8] Wagner, Robert, (date), "History of GM's OnStar". Web: http://www.ehow.com/info_11415251_history-gms-onstar.html
- [9] Patterson, Ben. (2005,February 22;updated 2008,March 4). "3G Cell Phone Service". Web:http://reviews.cnet.com/4520-3504_7-5664933-1.html
- [10] Krazit, Tom, (2008, July 7), "iPhone 3G Launch Day is Friday". Web: http://news.cnet.com/8301-13579_3-9983810-37.html
- [11] Heile, Bob. (2012, April 26), "ZigBee Light Link". Web: http://www.zigbee.org/portals/0/documents/events/2012_04_26_ZLL-Green%20Lighting-Heile.pdf
- [12] Ergen, Sinem Coleri, (2004, September 10), "ZigBee/IEEE 802.15.4 Summary". Web:<http://pages.cs.wisc.edu/~suman/courses/838/papers/zigbee.pdf>

- [13] M2M World News, (2012, May 17). "90 Million Homes Worldwide Will Employ Home Automations Systems by 2017". Web: <http://m2mworldnews.com/2012/05/17/>
- [14] Radiocommunications Study Group, IEEE . (2010, November), "Input towards working documents on Objectives and requirements for mobile wireless access systems for communications to a large number of ubiquitous sensors and/or actuators scattered over wide areas in the land mobile service ". IEEE, Document 5A/IEEE-09-e
- [15] Ericsson . (2012, December 4), "Lowering the threshold for M2M communication ". Web:http://www.ericsson.com/news/121204-lowering-the-threshold-for-m2m-communication_244159017_c
- [16] Crosby, Tim. (2013, February 22), "How Machine-to-Machine Communication Works". Web:<http://computer.howstuffworks.com/m2m-communication.htm>
- [17] Zhong, Yiru. (2011, July), "Connecting devices - an integrated approach to Machine-to-Machine technology". Web: <http://www2.alcatel-lucent.com/blogs/tracktalk/issue-2/connecting-devices-an-integrated-approach-to-machine-to-machine-technology/>
- [18] ADT, (2013, January), "Compare Burglary and Alarm Packages". Web: <https://www.adt.com>
- [19] Coffey, Jerry (2011, September 21). "Edwin H. Hall". Web:<http://www.universetoday.com/90143/edwin-h-hall>
- [20] Hebel, Martin and Bricker, George. (2010), "Getting Started with XBee RF Modules". Web: <http://www.parallax.com/portals/0/downloads/docs/prod/book/122-32450-xbeetutorial-v1.0.pdf>
- [21] MaxBotix Inc. (2005-2012). "LV-MaxSonar®-EZ1™ High Performance Sonar Range Finder". Web: http://www.maxbotix.com/documents/MB1010_Datasheet.pdf
- [22] Parallax Inc. (2012, June 13). "PIR Sensor (#555-28027)". Web: <http://www.parallax.com/Portals/0/Downloads/docs/prod/sens/555-28027-PIRSensor-v2.2.pdf>
- [23] Figaro (2005, March). "Technical Information on Usage of TGS Sensors for Toxic and Explosive Gas Leak Detectors". Web: <http://www.figarosensor.com/products/common%20281104%29.pdf>
- [24] Comfile Technology. (2012, December 13), "CUBLOC User Manual 3.3". Web:<http://cubloc.com/download/cubloctouchmanual.pdf>
- [25] NetBurner, Inc. (2012), "PINK 5V (NNDK-PINK-KIT)". Web:http://www.netburner.com/download/PINK_Documentation.pdf
- [26] Porges, Seth. (2009, June 1), "How to Email Text Messages to Any Phone". Web:<http://www.popularmechanics.com/technology/how-to/4318204>

VITA

Mark Goff was born in Central City, Kentucky to the parents of June and Billy Goff. He earned his bachelor degree in Electrical Engineering at the University of Kentucky. Mark went to work for the Tennessee Valley Authority (TVA) right after college as a field test engineer at the Paradise Fossil Plant. Mark then joined the TVA's Transmission Support Department as a staff engineer in Chattanooga, TN in 1990. Mark developed the Substation Predictive Maintenance program for the Tennessee Valley Authority, and also received an EPRI's Power Delivery & Market Product Champion Award in 2006. He met his wife, Cassandra, while working as a staff engineer.

Mark and his wife, Cassandra, decided to go back to pursue a master degree in Electrical Engineering at the University of Tennessee at Chattanooga in Spring of 2011. Mark is also a registered professional engineer in the state of Kentucky.