Utilizing an Obsolete Mobile Phone as a GSM Modem for an SMS-Based Alarm System

CHARLES RYAN Q. CABASA
BERNARD A. CAMPECIÑO
LOPE BEN C. PORQUIS

Abstract

The SMS-based alarm system is a stand-alone security device which sends text alerts whenever a security button/switch is triggered. A PIC16F877A microcontroller is used to control the SMS capability of a Nokia 3310 mobile phone through the FBUS connection. As long as there is sufficient signal strength and prepaid load, the system will be able to send alert messages to a receiver cellular phone. The results observed from a series of iterative tests prove that the device is reliable. This security device can be used by people who want to make their real-estates safe from intrusion when they are out of town. A message could be sent stating, for example, that a door has been opened and immediate action can be initiated. This project is a good starting point for further improvements such as an appliance control using a cellular phone.

Keywords: SMS-based Alarm System, Nokia 3310, PDU, Nokia Data Suite, Serial Port Monitor, GSM Modem, FBUS/MBUS, mobile phone interfacing.

CHARLES RYAN Q. CABASA, an Undergraduate student of the Department of Electronics and Communication Engineering, College of Engineering (COE) MSU-IIT, His interest is computer interfacing. He is from Iligan City. BERNARD A. CAMPECIÑO is an Undergraduate student, Department of Electronics and Communication Engineering, MSU-IIT, His interest is computer interfacing and comes from Iligan City. LOPE BEN C. PORQUIS, Assistant Professor, Department of Electronics and Communication Engineering (COE), MSU-IIT. His interest is robotics and he is from Iligan City.

I. Overview

Security is a vital aspect for any human being. Properties that need monitoring and protection from intruders must be kept secured. Keeping our properties secure is a challenging aspect in terms of trade-off between cost and reliability.

Text messaging is an emerging communication technology which became so popular that its growth is rapidly increasing. Today almost everywhere is accessible by a text message. SMS has also given people instant access to a wealth of information, tracking, control of the appliances remotely, and many more. In this research we are trying to develop a device which will utilize SMS technology to detect intrusion.

II. Objectives

The goal of this research is to develop a stand alone sms-alarm system using an old mobile phone as a GSM modem. Such goal can be achieved by specifying a set of primary activities such as:

1. To develop a functional block diagram for the whole system.
2. To design and implement the electronics of each functional block.
3. To design an algorithm and write a firmware code for the prototype.
4. To test and evaluate the system for reliability.

III. Methodology

The system allows a user to monitor selected devices from a mobile phone and will be broken down in three main parts: the receiving mobile phone (serving as a device status interface), the control unit (receiving, interpreting and issuing commands), and the security switches.

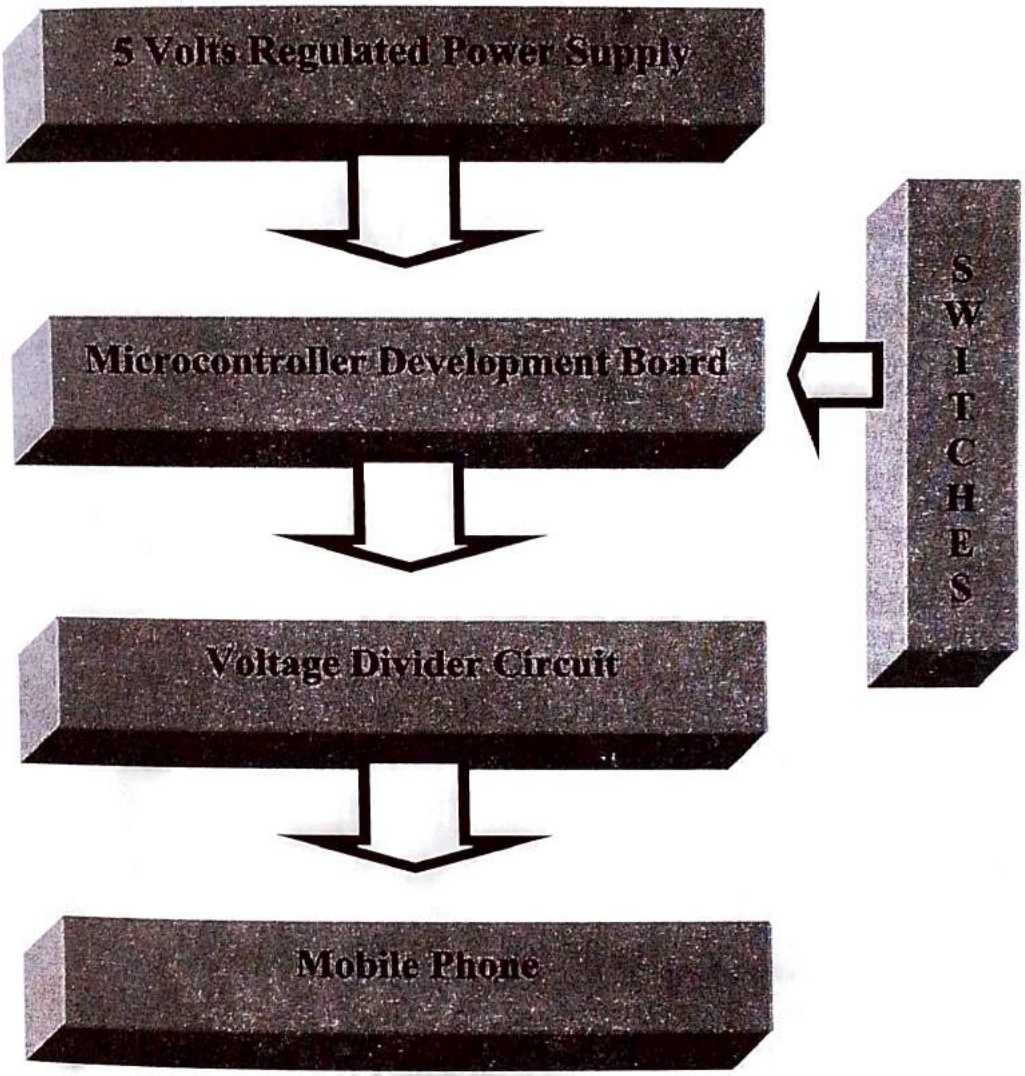

Figure 1. Prototype Block Diagram.

Power Supply

The system is designed to be completely independent from an external power source. A 9 volt battery is used to supply the necessary power needed for the host system. The mobile phone also depends on its own power source which is its battery pack. The 9-volt battery source is regulated to 5 volt potential which is necessary for the host microcontroller to operate.

Microcontroller Development Board

The host was based from a PIC16F877A microcontroller. It operates at 20 MHz in order to keep up with the FBUS protocol. A 20 MHz clock is necessary to produce a 115,200 bps baud rate. Assigning an oscillator with a frequency less than 20MHz would make an erroneous packet sequences resulting to system malfunction.

COMTEST is used to test the functionality of the PIC development board. The test will determine if there are errors on the transmitted packets. Figure 2 illustrates the functional block sequence for testing the PIC development board.

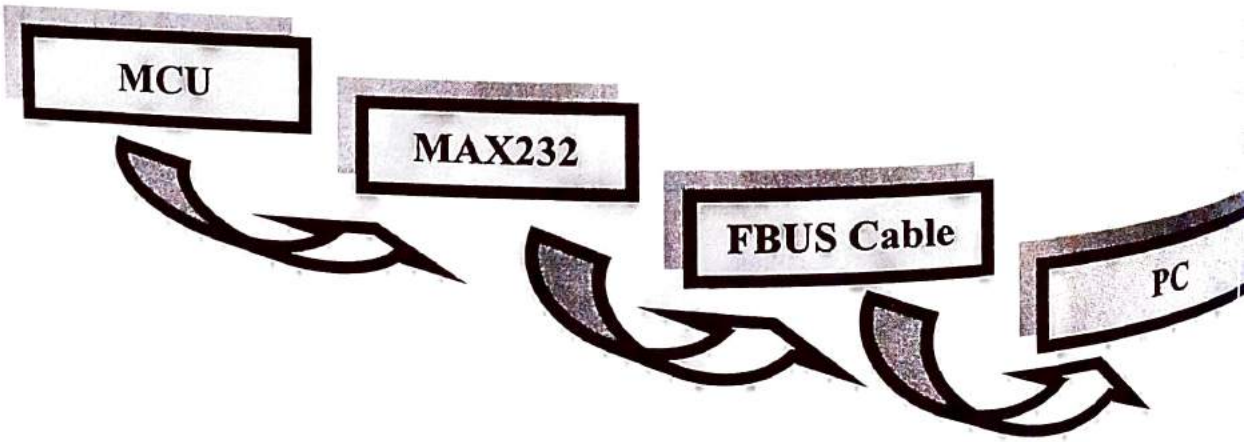

Figure 2. COMTEST Functional Setup.

Voltage Divider Circuit

PIC16F877A has a wide operating voltage level from 2 volts to 5.5 volts but it was set to operate at 5 volt level for reliable results. Nokia 3310 is a 3.3-volt device, such low voltage made the mobile phone operational between 2.2-volts to 3.60-volts. However, Nokia 3310 does not have 5-volt tolerant I/O. Thus to keep the internal circuits from damage, a voltage divider circuit consisting of 560-ohm and 470-ohm resistors are used to lower down the host signal to 2.7 volts. The mobile phone was able to function at this voltage level. The divider circuit is attached only to the transmit pin of the microcontroller since the design is intended for one way communication only – host to mobile phone.

Alarm Switches

The alarm sensors used are only simple limit switches. These switches will simply drive the port pins to either logic 0 or logic 1. Logic 0 is achieved by switching to ground and logic 1 is achieved when switched to 5-volt. The use of double-pole switches is the best alternative to easily get logic 0 and logic 1. Alarm switches were connected to port R_{B0}, R_{B2}, and R_{B4}. Each switch is assigned with a corresponding alarm message. Once somebody pushes any of the alarm switches, the firmware embedded enables the control unit to send these messages to the receiver mobile phone.

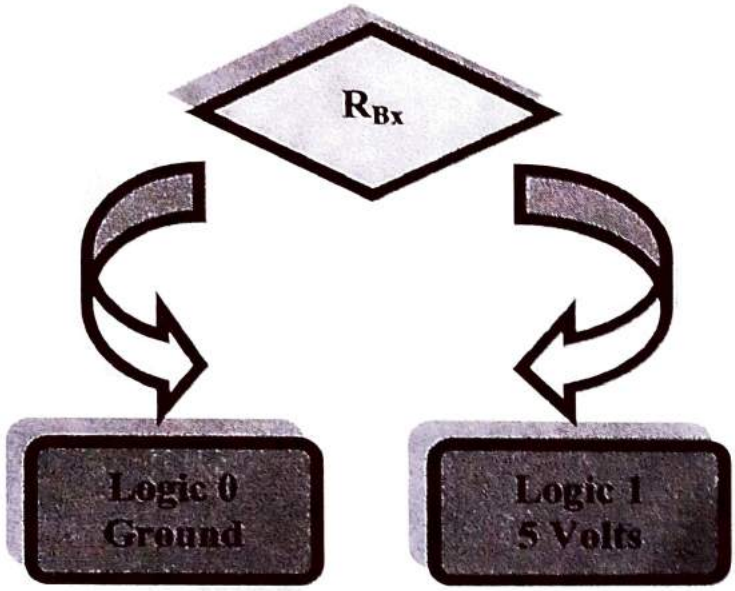

Figure 3. Double–Pole Switch Block Diagram.

Mobile Phone

An old Nokia 3310 served as a GSM modem to attain connectivity to the GSM network. Any mobile number can be used as a sender for the microcontroller while the receiving number should be set permanently in the firmware. The project is not limited by the model of the receiver mobile phone as long as its SIM number is registered in the control unit.

PDU Analysis

The core of the project is the analysis of the Protocol Description Unit (PDU) for SMS messaging. PDU is a standard protocol for communicating with mobile phones. SMS information is always packed into a 7-bit format.

The analysis is implemented by getting the packet sequence during transmission of the desired alert messages. Below is a sample implementation of a full SMS message frame sent from PC to Nokia 3310 mobile phone.

Byte: 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
Data:1E 00 0C 02 00 3C 00 01 00 01 02 00 07 91 36 19 07 00 10 03 FE 12 00 70 11 00

Byte: 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51

Data: 00 00 12 0B 81 90 72 69 79 05 F5 00 00 00 00 FF E1 43 00 00 00 D7 41 76 58 DE

Byte: 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67
Data: 06 C5 40 E1 31 3D 6D 0F D3 CB E4 10 01 43 60 6D

F-Bus Frame Header

Byte 0: F-Bus Frame ID. Cable (0x1E), Infrared (0x1C).
Byte 1: Destination address.
Byte 2: Source address.
Byte 3: Message Type or 'command'. 0x02 (SMS Handling).
Byte 4 & 5: Message length. In our case it is 60 bytes long.

Short Message Service Frame Header

0x00 Byte 6 to 8: Start of the SMS Frame Header. 0x00, 0x01,

Byte 9 to 11: 0x01, 0x02, 0x00 = Send SMS Message.

Short Message Service Centre

Byte 12: SMS Centre number length. 0x07 is 7 bytes long. This includes SMSC Number Type and SMS Centre Phone Number

Byte 13:SMSC number type (e.g. 0x81-unknown 0x91-international 0xA1-national)

Byte 14 to 23: (Octet format) SMS Centre Phone Number. In our case +639170000130.

Transfer Protocol Data Unit

Byte 24: Message Type. In our case it is 0x11. The message is SMS Submit and Validity Indicator present.

Byte 25: Message Reference if SMS Deliver & Validity Indicator used.

Byte 26: Protocol ID.

Byte 27: Data Coding Scheme.

Byte 28: Message Size is 0x12 in hex or 18 bytes long in decimal. This is the size of the unpacked message.

Destination's Phone Number

Byte 29: Destination's number length.

Byte 30: Number type (e.g. 0x81-unknown 0x91-international 0xA1-national)

Byte 31 to 40: (Octet format) Destination's Phone Number. (e.g. in our case 09279697505)

Validity Period

Byte 41: Validity-Period Code. The time period during which the originator considers the short message to be valid.

Byte 42 to 47: Service Centre Time Stamp.

The SMS Message (SMS-SUBMIT)

Byte 48 to 63: This is the SMS message packed into 7 bit characters.

Byte 64: Always 0x01.

The F-Bus Usual ending

Byte 65: Packet Sequence Number

Byte 66 & 67: Even & odd checksum bytes.

Acquiring message frame requires a software utility called Serial Port Monitor. The software logs any data that comes in and out the RS232 terminal of the PC. Another software utility named Nokia Data Suite (NDS) is also used to control the mobile phone using the PC. SMS messaging function of the mobile phone can be done on the PC using the NDS utility.

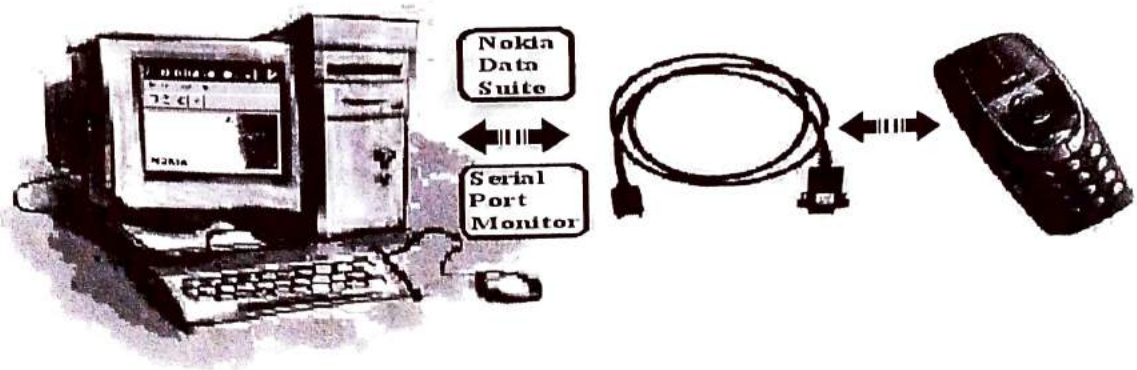

Figure 4. Setup for Acquiring Message Frames.

FBUS Cable Experimentation

FBUS cable functionality was tested by the use of the Nokia Data Suite software that supports communication between the Nokia 3310 and the personal computer. This software indicates the signal and battery level and enables the computer to send and retrieve messages from the phone. The mobile phone analysis was also done through Nokia Data Suite experimentation.

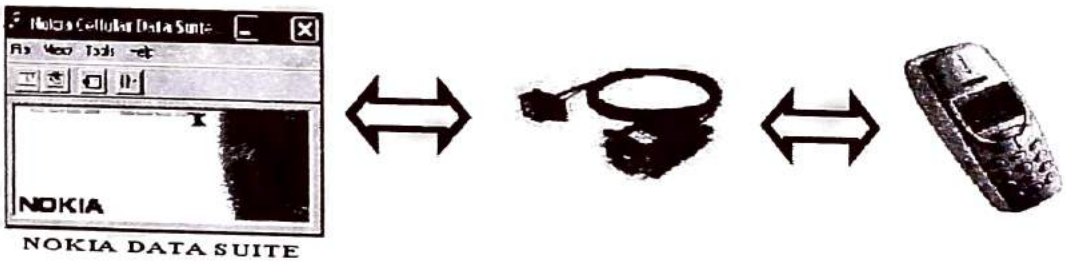

Figure 5. FBUS Cable Experimentation Setup.

The resulting packets were observed and captured using the Serial Port Monitor (SPM) software that can be downloaded from the internet. The FBUS cable was used in order for the cellular phone and the personal computer to communicate. The serial port monitor software is a logger that records any activity in the serial port. This application must be activated before text messages are sent using the Nokia Data Suite so that correct packets can be captured.

Voltage Divider Cable

The voltage divider cable is a direct way to connect the microcontroller and the mobile phone. The circuit shown in Figure 7 used 470 and 560 ohm resistors.

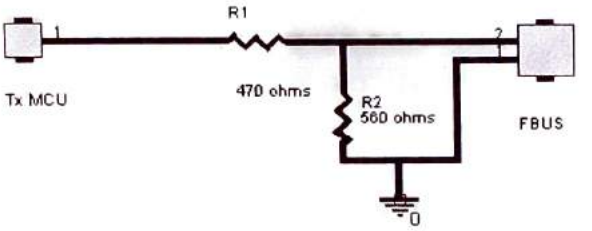

Figure 6. Voltage Divider Schematic.

Mobile Phone Experimentation

The preliminary process of mobile phone experimentation is the installation of the Nokia Data Suite and mobile phone. The mobile phone is deemed functional if it is able to send messages via the PC through the NDS. Voltage levels for each of the pins of the serial port can also be monitored with the use of an oscilloscope.

A Visual Basic test application was developed to test the SMS functionality of the mobile phone using captured messages from the serial port monitor. Figure 7 illustrates the theory.

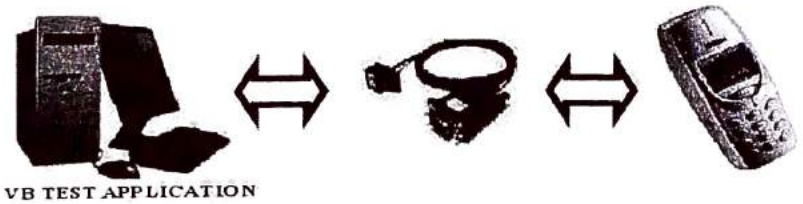

Figure 7. Mobile Phone Experimentation.

The resulting data in the serial port monitor are in the PDU mode. Each of the alert messages served as an input to the Visual Basic Test Application. Three frames appeared on the Serial Port Monitor, but the last two frames were enough for VB test application to send messages. These frames were successively sent to the phone with a delay of one second in between frames. Several parameters that were useful for reference were included in the test application. The Visual Basic Test Application can test if the mobile phone is able to perform the commands issued by the application.

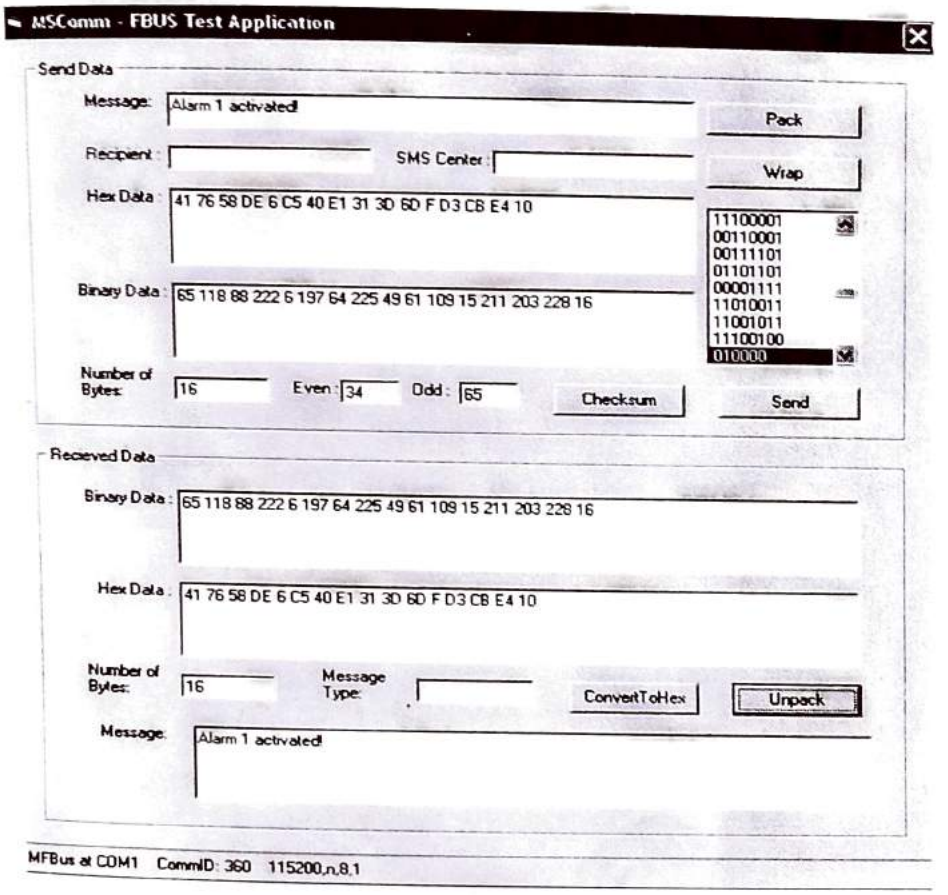

Figure 8. Visual Basic Test Application.

Device Testing and Evaluation

Each alarm switch is tested to assure that the device will send an alarm message when triggered. The Activate/Deactivate feature is also tested. If the device is activated, it must send a message if any switch is triggered. On the other hand, if it is deactivated, the device can not send alarm messages if any switch

is triggered. When the alarm switches are triggered simultaneously a race condition occurs and depending on where the current program flow is, one of the alarm messages will be sent.

Troubleshooting of the hardware was made easy due to accessibility headers installed on the development board. These header connections enable users to isolate the hardware components for a thorough checking of possible defects. The device is then placed in a secured area so that intruders will not notice the existence of the alarm.

IV. Results

The researchers underwent many trial and error schemes before getting through the desired operation and outcome. Almost every part of the hardware had its limiting factors that, if ever violated, would produce an evident error at the later part of the procedures. The first attempt in developing the security device includes a sender mobile phone (Nokia 3310) and its FBUS data cable (DAU-9P), PIC16F877A microcontroller, and a MAX232. The setup is shown below.

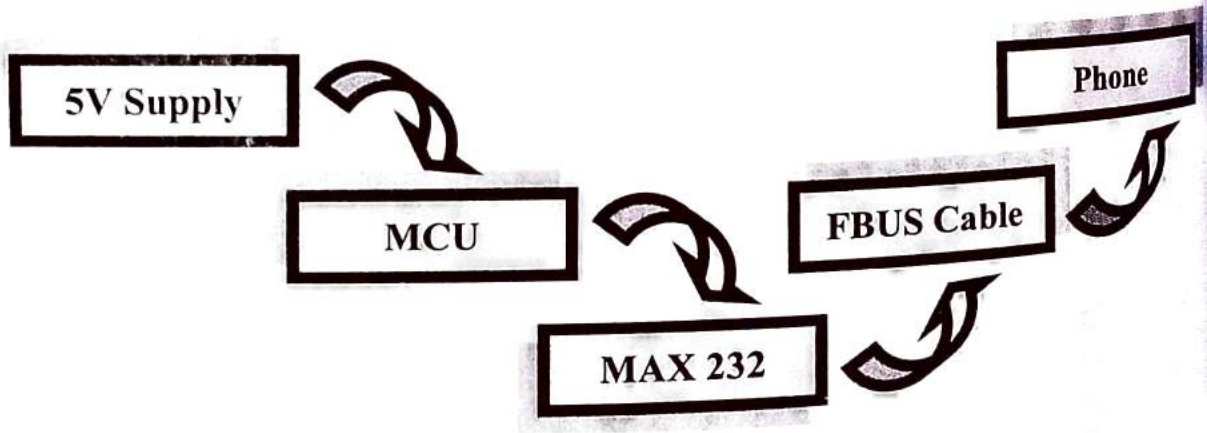

Figure 10. Experimental Setup.

A Visual Basic application was developed to test the mobile phone for SMS transmission using the message frames that we have captured from the Serial Port Monitor. The test was successful and increases the level of confidence that a microcontroller can be used as a replacement for sending message frames to the cell phone. One significant problem we encountered was that the insufficient voltage signal on the MAX232 pin. This situation halted the FBUS cable implementation as a communication link for the host and the mobile phone. We resolved the problem by using a voltage-divider data cable as a replacement for the MAX232 and the DAU-9P serial data cable. The problem for using the voltage divider cable is that it can support only one way transmission as compared to the FBUS cable. However since we are using only one way transmission, the alternative cable was already a good solution.

The EEPROM peripheral of the microcontroller was utilized since the RAM ran out of memory space for the three alarm messages. The alarm message frames are stored in the EEPROM. The memory capacity allows up to four alarm messages to be stored in the EEPROM.

There is no restriction on the kind of network that provides SMS messaging. Smart and Globe Network are two of the known network providers. The SMS alarm system functioned properly with these networks provided that enough prepaid credit is loaded on the SIM.

The triggering of the alarm switches was tested thoroughly. Different triggering situations were simulated to test the durability of the device and the robustness of the algorithm. Once a switch has been triggered and a message was sent to the GSM network, the device will not be able to send another message even if a succeeding alarm switch was triggered. This is due to the one-way communication constraint of the system. An acknowledgement frame must be sent to the system by replying a dummy message. This will tell the system that the message has been received by the recipient.

The reliability of the device is evaluated by multiple triggering of the switches. The results were tabulated and it

showed that the device is functional. The reliability that the alarm messages are successfully and immediately received by the recipient depends on the GSM network conditions.

Table 1. Evaluation Results

Trial No.	Alarm Switch Number			Remarks
	1	2	3	
1	Message sent	Message sent	Message sent	functional
2	Message sent	Message sent	Message sent	functional
3	Message sent	Message sent	Message sent	functional
4	Message sent	Message sent	Message sent	functional
5	Message sent	Message sent	Message sent	functional
6	Message sent	Message sent	Message sent	functional
7	Message sent	Message sent	Message sent	functional
8	Message sent	Message sent	Message sent	functional
9	Message sent	Message sent	Message sent	functional
10	Message sent	Message sent	Message sent	functional

V. Conclusion

The SMS alarm system is a security device which uses an obsolete mobile phone as a GSM modem for connectivity with the GSM network. Only simplex communication between the MCU and the mobile phone was implemented. The MAX232 level converter was eliminated since its voltage level is not enough to

drive the proper operation of the FBUS cable. A simple voltage divider cable was used as a replacement and performs the level conversion properly.

If the alarm switches are triggered simultaneously a race condition occurs and depending on where the current program flow is, only one of the alarm messages will be sent. Once a switch has been triggered and a message was sent to the GSM network, the device will not be able to send another message even if a succeeding alarm switch was triggered. This is a practical way to minimize the waste of prepaid load due to excessive triggering of the sensor caused by the same source of disturbance. .

The device worked effectively as the researchers expected. The GSM network constraints can be a restriction to the reliability of the alarm system. The objectives of the projects were fully attained.

VI. Recommendations

1. The researchers recommend a two-way communication between the host and the mobile phone. The microcontroller should be able to interpret commands coming from the cellular phone. Furthermore, it is required for the microcontroller to have a high memory capacity to perform the two-way scheme.
2. The researchers motivate enthusiasts to make impressive applications for this device. One way is remote controlling home appliances or automobiles in cheapest possible way. The researchers have done the first step.
3. The researchers recommend the use of advanced sensors like infrared and wireless motion sensors.

VII. References

Adeva, Manuel & Ungui, Felix Jorge. (2006). *Remote Controlled Household Automation via SMS.*

Bhudy. (2006). *plz]8051 + cell phone.* [Online]. Available: http://www.edaboard.com/ftopic202032.html

Hayt, William H. Jr, Jack E. Kemmerly, and Steve M. Durbin. (2002). *Engineering Circuit Analysis.*

Katzen, Sid (2001). *The Quintessential PIC Microcontroller.* Springer.

NavMicroSystems. (2004). *Pic to GSM Phone connection.* [Online]. Available: http://www.picbasic.co.uk/forum/member.php

Peacock, Craig .(2005). *Interfacing the Serial / RS232 Port.* [Online]. Available: http://www.beyondlogic.org/serial/serial.htm

Peacock ,Wayne. (2005). *An Introduction to Nokia F-Bus.* [Online]. Available: http://embedtronics.com/nokia/fbus.html

Pettersson, Lars. (2002). *SMS and the PDU format.* [Online]. Available: http://www.etsi.org

Sandstorm, Peter. (2004). *MikroGuard Mark 1.* [Online]. Available: http://www.spaceorbit.net/index.html

Wikipedia. (2007). *Short message service.* [Online]. Available: http://en.wikipedia.org