DEDAN KIMATHI UNIVERSITY OF TECHNOLOGY

DEPARTMENT OF ELECTRICAL AND ELECTRONIC ENGINEERING

BSc. Electrical and Electronic Engineering

Text Message-Based Electrical Devices Monitoring and Control System Using GSM Technology

BSc. Project Report

NAMES:

1. OBIRI MOKUA NAHSHON **Reg. Number:** E021-0917/2012
2. KUTIRI MUKUI BILLEZRA **Reg. Number:** E021-0899/2012

JANUARY, 2017.

A project report submitted to the Department of Electrical and Electronic Engineering in partial fulfillment of the requirements for the award of the degree of Bachelor of Science Electrical and Electronic Engineering.

January 2017

DECLARATION

This project report is our original work, except where due acknowledgment is made in the text and to the best of my knowledge has not been previously submitted to the Dedan Kimathi University of Technology or any other institution for the award of a degree or diploma.

NAMES:

OBIRI MOKUA NAHSHON **Reg. Number:** E021-0917/2012

SIGNATURE: …… **DATE**: ……

KUTIRI MUKUI BILLEZRA **Reg. Number:** E021-0899/2012

SIGNATURE: …… **DATE**: ……

This research report has been submitted to the Department of Electrical and Electronic Engineering, Dedan Kimathi University of Technology, with my approval as the supervisor.

Signature: …… **Date**: …….

Name: Mr. TESHOME SOLOMON.

ACKNOWLEDGEMENT

Special thanks to the particular group individuals who have contributed to the development of this project. We are deeply grateful to the Electrical and Electronic Engineering Department members, Dedan Kimathi University of Technology for their mentorship and inspiration.

Great thanks to our supervisor, Mr. Teshome Solomon, Chairman of Department, Dr. Ciira, and the project co-ordinator, Mr. Kimathi, alongside the Dedan Kimathi University fraternity.

Above all, Thanks to The Almighty God.

ABSTRACT

It is no secret that the average number of electrical appliances under the control of an individual has increased tremendously in the recent past throughout the world. With the increase in the number of appliances, there arises the problem of controlling these devices, and the problem grows when the person(s)-in-charge and the devices are extremely far apart geographically. Recently, different researchers have tried to solve the problem at hand which is to monitor effectively and control devices remotely while at the same time enhancing accountability in case a device has more than one operators. However, they have encountered some challenges as elaborated in chapter two of this proposal

In this project, a text message based electrical devices monitoring and control system using Global System for Mobile (GSM) Technology was implemented with a GSM shield, Atmega328p microcontroller, Light Emitting Diodes (LEDs), relays and lamps. The Atmega328p microcontroller works as the "heart" of the full implementation while a GSM shield acts as the communication interface between the system and the network. The GSM shield was fitted with a Subscriber Identifier Module (SIM) and configured so that it receives and sends messages over a network. The microcontroller was programmed to retrieve the message received by the shield after being notified of the availability of an unread text message and in response turn on or off an electrical appliance according to the contents of the message. It was also programmed to monitor the on/off status of the appliances and inform the user via an SMS message whenever asked to. The status of the electrical devices is displayed by LEDs which also act as the Human Machine Interface (HMI).

TABLE OF CONTENTS

DECLARATION ii
ACKNOWLEDGEMENT iii
ABSTRACT iv
TABLE OF CONTENTS v
LIST OF FIGURES vii
LIST OF TABLES vii
LIST OF ABBREVIATIONS viii
CHAPTER ONE: INTRODUCTION 1
1.1 Background 1
1.2 Problem Statement 2
1.3 Justification 2
1.4 Objectives 3
1.4.1 Main Objective 3
1.4.2 Specific Objectives 3
2 CHAPTER TWO: LITERATURE REVIEW 4
2.1 General Principles of Operation 4
2.2 Current Trends 4
2.2.1 Bluetooth-Based Home Automation System 4
2.2.2 DTMF-based Home Automation System 6
2.2.3 Internet-Based Home Automation System 7
2.2.4 Decentralized Approach to Home Automation Systems 8
2.3 The Implemented Approach 9
3 CHAPTER THREE: METHODOLOGY 11
3.1 Block Diagram 11
3.2 Explanation of the Block Diagram 12
3.2.1 GSM Modem/Shield 12
3.2.1.1 GSM Shield Board Specifications 12
3.2.2 Arduino Uno R3 14
3.2.2.1 The Arduino software 15

3.2.2.2 Creating the Program 16
3.2.3 Interfacing the GSM shield with Arduino 16
3.2.4 Relays 17
3.3 Flow Chart of the System 18
3.4 Operation 18
3.5 Main Components of the Project 19
3.5.1 GSM Technology 19
3.5.2 Short Message Service 19
4 CHAPTER FOUR: RESULTS AND DISCUSSION 21
4.1 Results 21
4.1.1 User Authentication 21
4.1.2 Control Operations 22
4.1.3 Monitoring operations 23
4.1.4 The Human Machine Interface 24
4.1.5 User friendliness 24
4.2 Discussion 25
5 CHAPTER FIVE: CONCLUSION AND RECOMMENDATION 26
5.1 Conclusion 26
5.2 Recommendations 26
REFERENCES 28
APPENDIX 30

LIST OF FIGURES

Figure 2:1 Basic Block Diagram of System Automation 4
Figure 3:1 The Block Diagram of the System 11
Figure 3:2 GSM Shield Model 12
Figure 3:3 Arduino UNO Board 14
Figure 3:4 Arduino IDE Window 15
Figure 3:5 Circuit diagram of relays 17
Figure 3:6 The System Flowchart 1 18
Figure 3:7 The GSM Architecture 19
Figure 4:1 a Photograph of the Implemented System 21
Figure 4:2 User Authentication Sample Report 22
Figure 4:3 Control Sample Operation 23
Figure 4:4 Monitoring Sample Operation 24

LIST OF TABLES

Table 3.1: Arduino UNO specifications 14

LIST OF ABBREVIATIONS

AuC	Authentication Centre
BSC	Base Station Controller
BTLE	Bluetooth Low Energy
BTS	Base Transceiver Station
CA	Communication Authority
DTMF	Dual Tone Multi-Frequency
GPRS	General Packet Radio Service
GSM	Global System for Mobile
HAP	Home Automation Protocol
HLR	Home Location Register
HMI	Human Machine Interface
ICs	Integrated Circuits
I^2C	Inter-Integrated Circuit
IDE	Integrated Development Environment
ISDN	Integrated Service Digital Network
LEDs	Light Emitting Diodes
MSISDN	Mobile Station International Subscriber Directory Number

OMC	Operations and Maintenance Centre
PSTN	Public Switched Telephone Network
SIM	Subscriber Identifier Module
SMS	Short Message Service
SMSC	Short Message Service Centre
REALSWSN	Real World Wireless Sensor Networks
RF	Radio Frequency
VLR	Visitor Location Register
WSN	Wireless Sensor Networks

CHAPTER ONE: INTRODUCTION

This chapter will present the background to the study, the statement of the problem, the justification, the main objective and specific objectives of the project.

1.1 Background

Electrical appliances and instruments have made a profound impact on the 21st century. The appliances can be any device in the home, office or industry such as air conditioners, bulbs, and motors. Industries have acquired a variety of appliances to increase their productivity, organizations have purchased them to enhance efficiency, while individuals have bought them for comfort and entertainment at home. Currently, the technologies used to control these devices include Bluetooth, Infrared, and Radio Frequency (RF). These technologies have been very reliable in controlling the devices. However, their effectiveness has been hampered greatly by the limited distance of operation. Currently, a single person could be in charge of several devices at one particular time. These devices could be widely separated geographically. This calls for a more effective system for remotely controlling and monitoring of these devices.

The GSM technology is a widely known cellular network. In Kenya, the mobile penetration rate stands at 94% of the population and the Communication Authority (CA) projects it to rise to 98% over the next few years [1]. The GSM being a basic standard, it is correct to say that all the mobile phones are enabled. The cost of sending text messages has dwindled to very little amounts. All these factors make the GSM technology a very ripe means for controlling devices since it affects the control and monitoring of appliances over great distances of separation. The separation distance is not limited to the national boundaries as the roaming feature of the GSM technology allows communication over international boundaries. The case of remote control capability and

the possibility of achieving it at a reasonably low cost have motivated the need to research into it not only for industrial application but also for domestic use.

1.2 Problem Statement

There is a challenge in effectively controlling and monitoring of appliances, especially from remote areas. This problem grows when the number of appliances under control is large. The situation even worsens when the number of people controlling the devices is more than one, and there is a need for transparency and accountability for any operation performed. Ever since the commercialization of Integrated Circuits (ICs), there has been an increase in the average number of appliances per person throughout the world. In the developing countries, the numbers have been slightly lower compared to their developed counterparts. However, the numbers are set to rise significantly especially with the decreasing costs of connecting to the mains power such as in Kenya. This is a clear indicator that the problem is set to rise

1.3 Justification

Technology has widely advanced in the last decade or two making life more efficient and comfortable to live. The comfort and ability to control devices from one particular geographical location have become a necessity as it saves much time, effort, and is also convenient. Therefore, there arises a need to do so in a systematic manner which is implemented with our system. The system developed is an extended approach to automating a control system.

Moreover, it enhances transparency since the control messages issued to the devices and the status messages generated by the system can be linked directly to an individual's Subscriber Identification Module (SIM), and therefore, a record of control events can be obtained and stored for any useful purposes such as billing, accountability, transparency among others.

1.4 Objectives

1.4.1 Main Objective

To implement a text message-based system that monitors and controls the ON and OFF status of electrical devices using GSM technology.

1.4.2 Specific Objectives

1. To configure a GSM shield to receive text messages, communicate with a microcontroller and send text messages to a remote user.
2. To develop a program that enables the microcontroller act by the GSM shield instructions and the status of the electric devices linked.
3. To configure a relay subsystem that turns ON/OFF (controls) the devices at hand, after communicating with the microcontroller.

CHAPTER TWO: LITERATURE REVIEW

A variety of technologies for remote monitoring and controlling of electrical devices had been deployed in the recent past. Different researchers sought to improve the existing technologies. However, there remained some challenges associated with each technology. This chapter focuses on a few relevant publications, the challenges related to each of them, and ultimately highlights on the improvements made in this project.

2.1 General Principles of Operation

The following flow chart summarizes the principle of operation of all related works.

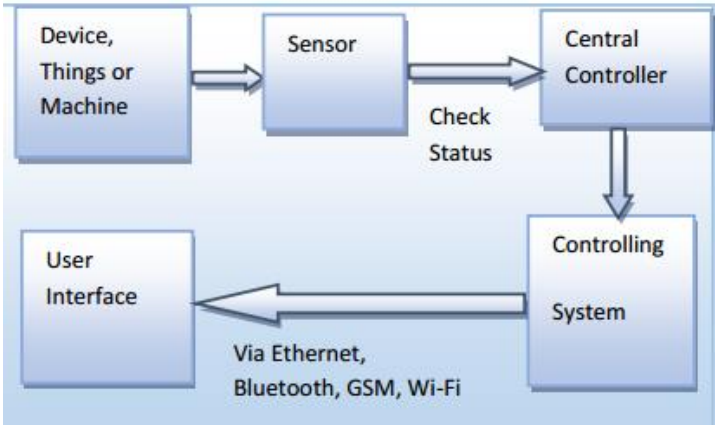

Figure 2:1 Basic Block Diagram of System Automation [2]

2.2 Current Trends

There are numerous technologies that had been used previously to control electrical devices. A few of them are explained below

2.2.1 Bluetooth-Based Home Automation System

The implementation of a home automation system using Bluetooth was proposed in 2002 [2]. A host controller implemented on a PC was used, which was connected to a microcontroller- based

sensor and device controllers. A new protocol on top of the Bluetooth software stack, called Home Automation Protocol (HAP), was used to make the communication between devices possible. The device controller was connected to electronic devices through the Inter-Integrated Circuit (I^2C) Bus. The system allowed more than one device controller to be connected to the host controller.

A home automation system using Bluetooth that could be accessed remotely through General Packet Radio Service (GPRS) was also proposed in 2003 [3]. A cell phone equipped with Bluetooth connectivity was used as a host controller in conjunction with a GSM modem that provided Internet connectivity. Home devices were fitted with Bluetooth communication adapters so that they could communicate with the host controller phone via Bluetooth. The paper discussed remote control and updating home devices along with fault diagnostics and detection. The work also talked about providing an electronics user manual on the phone using Bluetooth and Internet.

These systems encountered several challenges as follows:

- Bluetooth has a maximum communication range of 100m in ideal conditions. More may be needed in a home environment. This is a limited range compared with other available technologies
- Bluetooth communication has comparatively high power consumption, so the batteries of devices need to be frequently recharged or replaced.
- Bluetooth technology has advanced and improved to Bluetooth Low Energy (BTLE), which provides the same range of communication. However, it has serious security concerns such as eavesdropping and weak encryption as discussed in 2013[4].

Bluetooth looks like an attractive communication technology for creating smart homes. It is cheap, easy, and quick to set up. People are already familiar with the technology. The hardware

required for establishing Bluetooth communication is readily available. However, they also have serious flaws, as discussed above.

2.2.2 DTMF-based Home Automation System

Dual Tone Multi-Frequency (DTMF) was used in mobile communication way back in 1995[5]. There were three components in the systems: a DTMF receiver and ring detector, an Input/output interface unit, and a Personal Computer (PC). The PC detected the ringing of the line and then authenticated the user to use the keypad tones to control the devices as required. An example of a stepper motor control was taken up. That system had the advantage of being secure and allowing international standardization. This is because the DTMF tones were the same all over the world. A design and implementation of a DTMF- based home automation system was also described in 2012 [6]. The user called a Subscriber Identifier Module (SIM) number assigned to the home and pressed the digits on their phone's keypad to control the home's devices by generating a DTMF tone. The tone was received and decoded by the GSM module at home using a DTMF decoder. The decoded instructions were passed to the microcontroller so that user commands could be implemented at home. Home automation systems using DTMF were rarely implemented because;

- There are other better options for communication available. Like all other systems, DTMF- based home automation systems also had their security flaws. They were vulnerable to "fuzzing attacks," [7]. In a fuzzing attack, a user exploits a vulnerability in DTMF processing algorithms by giving unusual input data, which results in triggering an exception. This could cause the entire home network to crash.
- It suffered from the drawback that the number of appliances is limited by the number of keys on the keypad.

- Another hindrance to the adoption of the DTMF based control system was the high tariffs in making calls compared to some cheaper alternatives available such as text messages.

2.2.3 Internet-Based Home Automation System

Internet-based communication in home automation systems has always been a popular choice among researchers. The Internet is easily scalable, flexible when it comes to access and use, and very popular as a communication method in today's world, so the hardware and the network required for access are readily available, offers high bandwidth and very low communication cost, and devices can connect to and disconnect from the network easily. Utilizing the Internet as a means to access and control the home seemed to be the next logical step forward for home automation systems. From an end user's point of view, using the Internet to access their home was easy, convenient, cheap, flexible, and offered no complication of an added technology to learn. User interface devices like laptops, smartphones, PCs, and tablets were easily available on the market, and these devices are already a part of people's daily lives. So, incorporating home automation into these already- popular user devices seemed to be the natural progression.

These systems raised some security concerns as follows:

- People were careless in nature. They tended to write complicated passwords and usernames on paper near their workstations or underneath their keyboards, thinking "who bothers to look there?"
- People often repeated the same passwords and usernames on different websites and forums. This behavior made them vulnerable to phishing attacks.

During the course of time, a homeowner would log into the home from different networks like from the office, from their friend's house, from public Wi-Fi networks such as coffee shops, or even parks, sometimes using untrusted devices. The network chosen by the user to access the home could be vulnerable. This could result in the user being exposed to a variety of attacks like man-in-the-middle attacks. Moreover, when accessing the home from a compromised device, legitimate user credentials could be stolen by the use of simple software tools such as a key logger.

2.2.4 Decentralized Approach to Home Automation Systems

Home automation systems discussed so far used a central controller or centralized approach, which had a single point of failure. In this section, we discuss another method. Proposed in 2008 was a decentralized approach to home automation control [8]. They implemented the decentralized approach by integrating actuators into the Wireless Sensor Networks (WSN) of the home. They proposed a distributed control or Process architecture. The information from the sensors was received and processed by one or more control nodes, which in turn initiated the appropriate actuators to change or control the environment as previously specified by the user. The system thus eliminated the need for a central controller.

These systems had the following challenges:

- A sophisticated attacker with prior knowledge of the network and actuator positions could simply disconnect them from the network. No alert mechanisms were implemented for such a case.
- The communications proposed here were done in clear text, so an attacker with the right hardware could eavesdrop on the communication.

- A home automated system consisted of complicated tasks which required analyzing and processing various values and inputs from different parts of the home during various points of time. It required some processing power and storage, which the actuator nodes could not provide then.

The decentralized approach to home automation was an interesting concept, but it required much work from the research community to be efficiently and securely implemented in a home environment. In addition to this, the actuators discussed here required a significant increase in processing power and storage for it to be useful in a decentralized architecture.

2.3 The Implemented Approach

As seen above, most existing systems are inclined towards home automation. Despite the enormous setback that none is meant for industrial applications, they also suffer a huge number of weaknesses as has been observed. These problems were solved by our developed system as follows:

Our system, text message-based electrical devices monitoring and control using GSM technology, is not limited regarding the distance of operation. It employs GSM technology, a global standard. The second drawback highlighted in the other technologies is the security of operation which was alleviated in this system by restricting the legible system operators; subject to customization.

Moreover, this system has an advantage over the other systems in that, in as much as it achieves remote control of devices over long distances, the initial acquisition cost is quite low because prices of basic cellular phones have dropped significantly compared with other devices that can be used for the same function.

Furthermore, the operation costs are significantly low since the cost of sending an SMS is incomparably low when contrasted to the cost for a call, which is necessary in the case of DTMF based control system. The originality of this project lies in the fact that an LCD screen was replaced with LEDs as the Human Machine Interface (HMI). This is a better means of displaying the system processes to an onlooker since the different colors of the LEDs can easily be interpreted at a glance compared to the LCD screen where one has to move very close to read the text displayed.

CHAPTER THREE: METHODOLOGY

This chapter explains the theoretical and experimental methods that were chosen to achieve the set objectives. The chapter also emphasizes on the reasons we chose specific components, programs, programming languages, and materials to implement the system.

3.1 Block Diagram

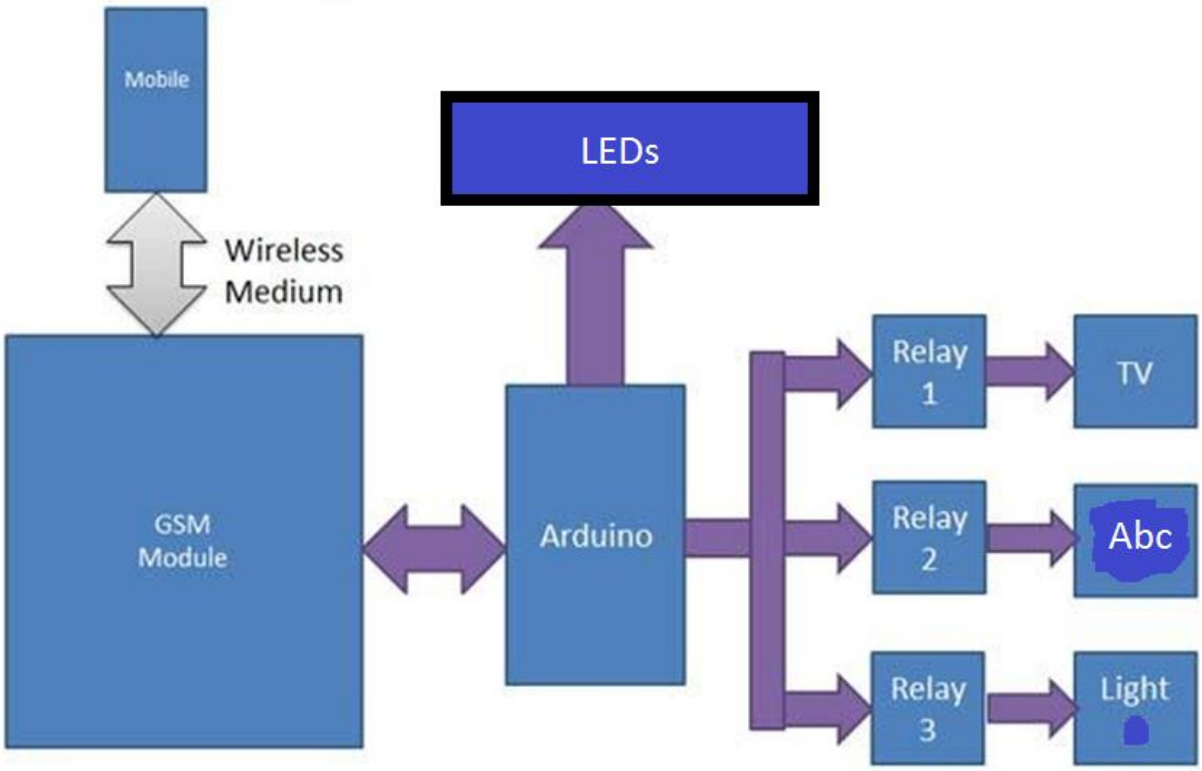

Figure 3:1 The Block Diagram of the System

3.2 Explanation of the Block Diagram

3.2.1 GSM Modem/Shield

Figure 3:2 GSM Shield Model [6]

3.2.1.1 GSM Shield Board Specifications

- Based on SIM Com's SIM900 Module
- Quad-Band 850/900/1800/1900 MHz
- Control via AT commands - Standard Commands: GSM 07.07 & 07.05 | Enhanced
- Commands: SIMCOM AT Commands.
- Short Message Service - so that one can send small amounts of data over the network
- (ASCII or raw hexadecimal).
- Embedded TCP/UDP stack – allows one to upload data to a web server.
- Speaker and Headphone jacks - so that one can send DTMF signals or play recording
- Like an answering machine.

- SIM Card holder and GSM Antenna - present onboard.
- 12 GPIOs, 2 PWMs and an ADC (all 2.8-volt logic) - to augment your Arduino.
- Low power consumption - 1.5mA (sleep mode)
- Industrial Temperature Range - -40°C to +85 °C

A GSM modem is a specified type of modem which accepts a SIM card, and operates over a subscription to a mobile operator, just like a mobile phone [9]. From the mobile operator perspective, a GSM modem looks just like a mobile phone. It can be a devoted modem device with a Universal Serial Bus (USB), Bluetooth connection, or serial connection used in this document.

GSM module is used in many communication devices which are based on GSM technology. It is used to interact with GSM network using a computer. It only understands AT commands and can respond accordingly. The most basic command is “AT,” if GSM responds OK then it is working well otherwise it respond with “ERROR.” There are various AT commands like ATA for answer a call, ATD to dial a call, AT+CMGR to read the message, AT+CMGS to send the SMS, among others. AT commands should be followed by Carriage return i.e. \r (0D in hex), like “AT+CMGS\r.”

When we send an SMS to GSM module by Mobile, it receives that SMS and sends it to Arduino.

3.2.2 Arduino Uno R3

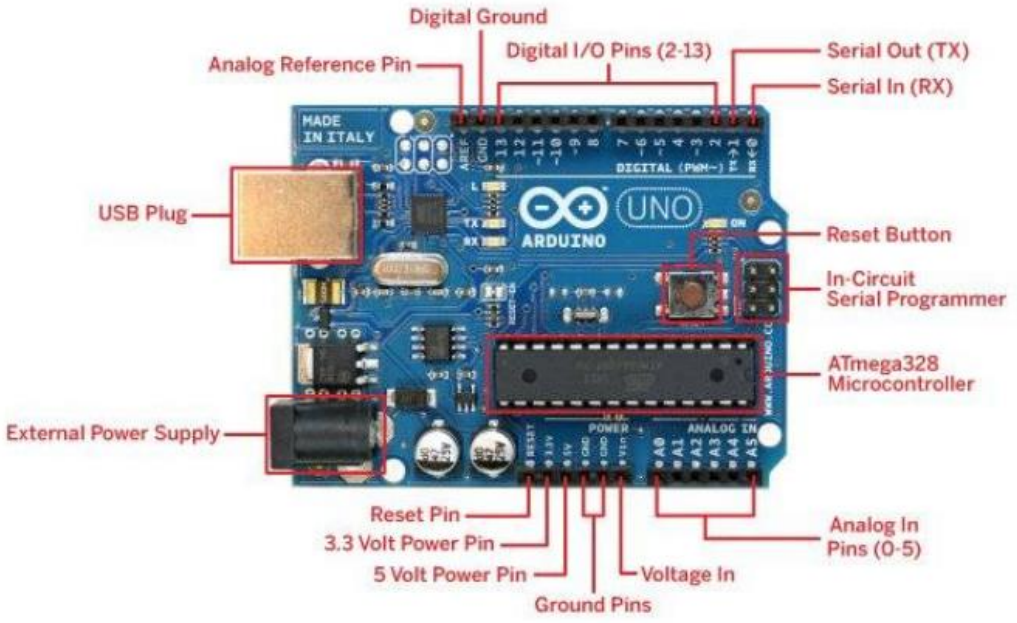

Figure 3:3 Arduino UNO Board [6]

The Arduino Uno is a microcontroller board based on the **ATmega328**.

In this project, Arduino was used for controlling the whole process. We have used GSM wireless communication for monitoring and controlling electrical appliances.

Table 3.1: Arduino UNO Specifications

Microcontroller	Atmega328
Operating Voltage	5V
Input Voltage (recommended)	7-12V
Input Voltage (limits)	6-20V
Digital I/O Pins	14 (of which 6 provide PWM output)
Analog Input Pins	6
DC per I/O Pin	40 mA
DC for 3.3V Pin	50 mA

Flash Memory	32 KB (Atmega328) of which 0.5 KB used by bootloader
SRAM	2 KB (Atmega328)
EEPROM	1 KB (Atmega328)
Clock Speed	16 MHz

3.2.2.1 The Arduino software

Figure 3:4 Arduino IDE Window

The Arduino UNO microcontroller was programmed using the Arduino software (Integrated Development Environment (IDE)), and its window is as shown above. It is a special software installed on a computer that allowed us to write sketches for the Arduino board in a simple language modeled after the Processing language. When the sketch was uploaded to the board: the code was translated into the C language and was passed to the avr-gcc compiler; an important piece of open source software that makes the final translation into the language understood by the microcontroller. This last step was quite important because it is where Arduino makes life simple by hiding away as much as possible of the complexities of programming microcontrollers.

3.2.2.2 Creating the Program

A program was created in the Arduino IDE and then uploaded to the Arduino board. The code was entered in the proper syntax which means using valid command names and a valid grammar for each code line. Sometimes the error message was cryptic, and one had to do a bit of hunting because the actual error occurred before what was flagged. Although the program could pass cleanly through the syntax checker, it still might have not done what it was intended to. In this case, code debugging skills had to be honed. The Arduino performed as per what it was instructed to, rather than what it was intended. The best way to catch these errors was to read the code line by line and be the computer. Having another person go through the code also help.

3.2.3 Interfacing the GSM shield with Arduino

- First, the Arduino Uno was connected to the Laptop using a USB cable.
- The program was burnt into the microcontroller using the software.
- A SIM card was inserted into the shield and then mounted onto the Arduino UNO board
- The shield and the Arduino board were powered together. GSM shield offered the input to the microcontroller and also picked the output to be sent back to the user

3.2.4 Relays

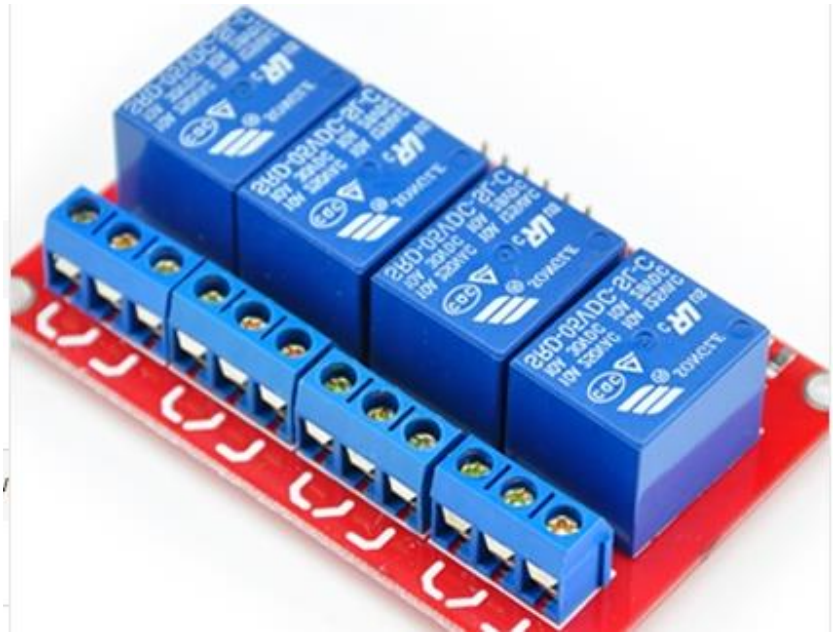

Figure 3:5 Circuit diagram of relays [8]

Relays are electromechanical devices, which are used as a switch. Current flowing through the coil of the relay creates a magnetic field which attracts a lever and changes the switch contacts. The main advantage of using a relay as a switch was that it provided electrical isolation between inputs with the help of magnetic coupling, and also we could handle a large power using a relay. In this project 5V, 4-Channel Relay interface board was be employed, and each one needs 15-20mA Current. It is equipped with high-current relay, AC250V 10A; DC30V 10A. It also features Indication LEDs for Relay output status. Each device to be controlled was connected to one channel which is a relay that can function independently. Hence the device could be turned ON/OFF, and its status monitored independently

3.3 Flow Chart of the System

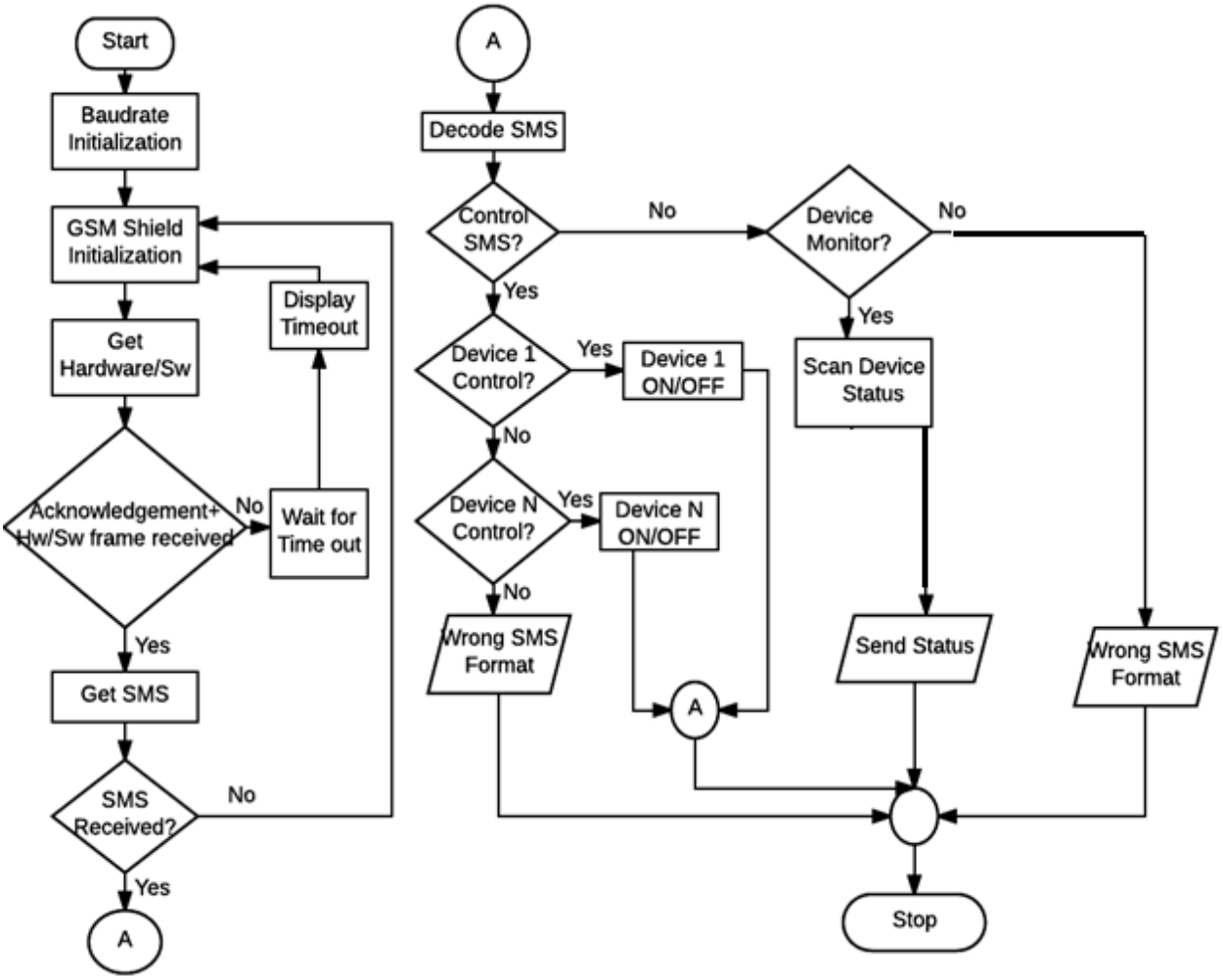

Figure 3:6 The System Flowchart 1

3.4 Operation

A user sends an SMS to GSM module by Mobile; the GSM receives that SMS and sends it to Arduino. Now, the Arduino reads this SMS and extracts the main command from the received string and stores in a variable. The microcontroller checks to ensure that the sender is among the authorized personnel. After this, the Arduino compares this string with a predefined string. If a match occurs, then it sends a signal to relay for turning ON and OFF the electrical appliances or reading their status.

One sends commands like “abc on”, “light off”, “status”, and so on for controlling electrical appliances.

3.5 Main Components of the Project

3.5.1 GSM Technology

GSM is a global system for mobile communication. Today’s second-generation GSM networks deliver high quality and secure mobile voice and data services (such as SMS/ Text Messaging) with full roaming capabilities across the world.

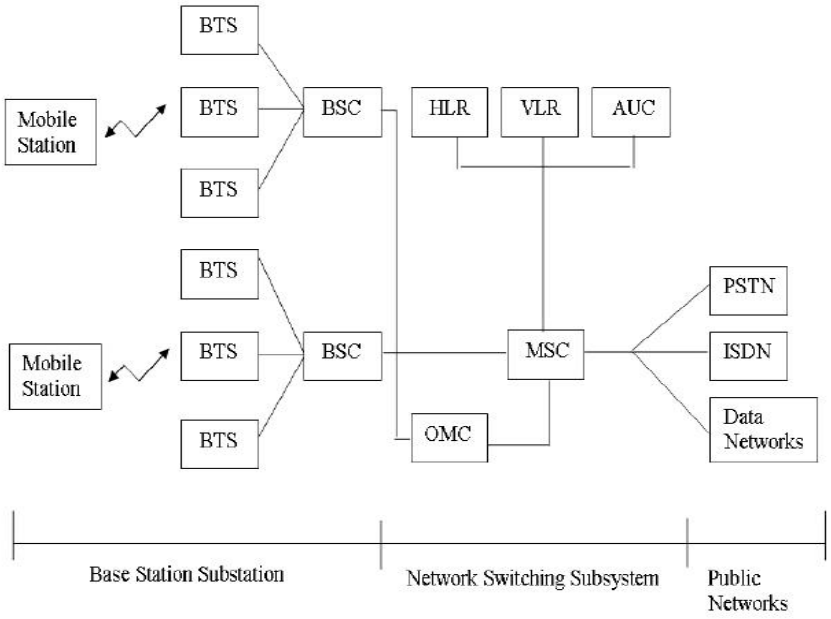

Figure 3:7 The GSM Architecture [11]

3.5.2 Short Message Service

It is a service that enables the sending and receiving of a message between mobile phones or GSM shields. One SMS message can contain at most 140 bytes (1120 bits) of data [12]. Once the message is sent, it is received by Short Message Service Center (SMSC), which must then get it to

the appropriate mobile device. To do this, the SMSC sends an SMS request to Home Location Register (HLR) to find the roaming customer. Once HLR receives the request, it responds to the SMSC with the subscriber's status: Inactive or active and where the subscriber is roaming.

If the response is "inactive," then the SMSC will hold onto the message for a period. When the subscriber access his device, the HLR sends an SMS notification to the SMSC and the SMSC will attempt delivery.

The SMSC transfers the message in a Short Message Delivery Point to Point format to the serving system. The system pages the device, and if it responds, the message gets delivered. The SMSC receives verification that the message was received by the end user, then categorizes the message as "sent" and will not attempt to send again.

SMS provides a mechanism for transmitting a short message to and from wireless devices.The service makes use of an SMSC, which acts as a store and forward system for short messages.One major advantage of SMS is that it is supported by 100% GSM mobile phones.

What Makes SMS Messaging So Successful Worldwide?

SMS is so success all over the world. SMS messaging is now one of the most important revenue sources of wireless carriers. Some of the reasons are discussed below.

- SMS Messages can be sent and read at any time.
- SMS Message can be sent to an offline Mobile Phone.
- SMS Messaging is less disturbing while one can still stay in touch.
- SMS are supported by 100% GSM Mobile Phones, and they can be Exchanged between different wireless carriers

CHAPTER FOUR: RESULTS AND DISCUSSION

4.1 Results

The text-based electrical devices monitoring and control system that uses GSM technology was implemented and functioned well.

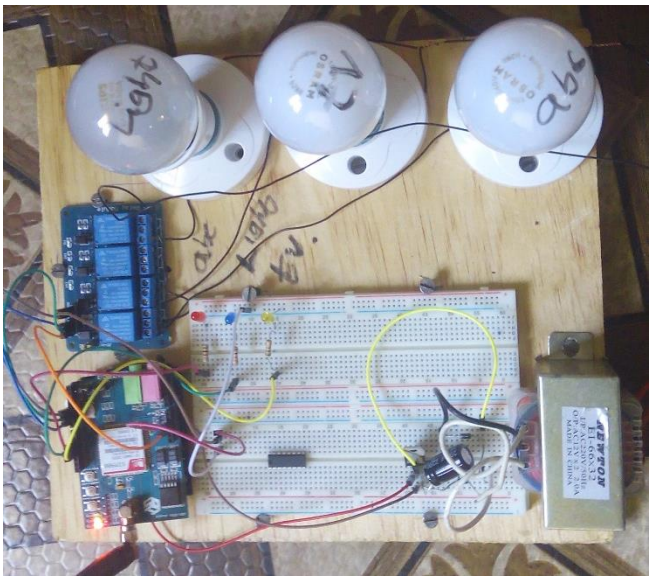

Figure 4:1 A Photograph of the Implemented System

4.1.1 User Authentication

The system was able to verify the legibility of an SMS-sender to operate the system. As per the current programming, the system recognizes only three MSISDN numbers which belong to Kutiri Billezra, Nahshon Mokua and our supervisor, Mr. Solomon Teshome. Any attempt to control the system through a text message from an unknown MSISDN was blocked, and the sender notified via a text message of his illegibility. The two system developers, Nahshon and Billezra, were then notified through a text message of the attempt, the contents of the message and the MSISDN number of the sender as shown in the samples below. This makes the system more secure since two legitimate users can have a glimpse of what an intruder was trying to accomplish and assess the possibility of the intrusion being malicious or just a mistake. This feature also enhanced accountability especially the legitimate users who are solely responsible for the operation of the system and can be held accountable over the devices they control.

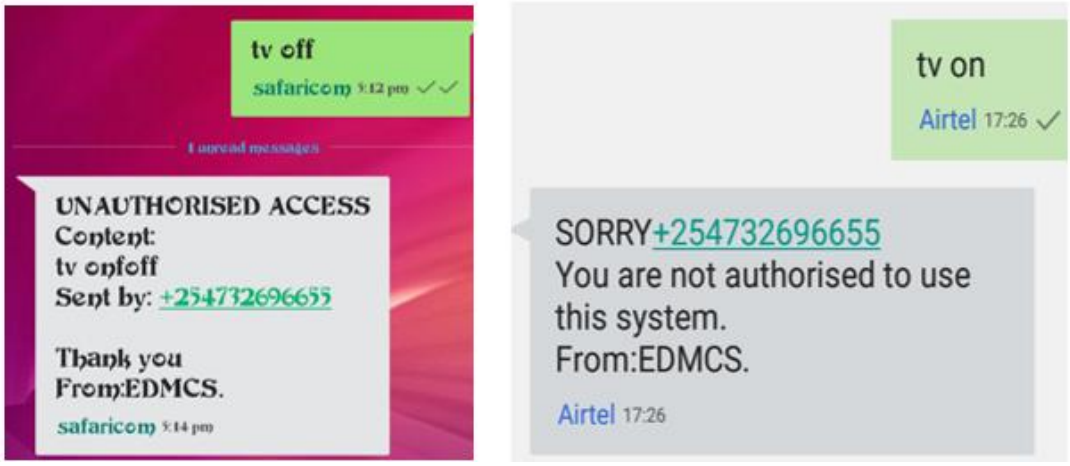

Figure 4:2 User Authentication Sample Report

4.1.2 Control Operations

The legible users could turn devices ON and OFF at will via text messages. Three lamps were connected to the relay, and they signified three loads: a Television set, lights and an arbitrary device called abc. The television set was turned on with an SMS “tv on” and turned off via a message “tv off”. The lights were turned on with a message “light on” and turned off with a message “lights off”. The arbitrary device, abc was turned on by a message “abc on” and turned off via a message “abc off”. It was also possible to turn on all the devices simultaneously via a

message “all on” and turn them off via a message “all off”.

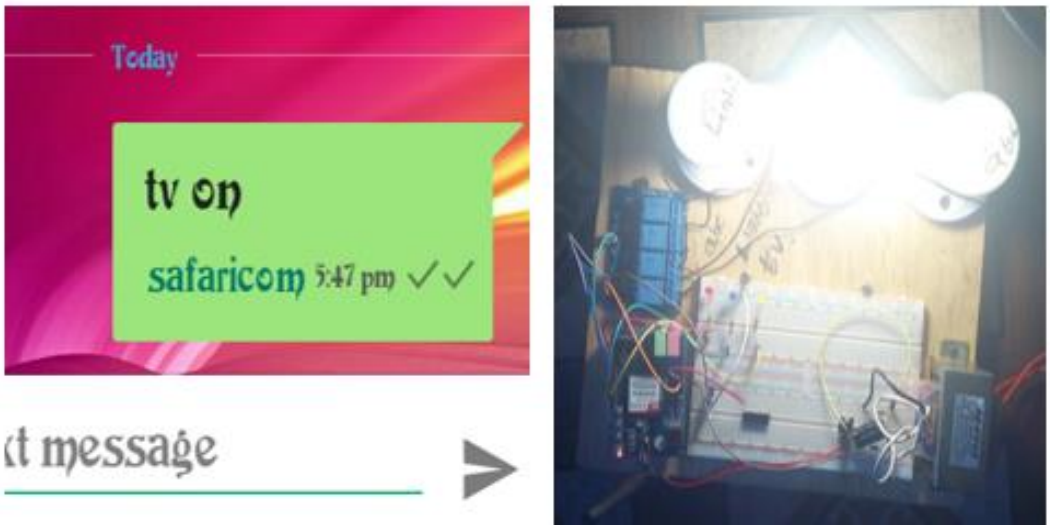

Figure 4:3 Control Sample Operation

4.1.3 Monitoring operations

In this case, the word monitoring is used to mean checking the status of the devices, whether ON or OFF. The legitimate users could get the status of the devices by sending an SMS to the SIM card inserted in the GSM Shield. The content of the message should be “status”. Then an SMS bearing the status of the devices would be sent back to him. The SMS begins with a title: STATUS REPORT. Followed by salutation then the ON/OFF status of the devices as shown by the sample SMS below.

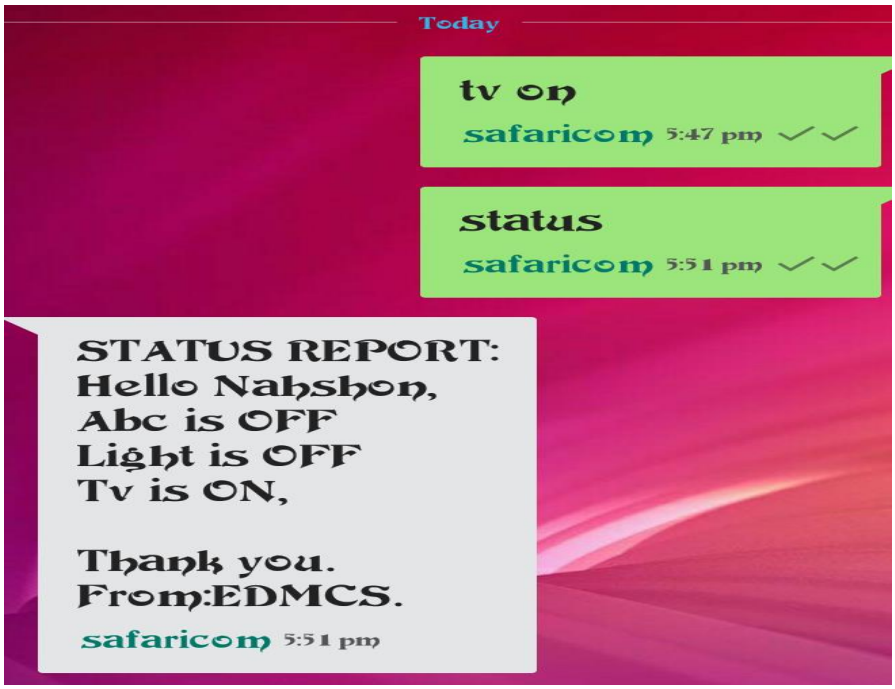

Figure 4:4 Monitoring Sample Operation

4.1.4 The Human Machine Interface

The HMI consisted of the three LEDs that displayed the ON/OFF status of the devices to any onlooker. Each LED displayed the status of a particular device. The yellow LED displayed the status of the television set; the blue LED displayed the lights while the status of the arbitrary device, ‘abc’ was displayed by the red LED.

4.1.5 User friendliness

The system was also user-friendly since it could offer an SMS feedback informing a user when he uses an SMS format not understood by the system. Apart from that, the choice of red, blue and yellow as the colors for the LEDs that form the human machine interface, makes it easy for an onlooker to know which device is on or off. This is because the three colors are easily distinguishable from each other even from a distance irrespective of their position. Furthermore, the message strings are easier to remember since they consist of the device to be operated and the state require.

4.2 Discussion

The system and the loads were powered simultaneously by 240V from a wall socket. The television set, the lights and a third arbitrary load, abc were represented by three lamps for demonstration where each lamp was labeled the device it represents. To turn ON any device, a predefined message string was sent to the MSISDN number of the SIM card in the shield. The messages include “tv on”, “lights on” or “abc on”. To turn off the devices, a predefined message string were sent to the SIM card, and the messages were “tv off”,”lights off” or “abc off”. It was also possible to turn on all the three devices at once using the message string “all on” and to turn them off using the message string “all off”. A wrong message format from an eligible user was met with a response from the system in which the user was notified of the incorrect format of the message string. An attempt from a stranger to operate the system was met with a response from the system in which the stranger was notified of his inability to operate the system, and two of the legitimate users were notified of the attempted operation, the MSISDN number of the sender and the contents of the message which could enable them to figure out the type of operation intended and whether it was malicious or just a mistake. While this system used the three devices mentioned, any other set of devices could be operated remotely with just a simple modification of the program on the Atmega328P. The range could extend to eight devices to maximally use all the pins on the Arduino UNO board and also have enough pins for the human machine interface

CHAPTER FIVE: CONCLUSION AND RECOMMENDATION

This final chapter the conclusion of the entire project and the recommendations made by the system developers for safe, efficient and smooth operation of the system

5.1 Conclusion

This project that was proposed on 3rd August 2016 sought to solve a challenge in the society. The challenge was to effectively control and monitor electrical appliances especially from remote areas. Having successively implemented the system and also working within the schedule, we met our main objective and by extension also met our specific objectives. It is at this point that we conclude that the text-based electrical devices control and monitoring system was well implemented and should be adopted in homes, offices and industries.

5.2 Recommendations

Having successively implemented the system, tested and concluded that it is ready for adoption, the following are the recommendations to ensure smooth operation of the system

The system could be used in offices, homes, and industries. In homes various electrical appliances such as the television sets, lights and fridges can be controlled and monitored. Turning on security lights before getting home can enhance safety at home because driving or walking into a well-lit homestead is safer than walking in a dark homestead. In industries, motor, relays, and conveyor belts can be controlled and monitored to enhance efficiency without wasting energy powering devices when they are not in use.

The SIM card in the GSM shield requires an airtime top-up for it to send status reports, wrong format notifications, unauthorized access notifications and notifications to intruders. However, to lower the operational costs, it is recommended to purchase SMS bundles from any preferred operator and the package would depend on the user's frequency of monitoring the system.

The system in place is made up of electronic components that may be adversely affected by dust, moisture, and mechanical stress. It is our recommendation that the users would place the system far away from these hazardous elements to ensure durability of the equipment

The GSM shield requires a GSM network to operate and therefore it is highly recommended that this equipment be mounted at a place where it can connect to the network easily even if the

electrical devices to be controlled and monitored are in a closed room where the network coverage is poor

The relay module in use is rated at 240V and 10A. It is recommended that the loads connected should not exceed this limit to prevent the module from overheating. In this project, the load section and the rest of the system are powered from the same source. However, this can be changed such that they are powered separately but simultaneously especially if the loads are located far away from the system or for electrical devices powered by DC sources

REFERENCES

[1] Intelecon Research and Consultancy Limited, "ICT Access Gaps Study", Communications Authority of Kenya, Nairobi, 2016.

[2] N. Sriskanthan, F. Tan, A Karande, “Bluetooth-based home automation system,” Microprocessors and Microsystems, Elsevier, vol. 26, pp. 281-289, 2002. Article

[3] H. Karma, N. Wakabayashi, R. Kanazawa, H. Ito, “Home Appliance Control System over Bluetooth with a Cellular Phone,” IEEE Transactions on Consumer Electronics, vol. 9, no. 4, pp.109-1053, Nov. 2003. Article

[4] M. Ryan, “Bluetooth: With Low Energy comes Low Security,” WOOT’13 Proceedings of the 7th USENIX Conference on Offensive Technologies, pp. 4-4, 2013.

[5] Baki Koyuncu, “PC Remote Control of Appliances by Using Telephone Lines”, 1995, IEEE Transactions on Consumer Electronics, Vol. 41(1), pp. 201-209.

[6] L. Muhury, A.H.M.A. Habib, “Device Control by Using GSM Network,” 15th International Conference on Computer and Information Technology (ICCIT), pp. 271-274, Dec. 2012. Article (CrossRef Link)

[7] R.Sasi, “HowI DOS’ed My Bank,” Hack in the Box Security Conference (HITBSecConf2013), Oct. 2013.

[8] M. Gauger, D. Minder, P. J. Marrón, A. Wacker, A. Lachenmann, “Prototyping Sensor-Actuator Networks for home automation,” in Proc.of the 3rd Workshop on Real-World Wireless Sensor Networks (REALWSN 2008), 2008.

[9] S. Willasen, “Forensics and the GSM Mobile Telephone system”, International Journal of Digital Evidence, 2003

[10] S. Singh, “Review on Darlington Transistor for Recent Modern Application”, IJCA, Feb 2015.

[11] M. Moully, “The GSM System for Mobile Communications”, Palasieur, France, 1992

[12] P. Jaiswal, “SMS based information systems”, University of Finland School of Computing Master’s Thesis, Sept 2011

APPENDIX

```
// include the GSM library
#include <GSM.h>
#define AbcRELAY 5
#define LightRELAY 4
#define TVRELAY 6
#define Abc 10
#define Light 11
#define TV 12


// initialize the library instances
GSM gsmAccess;
GSM_SMS sms;

// Array to hold the number a SMS is retreived from
char senderNumber[14];
char str[15];
String StatusMessage, AbcStatus, TvStatus, LightStatus, Unauthorised,UnauthorisedA, WrongFormat;

void setup()
{
 AbcStatus = String("OFF");
 TvStatus = String("OFF");
 LightStatus = String("OFF");
 pinMode(Abc,OUTPUT);
 pinMode(Light,OUTPUT);
 pinMode(TV,OUTPUT);

 LightStatus = String("OFF");
pinMode(Abc,OUTPUT);
pinMode(Light,OUTPUT);
pinMode(TV,OUTPUT);
pinMode(AbcRELAY,OUTPUT);
pinMode(LightRELAY,OUTPUT);
pinMode(TVRELAY,OUTPUT);
delay(1000);
digitalWrite(AbcRELAY,HIGH);
digitalWrite(LightRELAY,HIGH);
digitalWrite(TVRELAY,HIGH);
digitalWrite(Abc,LOW);
digitalWrite(Light,LOW);
digitalWrite(TV,LOW);
 // connection state
 boolean notConnected = true;

 // Start GSM connection
 while (notConnected)
 {
   if (gsmAccess.begin() == GSM_READY)
     notConnected = false;
   else
   {
     delay(1000);
   }
 }
}
```

```
void loop()
{
  char c;
  int i=0;
  int verifier=0;
  int user=0;

  // If there are any SMSs available()
  if (sms.available())
  {
    sms.remoteNumber(senderNumber,14);
    if(!(strncmp(senderNumber,"+254704733509",13)))
    {
      user=1;
      verifier=1;
    }
    else if(!(strncmp(senderNumber,"+254705563266",13)))
    {
      user=2;
      verifier=1;
    }
    else if(!(strncmp(senderNumber,"+254723110591",13)))
    {
      user=3;
      verifier=1;
    }

  }
  else
  {
    verifier=2;
  }
  while (c = sms.read())
  str[i++]=c;
sms.flush();
if(verifier==1)
  {
if(!(strncmp(str,"tv on",5)))
{
digitalWrite(TV,HIGH);
digitalWrite(TVRELAY,LOW);
TvStatus = "ON";
delay(200);
}
else if(!(strncmp(str,"tv off",6)))
{
digitalWrite(TV,LOW);
digitalWrite(TVRELAY,HIGH);
TvStatus = "OFF";
delay(200);
}
else if(!(strncmp(str,"abc on",6)))
{
digitalWrite(Abc,HIGH);
digitalWrite(AbcRELAY,LOW);
```

```
digitalWrite(AbcRELAY,LOW);
AbcStatus = "ON";
delay(200);
}
else if(!(strncmp(str,"abc off",7)))
{
digitalWrite(Abc,LOW);
digitalWrite(AbcRELAY,HIGH);
AbcStatus = "OFF";
delay(200);
}
else if(!(strncmp(str,"light on",8)))
{
digitalWrite(Light,HIGH);
digitalWrite(LightRELAY,LOW);
LightStatus = "ON";
delay(200);
}
 else if(!(strncmp(str,"light off",9)))
{
digitalWrite(Light,LOW);
digitalWrite(LightRELAY,HIGH);
LightStatus = "OFF";
delay(200);
}
 else if(!(strncmp(str,"all on",6)))
{
digitalWrite(TV,HIGH);

digitalWrite(Abc,HIGH);
digitalWrite(AbcRELAY,LOW);
AbcStatus = "ON";
digitalWrite(Light,HIGH);
digitalWrite(LightRELAY,LOW);
LightStatus = "ON";
delay(200);
}
else if(!(strncmp(str,"all off",7)))
{
digitalWrite(TV,LOW);
digitalWrite(TVRELAY,HIGH);
TvStatus = "OFF";
digitalWrite(Abc,LOW);
digitalWrite(AbcRELAY,HIGH);
AbcStatus = "OFF";
digitalWrite(Light,LOW);
digitalWrite(LightRELAY,HIGH);
LightStatus = "OFF";
delay(200);
}
else if(!(strncmp(str,"status",6)))
{
StatusMessage = String("STATUS REPORT:\nHello ");
if(user==1)
StatusMessage += "Billezra,";
else if(user==2)
StatusMessage += "Nahshon,";
```

```
StatusMessage += "\nAbc is ";
StatusMessage.concat(AbcStatus);
StatusMessage += "\nLight is ";
StatusMessage.concat(LightStatus);
StatusMessage += "\nTv is ";
StatusMessage.concat(TvStatus);
StatusMessage += ",\n\nThank you.\n";
StatusMessage += "From:EDMCS.";

// send the message
sms.beginSMS(senderNumber);
sms.print(StatusMessage);
sms.endSMS();
}
else
{
WrongFormat = String("OOPS, WRONG FORMAT:\nHello ");
if(user==1)
WrongFormat += "Billezra,";
else if(user==2)
WrongFormat += "Nahshon,";
WrongFormat += "\nUse message strings recognised by the system and in small letters,\n";
WrongFormat += "\nThank you.\n";
WrongFormat += "From:EDMCS.";
sms.beginSMS(senderNumber);
sms.print(WrongFormat);
sms.endSMS();
}
```

```
    }
    else if(verifier==2)
  {
    char Nahshon[14]="+254705563266";
    char Billezra[14]="+254704733509";
  Unauthorised = String("SORRY");
  Unauthorised.concat(senderNumber);
  Unauthorised += "\nYou are not authorised to use this system.\n";
  Unauthorised += "From:EDMCS.";
  UnauthorisedA = String("UNAUTHORISED ACCESS\nContent:\n");
  UnauthorisedA.concat(str);
  UnauthorisedA += "\nSent by: ";
  UnauthorisedA.concat(senderNumber);
  UnauthorisedA += "\n\nThank you\nFrom:EDMCS.";
  // send the message
  sms.beginSMS(senderNumber);
  sms.print(Unauthorised);
  sms.endSMS();
  sms.beginSMS(Billezra);
  sms.print(UnauthorisedA);
  sms.endSMS();
  sms.beginSMS(Nahshon);
  sms.print(UnauthorisedA);
  sms.endSMS();
  }
  }
  delay(200);
}
```