REMOTE TELECOMMUNICATIONS SITES OVERLAY MONITORING SYSTEM.

by

MWANGI MORRISON GITHINJI (14/04139)

A DISSERTATION

Submitted to

KCA UNIVERSITY

In partial fulfilment of the requirements for the award of degree of

MASTER OF SCIENCE IN DATA COMMUNICATION AND NETWORKS

In the

FACULTY OF COMPUTING AND INFORMATION MANAGEMENT.

September 2016

DECLARATION

I declare that the work in this research project is my original work and has not been previously published or submitted elsewhere for award of a degree. I also declare that this research project contains no material written or published by other people except where due reference is made and author duly acknowledged.

Student Name: **Morrison Githinji Mwangi** Reg. No. **14/04139**

Signature: …….. Date: …….

I do hereby confirm that I have examined the Master's dissertation of

Morrison Githinji Mwangi

And have certified that all revisions that the dissertation panel and examiners recommended have been adequately addressed.

Signature: ……. Date: ……

Professor Patrick Ogao

Dissertation Supervisor.

Signature …… Date …….

Mr. Samuel Matende

Dissertation Supervisor.

ACKNOWLEDGEMENT

I wish to thank the Almighty God for his goodness and mercy upon me and especially for the provision of his grace during the time I undertook this research. Let his name be glorified now and forever.

Special thanks to my supervisors Professor Patrick Ogao and Mr. Samuel Matende whose support, guidance and encouragement was invaluable.

My sincere gratitude to the entire FOCIM department and staff for their contribution to towards the completion of this work.

To my fellow students, thanks for the encouragement and teamwork which has made this work to be completed in time.

Finally thanks to my wife and children for their moral support.

DEDICATION

This work is dedicated to my wife Faith, my son Dennis and my daughters Annette, Ivy and Blessing for standing with me in prayer during this period, and for believing in me always.

ABSTRACT

Mobile telecommunications service providers operate numerous geographically dispersed remote sites for the purpose of increasing network coverage and enhancing signal quality in order to deliver acceptable quality voice, data and internet services to their subscribers.

It is not practical to have all these sites manned by maintenance personnel. In order to improve reliability, it is the norm to provide built in redundancies in these remote sites so that failure of primary equipment results in handover of function to similar secondary equipment. This is normally implemented in the transmission equipment, servers, power and environmental control equipment such as air conditioners.

The most common sources of failure in telecommunications facilities in the remote sites are power failure, environmental control failures and security breaches. Monitoring of these conditions is achieved by use of appropriate sensors to detect failure and/or breaches. Information from these sensors is ferried together with voice and data traffic as an overhead to a central network operation Centre (NOC). The NOC is manned round the clock to ensure conditions at remote sites are monitored and failure information relayed to field maintenance staff through calls and short messages.

The quality and availability of telecommunications service is monitored by communication regulators in most countries and is subjected to service level agreements by customers. Both these situations can be very costly to service providers if violated.

Recovery at remote telecommunication sites is a race against time. In order to attain quick turnaround during failure, alarm information must reach the field maintenance staff within the shortest time possible. Alarm routing through the NOC normally faces avoidable delays.

In this research, an overlay monitoring network is designed to monitor alarm information at remote telecommunications sites and relay the same directly to the field response staff. This overlay network is designed as an artifact using a sensor network and a microcontroller as the intelligent device. Alarm information is relayed to relevant response teams directly through the use of text messages. Where total telecommunications failure may affect network to the GSM unit in the artifact, a SIM card for a different operator can be used instead.

TABLE OF CONTENTS

LIST OF FIGURES

1. INTRODUCTION

1.1 BACKGROUND OF PROBLEM

With the advent of the broadband technology and the mobile networks, the communications infrastructure requirements changed fundamentally. Additionally to a rather constant number of head offices, there are a constant growing number of geographically distributed middle and small plants i.e. Remote digital line units (RDLU), in wire line networks and Base Transceiver Stations (BTS) in wireless or mobile networks. Although in the predominant number of these plants no constant skilled personnel are present, there is mostly no highly developed remote monitoring for these installations. (Schmerbeck, 2005). The structure of the remote telecommunications plants essentially is determined by the requirement of a high degree of availability and security. Construction of the distributed telecommunications network installations which is in or close to inhabited areas with adequate public mains supply is quite different to self-sustaining isolated network installations.

Installations which lie within inhabited areas will in most cases be served from the commercial grid. To guarantee supply during AC mains failure, diesel electric generators (DEGs) are normally used as alternate AC generators. These, together with direct current (DC) batteries also referred to as Uninterruptible Power Supply (UPS) with sufficient capacity to energize the telecommunications equipment for several hours.

Off grid sites will in most cases be equipped with a dual engine generator set which run alternately changing over after a predetermined run period like two weeks or in case there is failure in one. The dual set allows for alternate routine maintenance of these sites as one holds when the other is

on maintenance. Care must however be taken to ensure both are in good working order at all times to ensure AC supply.

Dependent on climatic conditions, these sites will be equipped with air conditioning systems to minimize the danger of breakdown caused by out of range temperature or humidity conditions.

Additionally, door contacts; smoke detectors and other intrusion sensors ensure detection of disturbance and failures.

The status of these monitored conditions are indicated by means of an alarm system which forwards the conditions to a Network Operation Centre (NOC). These alarms are usually condensed due to a limit on no of alarm lines available in the telecommunications system and classified as major or minor alarms. The team dispatched to site to check on the alarm will have to troubleshoot the exact problem once they get on site. This means that the team must be composed of diverse specialization in order to handle whatever cause of failure at site. The ferrying of alarm information on the telecommunication system increases overheads and reduces the payload of the system. Additionally since the alarms are relayed to the NOC, response time to these alarms will depend on the NOC monitoring team and the time taken to notice and alert the field teams.

Due to increasing demand for quality telecommunications services and the ease of rolling out mobile as opposed to landline services, the former has enjoyed immense growth opportunities. The number of mobile services remote stations continue to grow steadily as the demand rises. This growth has been accompanied by the need for a more elaborate maintenance of these installations to ensure availability of services to customers. Most mobile telecommunications service providers have resulted in demarcating their coverage areas into regional maintenance entities to enhance response to failures and to create network ownership to regional maintenance staff. With this also

comes the need to devolve network monitoring systems to the regional level without necessarily building fully functional network operating centers (NOCs).

The network operation center (NOC) handles network surveillance, traffic management including traffic monitoring & analysis and signaling management. Network surveillance includes network supervision and furnishing operations staff with overall view of the network elements (NEs) and network processes that comprise the network including switching, transport and signaling. (Misra, 2004). The network surveillance aspect of the network operation center is critical as it provides the overall visibility of the telecommunications network. As mobile telecommunications remote sites continue to grow thus increasing the total count of network elements, the need to partially devolve this surveillance to regional units rises. Since the network operation center is the one charged with the management of the overall health of the network, it must not lose visibility in this devolution, since it still has to come up with all the necessary statistics on overall network availability.

There is need however to have a system that can handle regional network surveillance and report directly to the regional maintenance staff. Such a system can be deployed as an overlay to the existing NOC system to enhance operations and relieve the NOC of this primary responsibility.

A majority of the frequent failures that affect remote telecommunications facilities are environmental and supply power related. The ten top alarms in a remote telecommunications facilities are:

a) Fire

A fire alarm is detected from the heat and smoke emanating from the fire. Heat and smoke detectors are used for this detection. In most installations a fire alarm triggers the sprinkler system and alerts the emergency response team. Remote telecommunications sites are fitted with smoke detectors. Additionally the temperature levels are normally preset and any out of range temperatures detected and reported to the network operation center.

b) AC Failure

The AC power failure alarm will be raised when the commercial AC power fails or ceases to be the primary source of power to the telecommunications equipment. Power supply is transferred to the backup sources i.e. the AC Generator and the UPS. This alarm will be raised due to commercial grid power failure and will normally be reset when power resumes.

c) Generator Failure

This alarm will occur when the generator which is the first backup source fails or ceases supply of power to the telecommunications equipment. Supply of power is then transferred to the UPS. Where the station is connected to commercial grid power, a generator failure alarm means the loss of two essential power supply sources to the remote site. This means that there is loss of commercial power and the standby diesel engine generator has failed to kick in. Alternatively, the generator can fail if the commercial power loss persists and the diesel used to run the generator runs out.

d) Rectifier, Fuse or Circuit Breaker Failure

These alarms will occur when one of these power supply equipment fail to supply AC power to the telecommunications equipment. The rectifier receives AC power from either the mains or the generator during mains failure, converts it to direct current (DC) which is supplied to the equipment and also provides charging current to the UPS. Telecommunications equipment normally operate on direct current from the rectifier. If there is a rectifier failure then the telecommunications equipment begins to draw the source power from the battery banks at site. This means that the standby batteries go to a discharging mode. This is normally the last supply line of power to the equipment and the length of time it can hold depends on the capacity of the bank and the total equipment load.

e) ATS Failure

In the event of a commercial grid power failure, the supply of alternating current (AC) is transferred to the standby diesel engine generator at the site. This alarm will occur when the automatic transfer switch (ATS) fails to switch the AC power supply from the commercial AC power to the AC generator. This alarm will manifest as a mains and generator failure and supply of power to the equipment will be transferred to the UPS.

f) UPS Failure

This alarm is raised when the second and ultimate backup source, the UPS (or batteries), fails or stops supplying power to the telecommunications equipment. A telecommunications service

outage then ensues. This normally happens when loss of the primary supply sources persist beyond the time that the battery bank can hold. This failure means that the UPS or batteries have totally discharged and there is no more direct current power to run the equipment. It is normally the practice to design the power budget to ensure that this ultimate back up source can hold the site for the duration that will be taken for the power response team to get to site and install a temporary back up source such as a mobile generator to hold the site as they troubleshoot on the site power supply systems.

g) HVAC Failure

This alarm will be raised when the heating, ventilating or air conditioning systems fail to function at preset values. Telecommunications equipment normally operate in defined temperature ranges. Since the equipment components also dissipate a lot of heat, telecommunications equipment is normally housed in air conditioned sheds or outdoor shelters which are well ventilated to ensure that heat does not accumulate to trigger a malfunction of the equipment or even precipitate a fire. This temperature ranges are monitored by suitable equipment and out of range temperatures reported for appropriate response and action.

h) BOD (Battery on discharge)

This alarm is raised when telecommunications site standby UPS system is in a discharge mode. This is an indication that the site is on the last power resource and complete discharge will lead to site outage. In most remote sites the UPS is designed to hold the site between four to Eight hours to allow for intervention on the first and second AC suppliers. The length of time the UPS will hold will depend on its capacity and the electrical load at the station.

i) High/Low Temperature –

This alarm is raised when the temperature in the telecommunications facility crosses the maximum or the minimum threshold values. In telecommunications facilities within the tropics with predominantly high temperatures, most sites are fitted with air conditioning systems or are housed in well ventilated shelters to keep temperatures within range. Failure of these air conditioning or ventilating systems will result in high temperature at site which may result in equipment malfunction, component damage and at worst a fire eruption.

j) Intrusion

An intrusion alarm will be raised if a locked door is opened without authorized access or if an unauthorized person is found within the telecommunications facility. Intrusion detection will normally be done by use of appropriate intrusion detection sensors such as motion sensors and vibration sensors. Unauthorized persons normally access remote telecommunications facilities to vandalize the unmanned sites. Most telecommunications service providers continue to suffer losses in the remote sites due to theft of diesel fuel and vandalism of critical equipment such as generators and air conditioning equipment. This has led to outsourcing of security to quick response units backed up by the police force. Intrusion detections will normally be detected at the network operation center and a distress call raised to the appropriate security team. In order to avoid false alarms when authorized staff access these facilities, appropriate access procedures are incorporated that ensure that the network operation center is informed of such access or suitable access codes are used to disarm the alarm systems for the duration that the authorized staff are on site. This is achieved by use of a text message log in procedure.

1.2 CAUSES OF PROBLEM IN RESEARCH AREA

a) Alarm handling in remote unmanned telecommunications installations is accomplished by aggregating all the alarms and forwarding them through the telecommunication channels as an overhead to the Network Operation Centre (NOC). Since there are a limited number of available alarm lines in the system, different alarms are combined and classified either as major or minor alarms depending on the impact on the network. Further troubleshooting is therefore necessary either on or offsite to narrow down on the exact cause of the alarm. The aggregation is necessitated by the need to preserve bandwidth for payload data. A lot of time would be saved if different common and critical alarms would be detected and transmitted discreetly to enable direct response from the appropriate field response units. This will ensure any alarm occurring at the remote site is uniquely identified immediately and is routed directly to the appropriate response person. This will cut any delays associated with the current alarm monitoring systems.

b) The main challenge with recovering from remote site failures is a race against time. There are several challenges in the accomplishment of quick and effective turnaround. If the central Network Operation Centre (NOC) receives an alarm but cannot quickly identify or notify the most appropriate resource to fix the problem valuable time will be lost. These lapses at the network operation center cannot in most cases be accounted for during performance audits and no particular department can own up to poor response as information conveyance delays are difficult to lay on either the NOC or the operations department. Further without remote diagnostic tools problems cannot be

prioritized. Every problem is assumed to be major hence time is lost on the most critical problems. (Westell, 2015). A lot of time would be redeemed if alarm information is delivered directly to the resources that are charged with service restoration. This way, alarm information will be available to the field response units in real time and response will be greatly enhanced.

c) The time taken to travel to remote telecommunications sites normally averages one hour to most remote sites but can run to three hours or more in rural locations which usually have accessibility challenges. This may be further compounded by traffic and weather conditions. In some cases multiple technical teams are even sent to separate sites just to determine where the root cause of the problem is located. Remote sites maintenance further constitutes a substantial portion of operations budget. It is desirable that any fault arising at these remote stations is handled by the appropriate team without duplicating response teams which will exacerbate costs. By distinguishing various alarm types and directing to the appropriate resource, valuable time may be saved and downtime shortened if not avoided altogether.

d) Hardware failures mostly associated with environmental factors contribute to 55% of all remote station failures. Such failures include power and air conditioning failures and communications equipment failure. Remote unmanned stations design normally incorporate several levels of redundancy of various components, such as multiple power supplies, network controllers and hard drives. However even with this level of protection, like any other disaster, an air conditioning equipment might fail on a hot

day, an unforeseen event may trigger a widespread power outage, or rodents may damage vital wiring in the equipment room. (Institute, 2013). All these possibilities may precipitate an unexpected network outage. Hardware failures will necessitate a site visit. By raising appropriate alarms to appropriate teams site visits will only be done by the appropriate teams.

e) In conventional systems, the health of the network is managed from the central NOC. If there is a central failure in the NOC that inhibits monitoring of external remote station alarms, then telecommunications sites may be lost and alarm information may not be immediately available for appropriate response. Such an eventuality will result in the network elements being invisible to the network surveillance team. At such times other failures in the network may go unnoticed resulting in unexpected losses. By devising a method where alarms can reach the field resources directly, such an eventuality will not arise.

f) By designing failure alarms to reach the field resources as they occur, we can keep track of network failures when and where they occur. This increases maintenance efficiency and reduces the likelihood or duration of network downtime. The overall turnaround time on maintenance will be therefore shortened. Further there will be optimization of maintenance costs to ensure that all trips made to remote stations are both necessary and cost effective.

1.3 PROBLEM STATEMENT

a) The design of telecommunications infrastructure is done such that remote unmanned station alarms are routed to the network operating center (NOC) where monitoring staff keep field response resources updated on sites that need to be attended due to failures; the NOC therefore acts as the nerve center for telecommunications service providers and is manned round the clock. Inevitably, valuable time is lost in the process of relaying information from the time it's captured to the time the field response team is raised which may occasion prolonged downtime. Alarm information should ideally be routed directly to the field response staff to facilitate quick response which is the essence of telecommunications networks maintenance.

b) Remote site alarms are aggregated into few alarm lines to the NOC and classified as critical, major or minor depending on severity. This is due to the limited bandwidth availed to overheads in order to create more space for payload voice and data traffic. Further troubleshooting has to be carried out either on site or off site to narrow down to actual failures. By routing this information directly to the field response resources, each alarm can be configured to reach the appropriate resource and therefore obtain the correct response to forestall failure or prolonged downtime.

c) By centralizing alarm handling to the NOC, the network becomes vulnerable to central failures rendering the network invisible to the monitoring teams. The network operation center (NOC) normally maintains visibility of all network elements (NEs) and raise appropriate trouble tickets for any fault on the telecommunications network. It is these

trouble tickets which are assigned to field response teams. Failures in the NOC equipment can hinder reception of alarm status information from remote sites thereby leading to remote failures going unattended. By routing alarm information directly to the field resource teams, we offload the primary monitoring load from the central NOC and improve overall response efficiency.

d) Field telecommunications alarm response resources normally operate round the clock to make the network resources available to users who normally subscribe to service level agreements of 99.99% availability or higher. By having a direct line of communication between the remote sites and the response team ensures that the service level agreements are not violated as overall response efficiency goes up and downtime consequently reduced or eliminated altogether thus ensuring revenue to the service provider. (Telford, 2007)

e) Telecommunication companies normally outsource non-core functions such as Security, Power & Air conditioning. Assignment of tasks to these outsourced resources is normally done through the network operations center (NOC) who will normally raise trouble tickets and assign these contracted firms. Response and recovery time is a major key performance indicator (KPI) between the telecommunications service provider and the outsourced entity and is dependent on the between the NOC and the contracted party. By generating system failure alarms directly to these contracted field response resources, assignment of tasks will happen in real time. This therefore means that monitoring and evaluation of these key performance indicators (KPIs) will ease considerably.

1.4 DEFINITION OF TERMS

a) **Base Transceiver Station (BTS) –** A base transceiver station (BTS) is a piece of network equipment that facilitates wireless communication between a device and network. This is the equipment normally deployed in mobile remote telecommunications facilities and enables the wireless communication between mobile service subscribers. Communication between the base transceiver station and the master switching equipment can be carried by high capacity backhaul microwave radio or optical fiber cable system

b) **The Remote Digital Line Unit (RDLU)** -provides the ability to locate the port sections of the switching system at a remote site. It can be equipped with its own batteries and chargers and can be located up to 30 miles from the switching equipment. The RDLU is designed to operate in hostile ambient temperature environments, so installation in an equipment closet is acceptable. This is the remote telecommunications facility for wire-line services.

c) **Alarm-** A visual or audio notification of deviation in preset parameters in the operation of an equipment. In remote telecommunications services alarm information at site must be ferried to the network surveillance team mostly as an overhead to the payload telecommunications traffic.

d) **Direct Current (DC) -** is the unidirectional flow of electric charge. Direct current is produced by sources such as batteries, power supplies, thermocouples, solar cells, or dynamos. Telecommunications equipment operate on direct current which is obtained by rectifying the source alternating current supply.

e) **Alternating current (AC) –** This is an electric current in which the flow of electric charge periodically reverses direction, as opposed to direct current whose flow of electric charge is in only one direction. Sources of alternating current include the commercial grid and AC generators. AC power is the main power supply to telecommunications equipment and is normally fed to the equipment through a rectifier.

f) **Rectifier –** A piece of equipment used to transform alternating current to direct current to be supplied to the telecommunications equipment.

g) **Uninterruptible power supply (UPS) -** This is an electrical equipment that provides emergency power to a load when the input power or commercial grid power fails. The UPS will normally hold the equipment during transition from commercial grid power to diesel engine generator power which in some cases can run into a minute. The UPS can supply power to the equipment in the event of other sources failure for a duration enough to work on and restore the primary sources.

h) **Automatic transfer switch (ATS) -** An equipment designed to sense the loss of commercial grid power and transfer generation of AC power to the standby generator which will automatically switch on and start generation once commercial power fails. The ATS will sense and transfer supply back to commercial power once it resumes and switch off the standby generator.

i) **Network Operation Centre (NOC) –**is a place from which administrators supervise, monitor and maintain a telecommunications network. The NOC handles network surveillance, traffic management including traffic monitoring & analysis and signaling management. Network surveillance includes network supervision and furnishing

operations staff with overall view of the network elements (NEs) and network processes that comprise the network including switching, transport and signaling.

j) **Telemetry-** is the automatic measurement and wireless transmission of data from remote sources. In general, telemetry works in the following way: Sensors at the source measure either electrical data (such as voltage or current) or physical data (such as temperature or pressure). These measurements are converted to specific electrical voltages. A multiplexer combines the voltages, along with timing data, into a single data stream for transmission to a remote receiver. Upon reception, the data stream is separated into its original components and the data is displayed and processed according to user specifications.

k) **Simple Network Management Protocol** (**SNMP**) **-**is an Internet-standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.

1.5 STUDY AIMS AND OBJECTIVES

1.5.1 AIM OF THE RESEARCH

The aim of this research is to improve the response of field response teams to network and security failures in remote unmanned telecommunications sites by offering an alternate report mechanism implemented as an overlay to existing systems in order to either forestall failure or reduce prolonged outages where network or security failure has already occurred.

1.5.2 OBJECTIVES OF THE RESEARCH

a) Identify critical security and network failures that affect remote unmanned telecommunications stations and which need to be transmitted directly to appropriate response teams.

b) Identify suitable sensors to capture these network failures and security breaches and generate appropriate alarms which can be transmitted to remote locations in order to alert response teams.

c) Design an alarm reporting system to transport this alarm information from the sensors to the target response teams using a microcontroller system coupled with a GSM module.

d) Develop a suitable program code for the developed artifact to enable the alarm information to be transmitted directly to the appropriate response team through customized short messages (SMS).

e) Implement this alarm reporting system as an overlay over the existing conventional alarm system to enable transmission of network failure and security breaches alarms directly to appropriate response teams.

f) Test and simulate the entire system to ensure the objectives are realized and that it has functioned as expected.

1.6 SIGNIFICANCE OF THE STUDY

a) When implemented the system will greatly improve supervision of remote unmanned stations by availing alarm status information to the relevant standby response teams thereby improving the response time. Due to the regional structure of most telecommunications service provider's maintenance organization, it will be possible to route alarm status information on facilities within a region to the relevant personnel manning that region thus enhancing smooth and effective maintenance of telecommunications facilities within the region. The security of the remote stations will especially be enhanced as the time taken to attend to an intrusion detection will be significantly shortened. Response units can also proactively poll parameter status on remote sites under their jurisdiction.

b) Due to the discrimination between various alarms and corresponding response teams, only the appropriate team for the specific required response will be raised thereby cutting cost on multiple teams attending to same alarm. This will free up much needed resources to attend to relevant failures in other parts of the network. Due to the high cost of running field response teams, a response team will normally be assigned a substantial number of stations which are geographically scattered. Movement between these sites has cost implications due to fuel used and time taken on transit. These costs will be significantly brought down when only the necessary journeys by the appropriate teams are undertaken. Field maintenance staff also suffer a lot of fatigue due to maintenance demands on the stations under their jurisdiction. Discrimination of the alarms will therefore allow the teams more free time between calls as they will only attend to alarms which are proper to them.

c) As field teams will be raised directly from the remote stations, NOC staff will be relieved of some of the pressure of being the primary fault occurrence sources and will now play a follow-up role to the field response teams. Network surveillance is only one of the many responsibilities that a network operations center undertakes. Since this is an overlay system, the same information will still be available to the NOC for the purpose of generating network performance reports which will help in performance evaluation of field response teams as well as monitor the key performance indicators agreed upon between the telecommunications service providers and companies outsourced to maintain none core activities such as power maintenance and provision of security services.

d) By implementing the overlay monitoring system, the telecommunications companies will be able to meet customer service agreements due to the improved response to failures. Telecommunications clients subscribe to service level agreements in the range of 99.9%. Apart from hedging against failure by introducing built in redundancies in the telecommunications equipment, it is imperative that any level of failure, even of redundant equipment is remedied with speed in order to maintain this availability. Failure to meet this stringent agreements normally results in a surcharge of rebates to customers, increases the churn rate and can result in fines from the telecommunications network regulator.

e) In the event of central failures that may affect the network operation center resulting in the inability to monitor network elements, the overlay monitoring system will act as a back up to the central network alarm information. The overlay system will ensure that network monitoring function and maintenance of the network continues even when

NOC operations are down. The overlay system can also be designed using SIM cards for different operators to ensure that even in the event of failure in the mobile services for the monitored network, alarm information will still be available over alternative mobile network through merely subscribing as ordinary users of the alternative network.

2. LITERATURE REVIEW

2.2 STATE OF THE ART IN MONITORING REMOTE TELECOMMUNICATION STATIONS

There whole world continues to experience an unprecedented growth in the telecommunications industry. The rapid evolution of new and advanced technologies, the offering of a broad range of voice and data services, and the ever increasing need by all for fast access to information are some of the factors that have contributed to a tremendous increase in the number of subscribers to telecommunication services. This turn of events has imposed huge demands for capacity and quality on telecommunications networks of both public and private operators. In order to keep up with this ever increasing demand, telecommunications operators are expanding and modernizing their existing infrastructure at a fast pace. Liberalization of the telecommunications industry has further led to the emergence of private service providers, a situation which has created healthy competition within the industry. In order to grow and increase their customer base, telecommunications service providers have been forced to offer good quality of service at a competitive price. (Hajela, 1996)

A lot of people around the world now extensively use mobile devices and therefore the demand for reliable, high capacity networks is on an all-time high. Apart from voice calls, most users are now heavily using mobile applications with a high demand for mobile data connectivity. Extensive availability and capacity are therefore a major challenge for telecommunications service providers. In order to meet this high demand from their clientele, telecommunications service providers have to take due care of central network elements (NEs) i.e. Base transceiver

stations (BTSs). The state of art in ensuring network elements (NEs) availability is to enable a real time monitoring of on-site technical equipment and energy availability. (Azeti, 2016).

To ensure availability of demand on mobile services, telecommunications service providers have invested in unmanned geographically spread sites remote from the central office. In order to ensure availability of service in these remote stations, any equipment, energy or security failure that may occasion service outage must be detected early and transmitted to the monitoring stations for appropriate intervention. There are two main methods in use currently to transport network and security failure alarm information between the remote unmanned stations and the manned central monitoring stations also known as Network Operations Centers (NOC).

a) TELEMETRY

Telemetry is defined as the automatic measurement and wireless transmission of data from remote sources. In general, this is how telemetry works: Sensors at the source measure either electrical data such as voltage or current or physical data such as temperature or pressure. These measurements are converted to specific electrical voltages by the use of appropriate transducers. These voltages are then combined by use of a multiplexer, together with timing data to enable coherent recovery, into a single data stream for transmission to a remote receiver. Once received, the data stream is separated into its original components and the data is displayed and processed according to the user specifications. (Winters, 2005).

When used in telecommunications systems, transmission of this remote data utilizes the existing communications links that carry voice and data traffic, as an overhead to this payload. In the normal digital regeneration systems, the telemetry channel uses overhead bits on one

signal channel. These bits are available through digital multiplexing schemes. In remote telecommunications site monitoring, telemetry bits are multiplexed together with voice/data communications channels as an overhead. One disadvantage of using telemetry and multiplexing the bits with the payload data is that loss of transmission also affects the remote sites monitoring. (John. L. Zyskind; Jonathan A. Nagel & Howard D. Kidorf, 2006).

The transportation of alarm information using telemetry systems is accomplished by connecting the sensor network at the remote site to a Remote Telemetry Unit (RTU); this is a small computerized unit, located in the remote site. The main function of this unit is to gather data from sensors and send it to the main computer or, conversely, to send control commands from main station to controllers at the remote site in order to actuate commands remotely. Besides, RTUs can perform routine local device manipulation. (Aistė Andrijauskaitė et al, 2009)

In some cases remote telemetry systems are incorporated in more elaborate Supervisory Control and Data Acquisition (SCADA) systems. A SCADA system performs four main functions: data collection; networked data communication; data presentation and control. These functions are performed by four SCADA system components; Sensors (digital or analogue) and controllers that are directly associated with the managed system; Remote Telemetry Units (RTUs) and SCADA master units, this is the main computer station consisting of few to several main computers that serve as the central processor of SCADA system; these units allow operators to monitor system events and manage control by analyzing received data; sometimes these units are called Human-Machine interface (HMI) or Human-Computer interface (HCI). Data communication network connects master SCADA units with Remote Telemetry units. The simplest SCADA system can be figured as a single circuit that notifies

only about one event. A real SCADA system can perform much more actions and monitor much more remote sites in longer distances, but the main principle remains the same. (Aistė Andrijauskaitė et al, 2009).

b) SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP) TOOL

Simple Network Management Protocol (SNMP) is an application layer protocol defined by the Internet Architecture Board (IAB) in RFC1157 for exchanging management information between network devices. It is a part of Transmission Control Protocol/ Internet Protocol (TCP/IP) protocol suite. SNMP is one of the widely accepted protocols for management and monitoring of network elements. Currently, most of the professional grade network elements come with bundled SNMP agent. These agents have to be enabled and configured to communicate with the Network Management System (NMS). (OpManager, 2016)

SNMP comprises of a management system which is a separate entity that is responsible for communicating with the SNMP agent enabled network devices. This is normally a computer that is used to run one or more network management systems. The SNMP management system key functions include: Querying agents; getting responses from agents; setting variables in agents and acknowledging asynchronous events from agents.

A managed device or the network element is a part of the network that requires some form of monitoring and management such as routers, switches, servers, workstations, printers and UPSs.

The SNMP agent is a program that is incorporated within the network element (NE). Enabling the agent software allows it to collect the management information database from the device

locally and makes it available to the SNMP manager, when it is queried for. The main functions of the SNMP agent are: Collecting management information about its local environment; Storing and retrieving management information as defined in the management information database; signaling events to the manager and acting as a proxy for some non–SNMP manageable network node. (OpManager, 2016)

Use of an SNMP monitor enables monitoring of network performance, auditing of network usage, detection of network faults, or inappropriate access. The SNMP monitor can communicate and interact with any SNMP-enabled device.

Since most sensors are not SNMP enabled devices, an SNMP device is installed in the remote site to provide a suitable interface. However some devices such as IP cameras are SNMP enabled and can be centrally monitored via an SNMP server.

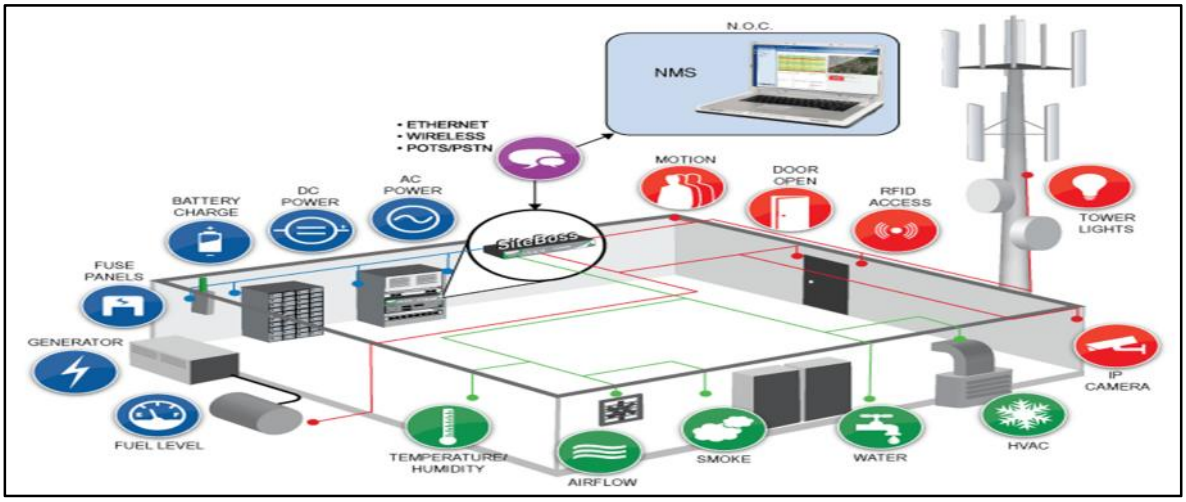

Fig 2.1. Remote site management using SNMP tool-Photo by Assentria (*http://www.asentria.com/solutions/passive-monitoring-power.aspx*)

2.3 STATE OF PRACTICE IN MONITORING REMOTE TELECOMMUNICATION STATIONS

a) REMOTE TELECOMMUNICATIONS SITES MONITORING IN KENYA

A GSM Association (GSMA) and International Finance Corporation report showed that Kenya had a total of 5,565 BTS in 2014. Out of the total about 75% are connected to the commercial grid power supply and the remaining 25% base station sites are off-grid and are located in areas without access to grid power infrastructure. (Adepetun, 2014)

Power issues constitute the greatest challenge in remote mobile base stations maintenance and is the major cause of telecommunications service outage. For remote sites that are off-grid, service providers have had to install dual diesel engine generators per site to ensure round the clock AC power generation. The dual set-up runs alternately changing over after every fortnight.

Safaricom Ltd has 13% of all their remote base stations in off-grid areas. Of these sites 10% are on 24/7 diesel engine generator power while 3% are on renewable energy hybrid systems. The BTSs on 24/7 generator support consume 70% of the diesel fuel that the company uses in remote sites back-up. There has been emphasis to shift towards greener cleaner power in order to reduce on generator running time and associated carbon emission. (Mukunzi, 2011)

According to the quarterly report by the Communications Authority of Kenya (CAK), the uptake of mobile services in Kenya continued to grow during the first quarter of the 2015/16 financial year between July and September 2015. According to the quarterly sector statistics report by the Communications Authority of Kenya (CA), at the end of the quarter, mobile

penetration stood at 88.1per cent with 37.8 million subscribers up from 36.1 million in the previous quarter. (Communications Authority Kenya, 2016)

Mobile service providers in Kenya employ a telemetry system to monitor their remote telecommunications sites. This entails the installation of parameter sensors in every remote site to monitor all the parameters of interest. Alarm information from these remote sites is aggregated and sent as an overhead through the voice and data backhaul circuits to the Network Operation Centers which act as the nerve centers for these service providers. Network operations center (NOC) staff monitor this alarm information on the remote network elements and send out notifications to the field response teams to attend to network issues within their jurisdiction. Notification on failures is normally done through voice calls from the NOC accompanied by broadcast text messages to all relevant persons. Provision of access to remote stations is done through the NOC by provision of unique log on codes to the various remote sites which are uniquely coded to ensure that persons requiring access log in and only enter the requested sites for which access has been provided. Such log on credentials are accompanied by trouble ticket numbers to verify what work is to be done at the remote sites. Once work at site is completed, the authorized personnel then log off and leave the site. The log off system will only accept to clear the outgoing officer after the monitoring systems ascertains that there are no active alarms that have triggered from that site during the period the officer was on site.

Mobile service provider Safaricom LTD had 2500 unmanned remote base transceiver stations by 2011. Safaricom like other mobile telecommunications service provider deploys a remote site monitoring system consisting of sensor network to monitor various site and equipment parameters. The parameters monitored include Power, Fuel, Security, HVAC and access management. (Mukunzi, 2011)

Telecommunications service providers normally outsource maintenance of non-core functions such as Power, Security and Heating Ventilating and Air conditioning (HVAC) issues to more specialized facility providers such as security companies and diesel generator maintenance companies. This enables them to concentrate their field operations on transmission and core network maintenance. Assignment of tasks to these third party companies is handled through the NOC which also monitors their performance in accordance to agreed parameters or key performance indicators.

This centralized telemetry system has a few draw drawbacks in that loss of primary transmission to the remote site will effectively cut off transmission of alarm information resulting in total site black out and inability to determine cause of failure. A situation may then arise where the network elements are no longer visible to the network operations center. This may necessitate sending several teams to site to ascertain cause of failure. Centralized systems are also vulnerable to central failures. If there is a central failure at the NOC alarm information dissemination to response teams will be affected. Such failure may include SMS server failure, alarm system server failures et al.

Allocation of trouble tickets and assignment of tasks to third party contractors does not happen in real time. Delays in human intervention in transmission of critical failure information may lead to contention during performance evaluation. In a system where fault allocation and trouble ticket issuance happen directly from the remote sites and in real time, fault recovery time improves considerably. The assigned resources are able to get to site in a timelier manner. Performance evaluation can then also be carried out on fault occurrence time and not on fault reporting time.

b) CLOUD BASED SOLUTIONS

Cloud based solutions entail the use of an internet gateway at the remote site. The gateway connects to the equipment at the remote site through a serial, Ethernet or input/output (I/O) connection. The gateway sends alarm status information through the internet to a cloud based data center. Alarm information is retrieved by logging in to the center through an appropriate universal resource locator (URL).

The cloud based solution enables fault management by availing alarm notification, remote configuration such as pre-configuring threshold of various parameters such as temperature and generation of scheduled reports from the cloud server. The alarm information is therefore held off network and available from different locations.

This concept is also widely used in smart homes design using IP cameras which upload footage at remote sites onto a cloud based server. By logging into the server from any location one can be able to carry out surveillance on a remote site. (O'Driscoll, 2014)

The cloud based solution is however dependent on the user having a suitable device and an internet connection in order to log on to the cloud server. Any failure in the cloud server or supporting resources could render the information unreachable in a timely manner. The use of a cloud server is not a real time solution due to the store and forward nature of internet services. The essence of telecommunications maintenance require that alarm information is delivered to the response team as soon as possible after occurrence.

The solution under development in this research entails delivery of alarm information in real time to the response team. Additionally it requires the field officers to have a simple phone which can receive text messages on various parameters at the remote site.

c) USE OF ALTERNATIVE NETWORK IN REMOTE SITES MANAGEMENT

In most remote telecommunication sites monitoring systems, alarm information is ferried together on the same communication channel as the payload voice and data traffic. This scenario suffers a major drawback in that loss of primary transmission from the remote sites also affects transmission of this critical alarm information and results in a blackout of the affected sites.

The use of an alternative network other than the one being managed depends on the volume of the management traffic, cost and security. The use of an alternative network has the advantage of introducing route diversity which is important in protecting this management traffic. The loss of transmission on the managed network will not affect the management or monitoring traffic which uses a different transmission path. In some cases the traffic generated by the management traffic itself could be significant and it may be preferable to use a separate network to avoid degrading the service offered by the network being monitored. (Flood, 1997)

This solution entails building a parallel network sometimes independent of the monitored network which may have huge cost implications. The justification for rolling out this parallel network can only be justified by the volume of the management traffic, its composition and cost.

In this research, the developed solution has no major cost implications due to the simplicity of the design. The solution enjoys the advantage of providing route diversity to the monitoring traffic. The solution is implemented as an overlay to the existing telecommunications channels to ensure that alarm information reaches the field response teams even during transmission blackout. Additionally the infrastructure adopted is separate from the core telecommunications equipment at site which further improves diversity and protection of the management information.

2.4 TECHNOLOGICAL DEVELOPMENTS

As the number of remote telecommunications sites continue to rise due to demand for improved quality of service and new service offerings, complexity in monitoring and maintenance of these remote sites continue to be a major challenge to service providers. The solution to these challenges lies mainly in adopting a more efficient approach to complete, intelligent remote site management, one designed specifically to address the unique diagnostic, recovery and preventative maintenance activities of field operations personnel and technicians. Studies show that improved operations management using intelligent remote site monitoring solutions can eliminate up to 40% of site visits and can drastically reduce Mean Time to Repair (MTTR) resulting in reduced operational costs, better network quality, and reduced churn rate.

Remote monitoring techniques have evolved over time from the traditional telemetry systems to SNMP based systems which enable transmission of site status over internet protocol (IP). The key enabler to remote monitoring is the IP network and IP-enabled devices. These network-based surveillance devices, such as encoders, cameras, door sensors and recorders, have been coming together as a solution for a number of years now. What have been gaining more adoption are high-definition cameras. With the maturity of these systems and high-definition capabilities are coming together to form new service offerings like remote video monitoring. This advancement has enabled integration of alarm information and processing in central servers where use of graphical interfaces displays the network on live maps. (Marier, 2014)

Advancement has also been achieved in the use of intelligent sensors that are configured to detect variations in set parameters and to generate signals for processing in order to report to the central processing servers. (Intelitower, 2011)

2.5 CRITIQUE OF THE LITERATURE REVIEW

Despite the advancement in sensor technology and monitoring techniques, the greatest challenge to any telecommunications company with a vast number of remote unmanned stations and multiple teams spread in the different geographical locations is the amount of time taken between the occurrence of a network failure alarm and the arrival of an appropriate resource to rectify the problem on or off site. Inevitably any centralized network operations center (NOC) operations will lead to delays in response as alarms may pass unnoticed in the NOC; there may be time lost between alarm occurrence and the information reaching the field teams. In a scenario where intrusion detection has occurred it is important that a security response is dispatched immediately to prevent extensive damage to site through loss of valuable equipment. In the state of the art, management traffic is in most cases ferried in the same transmission path as the network being monitored. This leads to loss of management traffic if there is failure or loss of transmission in the monitored network. The management traffic is further channeled to a centralized server from where information is disseminated to various geographically dispersed field management teams. Although in this method information may be available in real time at the collecting server, the same may not be the case for the field response teams. In practice the time taken between the monitoring team obtaining alarm information and the same becoming available to the resource to attend to the failure can run into hours due to the human intervention which can introduce serious lapses in the process.

The introduction of an overlay system to avail failure information directly to response team cuts through this likely lapses and enhances response time as the latency created by the centralized NOC which may sometimes be overwhelmed will be avoided.

2.6 CONCLUSION

Advances in remote station monitoring and surveillance have greatly improved the visibility of operations in these unmanned sites. Improvement in response to network and security issues to these sites will make them virtually manned sites. The purpose of this research is to improve on monitoring so that sites demarcated on a regional basis can extend alarms to the regional staff directly offloading the monitoring burden from a network operations center (NOC) which becomes increasingly burdened as the number of sites continues to grow in the network.

The state of practice will eventually shift to the deployment of alternate means of ferrying management traffic outside the transmission route used by the monitored network. The uptake of cloud services in most applications may lead to most operators preferring to use cloud servers to store their management traffic due to the advantage of holding the critical information off network.

In order to cut down losses caused by network failures, telecommunications operators must continually devise methods of reducing fault occurrence through rigorous preventive maintenance routines, design of remote network elements to incorporate inbuilt redundancies and expedition of recovery of these network elements from failure when it occurs. A key development towards achieving expeditious recovery must incorporate an efficient network surveillance system which is transparent to the operations staff.

The design undertaken in this research is aimed at vastly improving network surveillance to enhance response to network failures.

3. RESEARCH METHODOLOGY

Research is an intensive and purposeful search for knowledge and understanding of social and physical phenomena. It is a scientific activity undertaken to establish something, a fact, a theory, a principle or an application. It is a search for Knowledge. (Kumar, 2008).

Research is not just a process of gathering information, rather it is about answering unanswered questions or creating that which does not currently exist. Research can be seen as a process of expanding the boundaries of our ignorance. The discovery and creation of knowledge therefore lies at the heart of research. Research is a systematic quest for undiscovered knowledge. Good research is systematic in that it is planned, organized and has a specific goal. (Wayne Goddard & Stuart Melville, 2007)

The purpose of this research is to come up with a monitoring system implemented as an overlay to existing remote telecommunications sites monitoring systems to alleviate the challenges encountered by in-channel monitoring and centralized alarm management systems.

3.1 CURRENT METHODS APPLIED IN RESEARCH AREA

There are currently two main technological methods used in the area of remote telecommunications sites monitoring;

3.1.1 TELEMETRY METHOD

This is a method used in the older systems where sensors at the source which are basically transducers measure physical data (such as temperature or pressure). These measurements are converted into specific electrical voltages. A multiplexer at the source combines the voltages, along with timing data, into a single data stream for transmission to a remote receiver. Upon

reception, the data stream is separated by use of a de-multiplexer into its original components and the data is displayed and processed according to user specifications. This method utilizes the existing communications links that carry voice and data traffic. Telemetry utilizes a remote telemetry unit (RTU) at the remote site to collect this alarm information for transmission. This method uses overhead bits in the time division multiplexing system to carry the alarm information. This in-channel method of transmitting alarm information renders remote sites unmonitored should this network traffic be lost or if transmission path is down.

3.1.2 SNMP METHOD

In this more modern and advanced method use is made of internet-standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior. This enables remote troubleshooting of elements off site and can solve some device malfunction without somebody physically going on site. Additionally remote site configurations can be accomplished remotely. The SNMP protocol allows interactive sessions off site. Information can be conveyed using existing links or stored up in cloud servers for retrieval through the web. The SNMP method entails use of SNMP agent enabled network devices at the remote station. Since most sensors have no embedded SNMP agent, it is the practice to use an SNMP enabled device as an interface at the source. Some devices such as surveillance cameras come with bundled SNMP agent software. The SNMP method provides flexibility in the destination of the alarm data because of the use of the IP network. This means that the information may be routed to any physical or cloud server in any location. This information is retrievable from any location through the internet.

3.2 EVALUATION OF CURRENT METHODS

Research methodology is a way of systematically solving a research problem. It is a science of learning how research is conducted scientifically. It refers to the way in which research studies are designed and procedures by which data is analyzed. Research can be done using either descriptive or analytic, applied or fundamental, quantitative or qualitative; conceptual or empirical and experimental or Non-experimental methods.

1) Analytic versus descriptive Methods

Analytic description uses information and facts available to evaluate data. Analytical research involves critical thinking and evaluation of available information and facts relative to the research being conducted. Descriptive research methods on the other hand takes the fact finding route through the use of surveys with the purpose of describing present affairs. The research has no control over the variables but only endeavors to report what happened.

2) Applied versus fundamental methods

Applied research involves research to find solutions for immediate problems. It is a scientific study aimed at solving practical problems affecting people on a daily basis such as illnesses or to develop innovative technologies. Fundamental or pure research methods on the other hand are involved with formulation of theories. This type of research is undertaken to obtain fresh knowledge of underlying phenomena and observed facts without any practical application in the immediate term.

3) Quantitative versus Qualitative methods

Quantitative methods are based on actual measurement of quantity. They deal with hard facts or statistics. This methods are used when the phenomenon being studied is expressible in terms of quantity and figures. Quantitative methods normally use measurable data to draw conclusions or verify a study. Quantitative research methods are more logical and data based. Qualitative methods on the other hand use soft facts, interviews, exploratory and a descriptive view of a relative world. This methods involve use of exploratory methods. This methods are also used to develop ideas or hypotheses which can be potential in quantitative research. Qualitative research has more to do with how people feel, the way they think and the reason they make certain choices.

4) Empirical Versus Conceptual methods

Empirical methods are ones which rely on experience or observation. They are data based methods which come up with conclusions which can be verified by experimentation or observation. Conceptual methods on the other hand are related to abstract ideas or theories emanating mainly from thinkers and philosophers.

5) Experimental Versus Non-Experimental Methods

Experimental research methods involves making variations to the independent variables and studying the effects on the dependent variables under a controlled environment. Experimental research tends to explain the cause and effect phenomena. Non-Experimental research on the other hand involves measurement of the present level of the independent variable without aspiring to make any adjustment. It tends to describe and explain relationships and does not show functional interdependence.

3.3 DEFINITION OF TOOL TO BE ADOPTED

The tool adopted for the purpose of this research is an artifact. The artifact will be used to monitor alarm information at a remote unmanned telecommunications facility and to route this information directly to the relevant field response unit in order to realize the objectives of the research. This tool consists of a sensor block containing sensors to monitor all the parameters for which this design entails, an intelligent device block containing devices which can access this sensor information and analyze it in order to arrive at a decision and an output block to aid in reporting the results of various parameters at the remote station to the response teams.

3.4 PROPOSED METHOD

Since the goal of this research is to build a remote alarm monitoring system that is meant to improve on existing technologies, applied research will be used. Applied research conducts study whose result can be applied directly to a real world event.

Applied research aims at finding a solution for an immediate problem facing society or an industry/business organization. The central aim is to discover a solution to some pressing practical problem. (Kothari, 2004)

The design of the solution will entail construction of an artifact and will involve the following steps:

a) Determination of the critical remote alarms for which an alternative reporting path is preferred. This will mainly include environmental, power and security alarms.
b) Identification of suitable sensors to be used in collecting system status information and reporting on deviations in predefined thresholds.

c) Assembly and programming of the intelligent device in the artifact, the microcontroller, using micro basic for PIC programming language.

d) Incorporation of the output GSM unit to transmit the alarm information to the relevant individual field response unit through short text messages.

e) Implementation of the overlay system over existing monitoring systems.

3.5 CONCLUSION

The design of this artifact is aimed at enhancing remote telecommunications sites monitoring and to help decentralize network operations center (NOC) operations. It is further purposed to offload some of the supervision burden from NOC to the field units directly. The overlay system design intends to improve the overall efficiency in monitoring remote telecommunications systems. This design enjoys the advantages of being an alternate management network as it will not depend on the transmission infrastructure of the monitored network, and will also have the capability to deliver the alarm status information in real time to the field operations teams.

The designed solution will solve a problem affecting businesses and will therefore be consistent with the objective of applied research.

4. CONCEPTUAL MODEL, HARDWARE & SOFTWARE DESIGN

4.1 INTRODUCTION

This chapter deals with the development of the conceptual model and the various steps undertaken in the development of the artifact hardware and software.

4.2 CONCEPTUAL MODEL

A conceptual model is arrived at after review of literature. The model shows the relationship between variables and how they interact to give the desired results or outcome. A conceptual model is a descriptive model of a system based on qualitative assumptions of its variables, their interrelationships and system boundaries. The model helps one to impose order on the interrelation of variable. Figure 4.1 shows the conceptual model for this design.

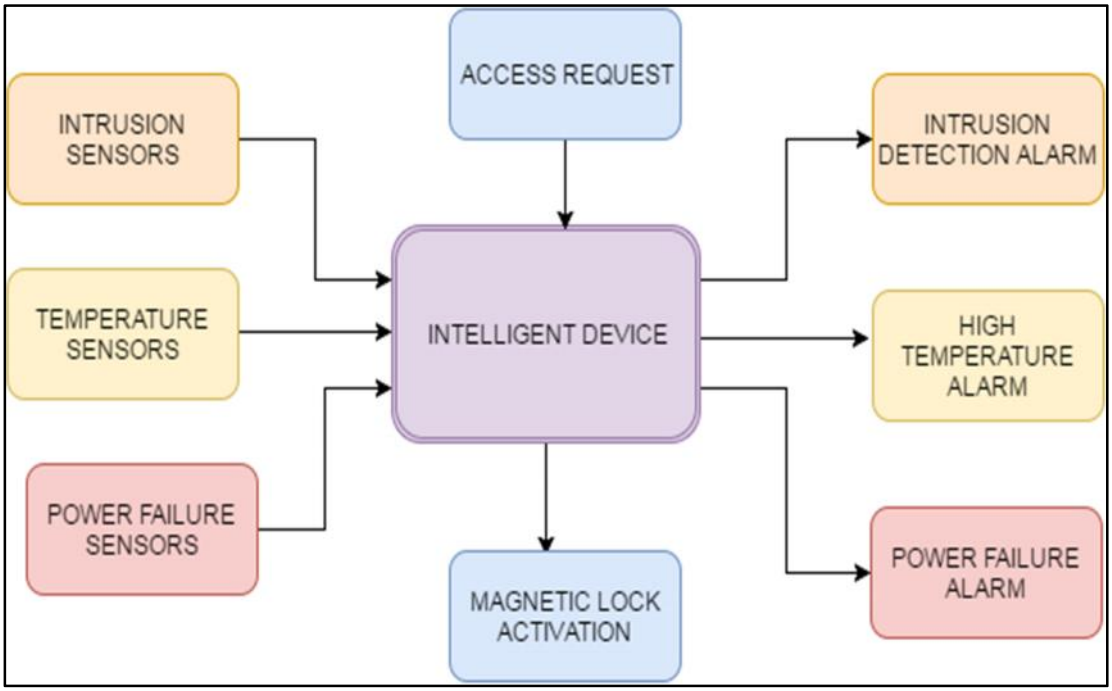

Fig 4.1. The conceptual Model.

The conceptual model consists of input and output variables. The input variables emanate from the sensor block and the received text messages. These input variables from the sensor block are in the form of electric pulses which are conditioned to become acceptable to the intelligent device. The input though the short messaging system are fed to an input port of the intelligent device. The output variables consist of the notification short messages which are sent out to response teams and the activation commands for actuation of desired mechanical manipulations. The input variables are linked to the output variables through the intelligent device in the framework. The intelligent device will receive the input variables, analyze them and generate the output variables based on this analysis.

The design as conceptualized entails the preparation and presentation of the input variables in a state that the intelligent device will recognize. The intelligent device design requires that it will recognize the input variables as presented, ably interpret the input variables, carry out analysis on the information carried by this input variables and generate outputs that will communicate any action required by the input variables. The intelligent device therefore incorporates a stored program to aid in this decision making process.

The output variables which consist of actions desired from the form of the input variables are communicated in a form suitable to actuate the requirements of the input variables. The output from the intelligent device is for example used to actuate a mechanical movement required to open a magnetic lock. The other out form is used to actuate a GSM unit to generate short messages which are sent over the chosen network to one or more recipients located remotely from the location of this device.

4.3 BLOCK DIAGRAM FOR HARDWARE DESIGN

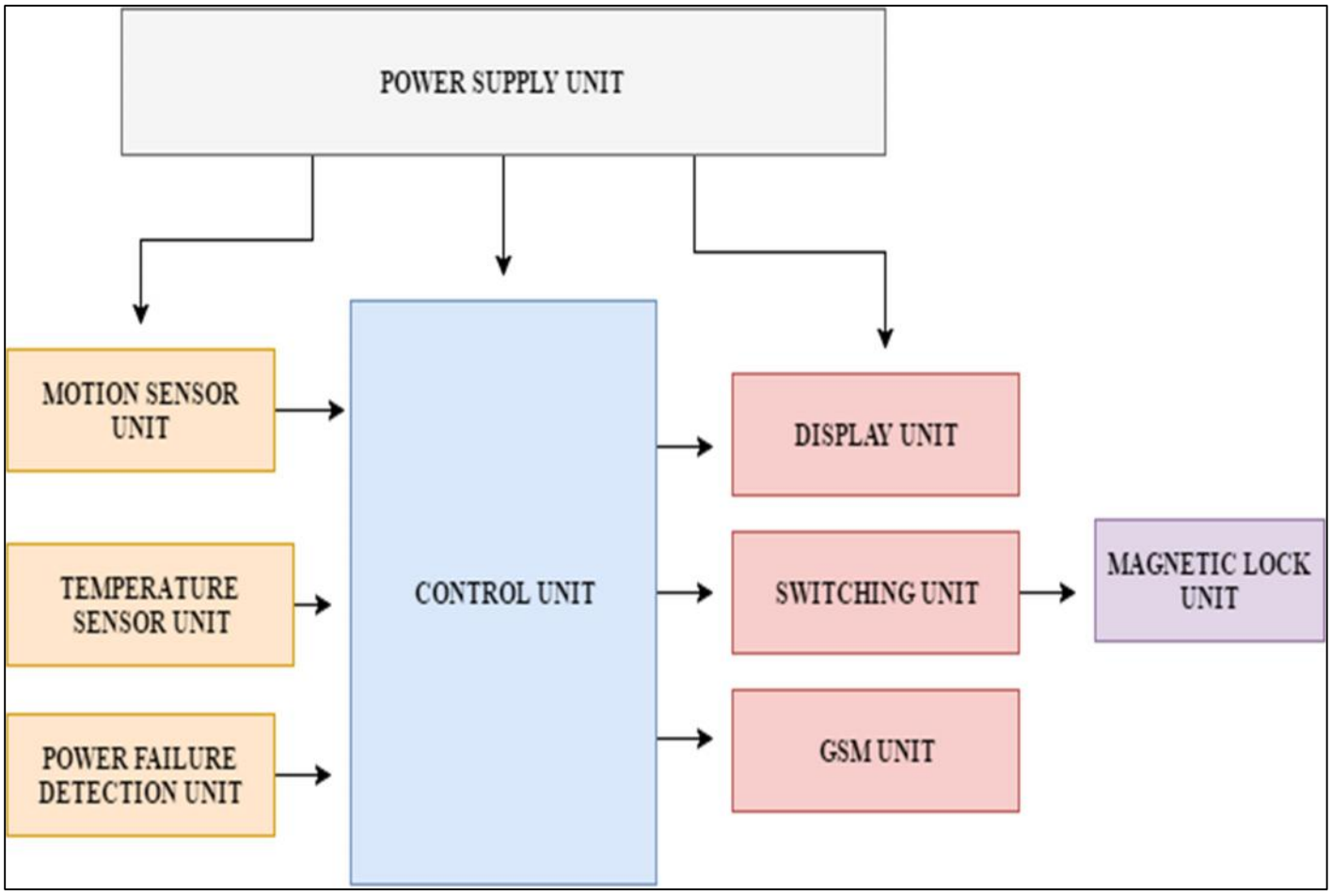

Fig 4.2.The Block Diagram

The block diagram for this research consists of the following blocks:

a) Power Supply

This device converts the input voltage from 240V AC to a stable 5V DC to power the electronic circuit. This ensures stable operation of the circuit. For on-site operation the device will be fitted with a rechargeable battery to ensure its operation even in the event of multiple power

source failure at the monitored station. This will ensure that the station will remain monitored in the event of a multiple power source failure at site. This rechargeable battery will have the capacity to supply the requisite 5Volts Dc power to ensure proper circuit operation.

b) Motion Sensor Circuit

The motion sensor generates a voltage signal to the Microcontroller when motion is detected in the protected area. The motion sensor used will only sense human beings to avoid false alarms. For the purpose of covering the entire protected area several motion detectors may be used and their outputs fed in parallel to the microcontroller. The signal from the motion detection circuit will indicate the presence of unauthorized persons in the protected area and will prompt the GSM module to send an SMS to the security response team.

c) Temperature Sensor Circuit

The temperature sensor monitors the temperature level in the room and converts it to an analog voltage signal which is proportional to the temperature level. This analog signal is passed through the microcontroller internal analogue to digital converter (ADC) which converts this analogue temperature to digital readings. When the temperature exceeds the set threshold, the GSM module sends a text message to the heating, ventilating and air conditioning (HVAC) maintenance team.

d) Power Failure detection circuit

This circuit converts the input power to a voltage signal to be used to monitor power failure of any of the three sources, AC mains, diesel engine generator and UPS supply. If the AC mains supply goes off, the microcontroller will send notification of AC mains off. The generator is

expected to come on after a brief delay. If the generator does not come on, then the microcontroller sends a second notification indicating that the commercial power is off and the generator is off. This means that the site is on uninterruptible power supply (UPS) which is the last supply to the equipment. In the event that the UPS also goes off, then a notification of outage of the three power sources is sent. This means that there is total service outage at the remote site due to total power failure.

e) GSM Module

This is the output device which transmits alarm information by SMS to the field response team. The GSM unit is connected to the microcontroller and receives both the message to be sent and the telephone number to which the message will be sent. The microcontroller is programmed in such a way that the various alarms are discriminated and sent to different response teams. It is also possible to program the microcontroller to send one message to multiple recipients.

f) Control Circuit

The Microcontroller device is the main component of the control circuit. The microcontroller consists of an inbuilt microprocessor device, memory units and input/output devices. The microcontroller operates according to the source program stored in the read only memory (ROM). It monitors the inputs from the temperature sensing circuit, the motion sensor and power failure detection circuit and prompts the GSM module to send the desired text message to the appropriate response team. The microcontroller also drives the local display unit and checks for input messages for access control in order to send appropriate signal to actuate the magnetic lock.

g) Display

The artifact is built with a local display which shows the status of the monitored parameters on an alphanumeric screen.

h) Switching Circuit

The switching circuit is used to open and lock the magnetic lock on receiving a voltage signal from the microcontroller. The voltage signal comes as a result of a turn on/off message sent remotely to facilitate access to the facility. This enables provision of access to the facility remotely by use of a coded message. Once the person granted access is off the site, another message is sent to lock the facility.

i) Magnetic Lock

This is a remotely activated magnetic lock which is activated by use of coded text messages in order to grant access to the facility to authorized personnel. Once the personnel clear with the facility a coded text to lock the door is sent to activate the lock.

4.4 FLOW CHART FOR SOFTWARE DEVELOPMENT

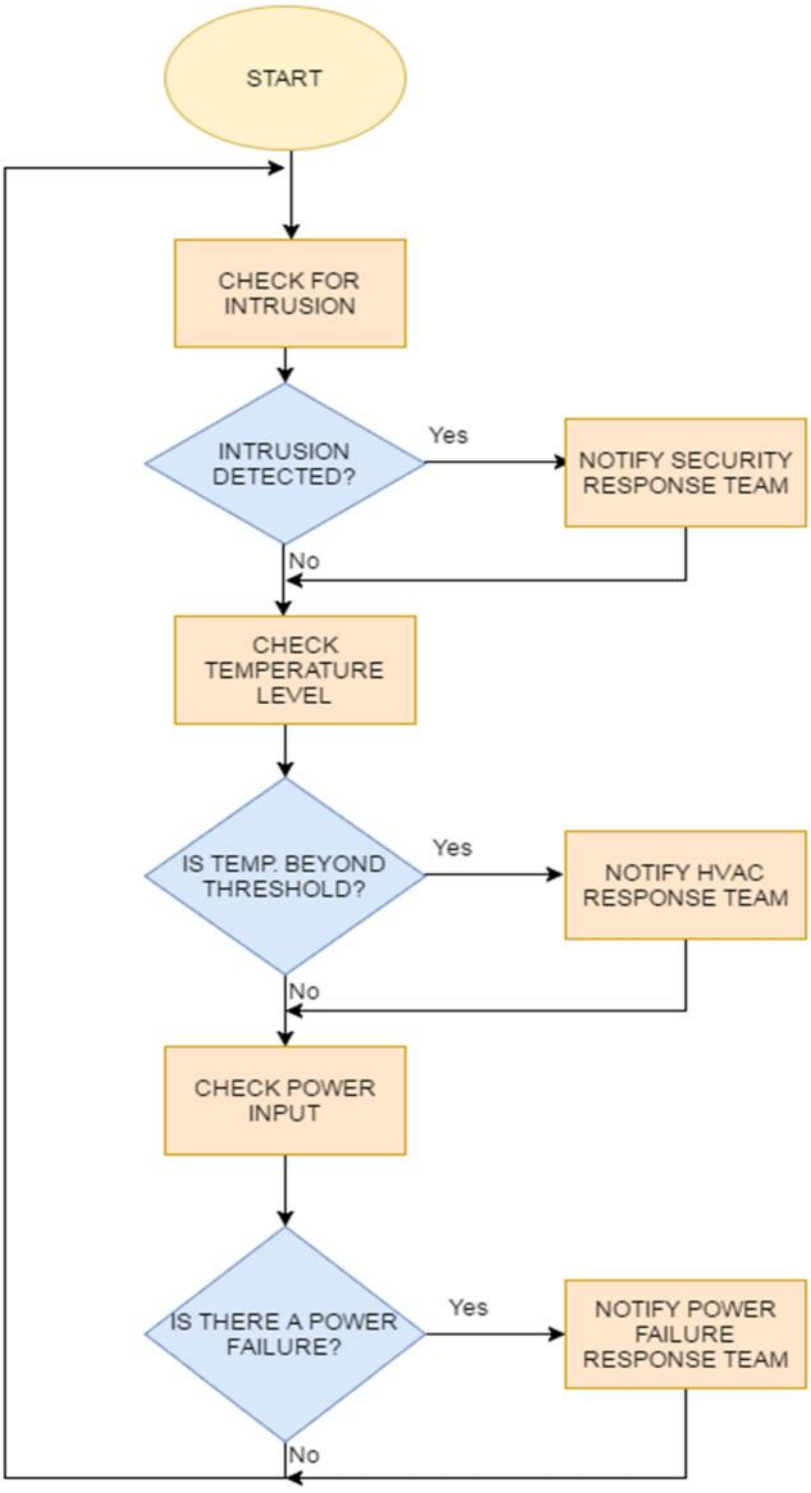

Fig 4.7. Flow Chart for software development

The flow chart design helps guide on how to obtain the code for the intelligent device in the artifact by showing the sequence of activities to be carried out.

Once switched on the device should engage in a continuous loop to scan the various parameters and report on their status.

The flowchart for the implementation of the source code indicates that the program will consist of several modules which will be executed in an endless loop to monitor the three parameters selected for this research.

The first module checks if there is any intrusion within the protected area and sends notification to the security response team. The second module then checks the temperature at the facility and notifies the appropriate team if the temperature goes over the threshold which may be an indication of failed air conditioning or a fire at site.

The third module monitors the three power sources to the equipment at the remote facility and sends notification to the appropriate power response team. In most cases loss of commercial AC power will consist most of the messages due to the unstable nature of grid power. This alarm may not require immediate response if the generator kicks in in good time and takes over supply to the equipment in the facility. If however there is loss of commercial AC supply and the standby generator fails to come on, then the remote site will be operating on the last line of supply which is the uninterruptable power supply (UPS) and will require immediate attention to work on the standby generator.

In some cases the direct current power supply to the equipment at the remote facility may fail. This situation leads to service outage at the remote facility and constitutes a telecommunications emergency to restore service.

5. IMPLEMENTATION AND TESTING

The implementation and testing phase entails the process of designing the hardware and software for the artifact and testing the functionality of both the hardware and software components.

5.1 HARDWARE IMPLEMENTATION

5.1.1 CHOICE OF COMPONENTS

The hardware construction of the artifact entails choice of appropriate components for the various blocks.

1) The LM 35 IC is used as the temperature sensor. It is a precision IC whose output voltage is linearly proportional to the temperature. It does not require external calibration to provide the required accuracy. Temperature sensors are basically classified into two types:

- Non-contact temperature sensors – These sensors use convection and radiation to monitor temperature.
- Contact temperature sensors – These sensors measure their own temperature. They are classified as electromechanical (Thermocouples), Resistance temperature detectors (RTD) and semiconductor based sensors.

The LM 35 temperature sensor is a semi-conductor based sensor. The sensor is calibrated directly in degree Celsius and has a linear 10.0mv/degree Celsius factor. This means that if the output of the LM35 is 220mV, then the temperature is 22 degrees Celsius. If the room temperature is 32 degrees Celsius, then the output of the LM35 will be 320mV or 0.32Volts.

It is suitable for remote applications and operates from 4-30Volts.

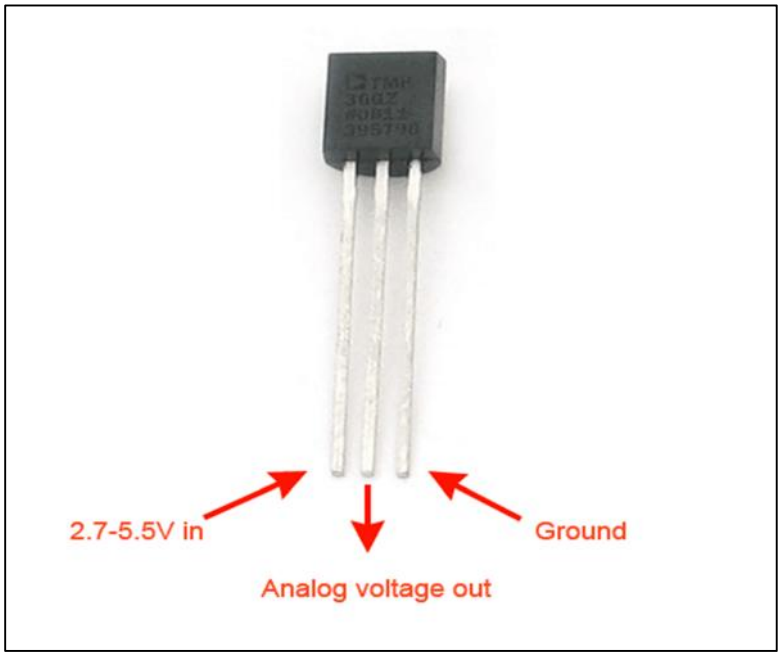

Fig 5.1. The LM 35 temperature sensor –Photo by DNA Technology India

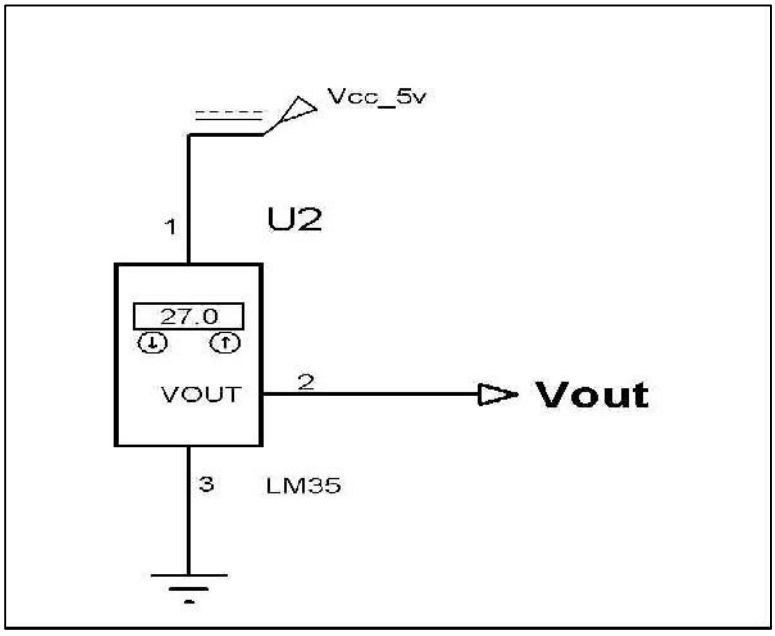

Fig 5.2. The LM 35 temperature sensor interfacing circuit –Photo by DNA Technology India

The LM35 temperature sensor is directly interfaced to the analog to digital convertor (ADC) since the output is linear.

2) The motion detector is a device used to detect the movement of objects and especially people. There are several technologies employed in the manufacture of motion detectors:

- Passive Infra-red technology (PIR) - Passive infrared sensors are sensitive to a person's skin temperature through emitted black body radiation. There is no energy emitted from the sensor hence the use of the word passive. This is in contrast to sensors which emit infrared beams which when crossed or interrupted detect intrusion.
- Microwave technology – These sensors detect motion through the principle of Doppler radar. This is done through the emission of a continuous wave of microwaves. Any phase shifts in the reflected microwaves are due to an object moving to or from the receiver.
- Ultrasonic technology – An ultrasonic wave is a sound at a frequency higher than the human ear audio range. These waves are emitted and reflections from nearby objects received. As in the Doppler Effect, phase shifts in the received reflections will indicate motion.
- Video camera software technology – it is possible to use the output of a digital video camera to detect motion. If the observed field is normally illuminated, this may be considered a passive technology. However it can be used with near infrared illumination to detect motion in the dark.

In this research a passive infrared (PIR) motion detector is used as the primary objective is to detect human intrusions.

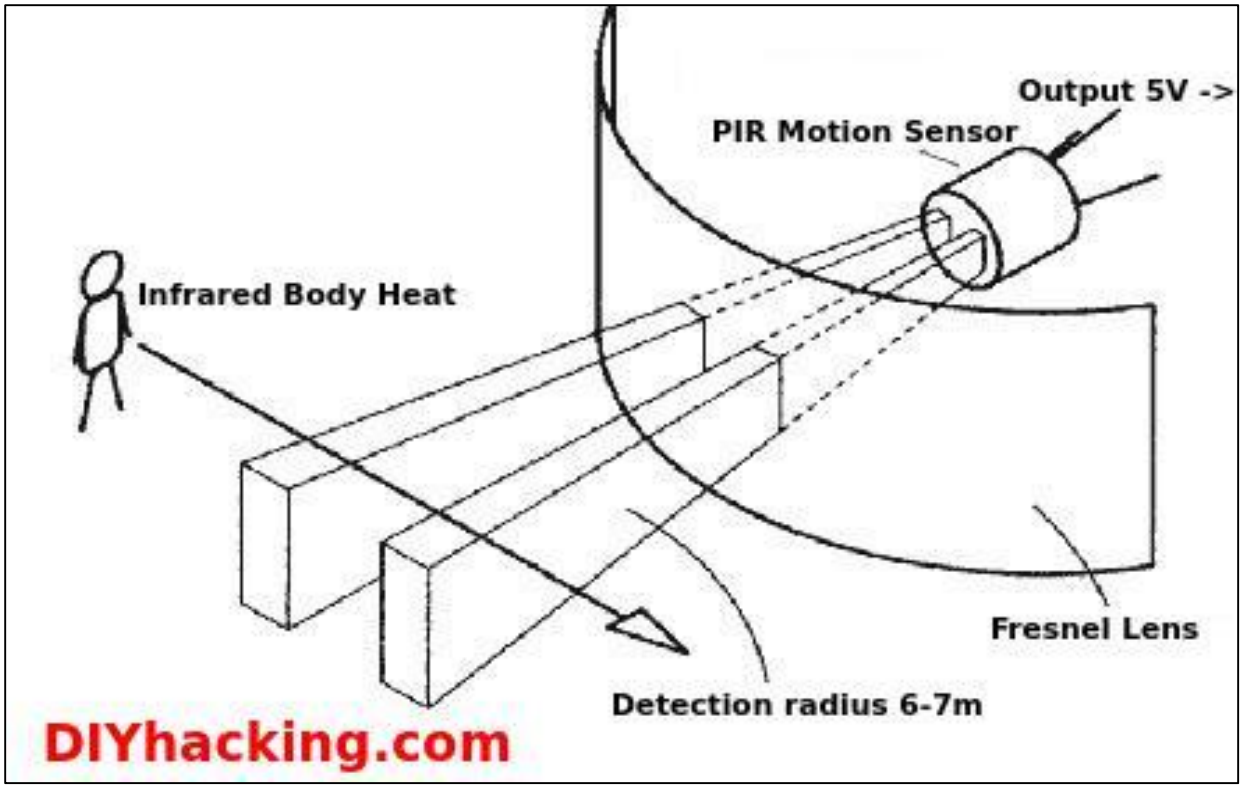

Fig 5.3. A Passive infrared motion detector –Photo by DYhacking.

3) The three input power devices, the AC mains, Generator and UPS are simulated by use of make/break switches which indicate the presence and absence of input power from the various devices.

4) The PIC 18F452 Microcontroller is the intelligent device in the artifact. It is a high performance enhanced flash microcontroller with a 10-bit Address/Data bus. The microcontroller is basically a single built in microcomputer system consisting of a microprocessor, memory devices and input/output devices. It is programmable using the Micro Basic for PIC programming language.

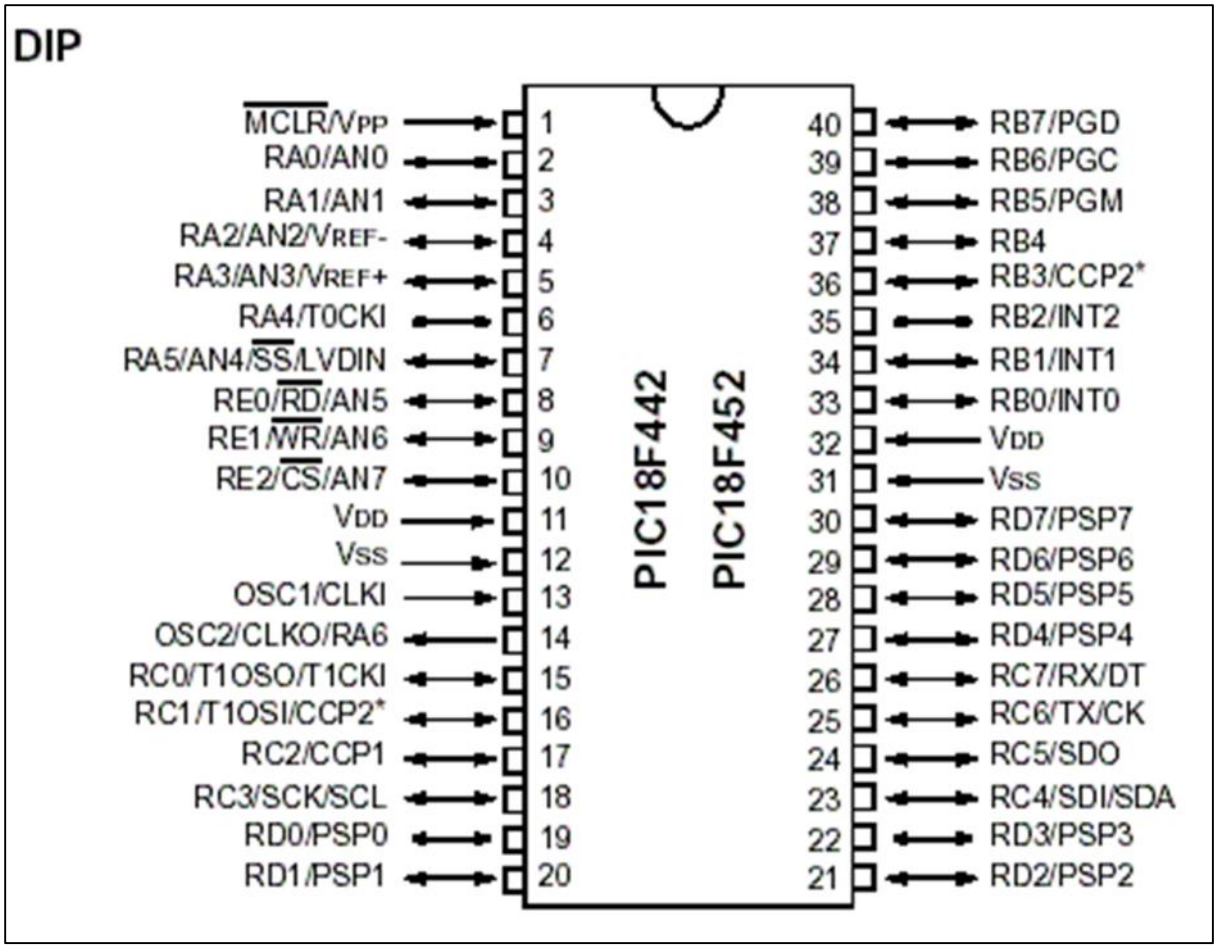

Fig 5.4. The PIC18F452 pin assignment –Photo by futurlec electronics components super store.

5) The GSM unit is the output device and is used to transmit short messages to the various specialized response teams for appropriate action. The GSM unit is fitted with a SIM card for the preferred network which sends the short messages to the field response units when network and environmental failures occur.

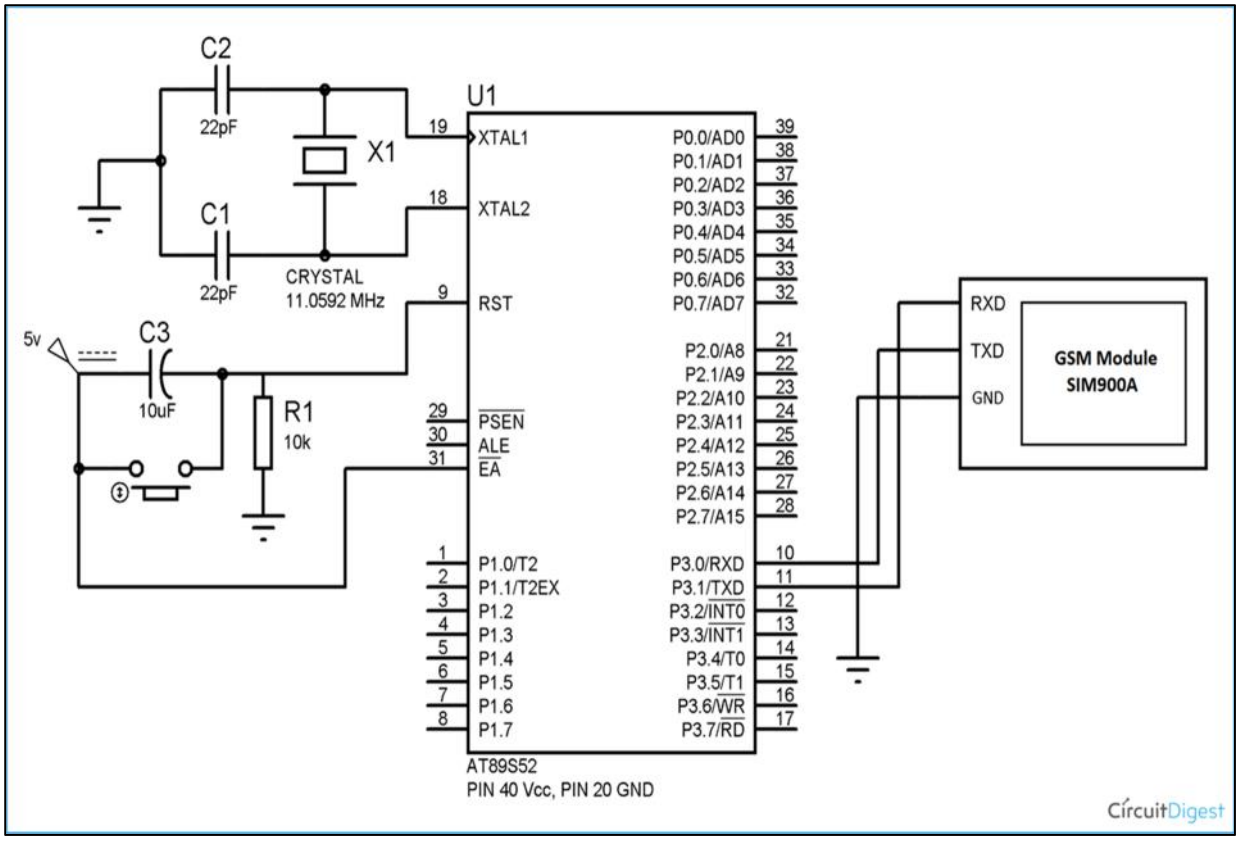

Fig 5.5. Interfacing a GSM module with a PIC microcontroller –Photo by circuit digest.

6) The Magnetic Door lock is activated by means of a short message from the user to the intelligent device and in this research is simulated by use of a light emitting diode. By sending the appropriate code to the GSM unit of the artifact, the microcontroller sends an actuating signal which is indicated by the glow of the simulating LED. A lock text code will also send another actuating signal which will be indicated by the LED going off.

5.1.2 THE BLOCK SCHEMATIC LAYOUT

The artifact is implemented in the indicated blocks as shown in the block schematic figure 5.6.

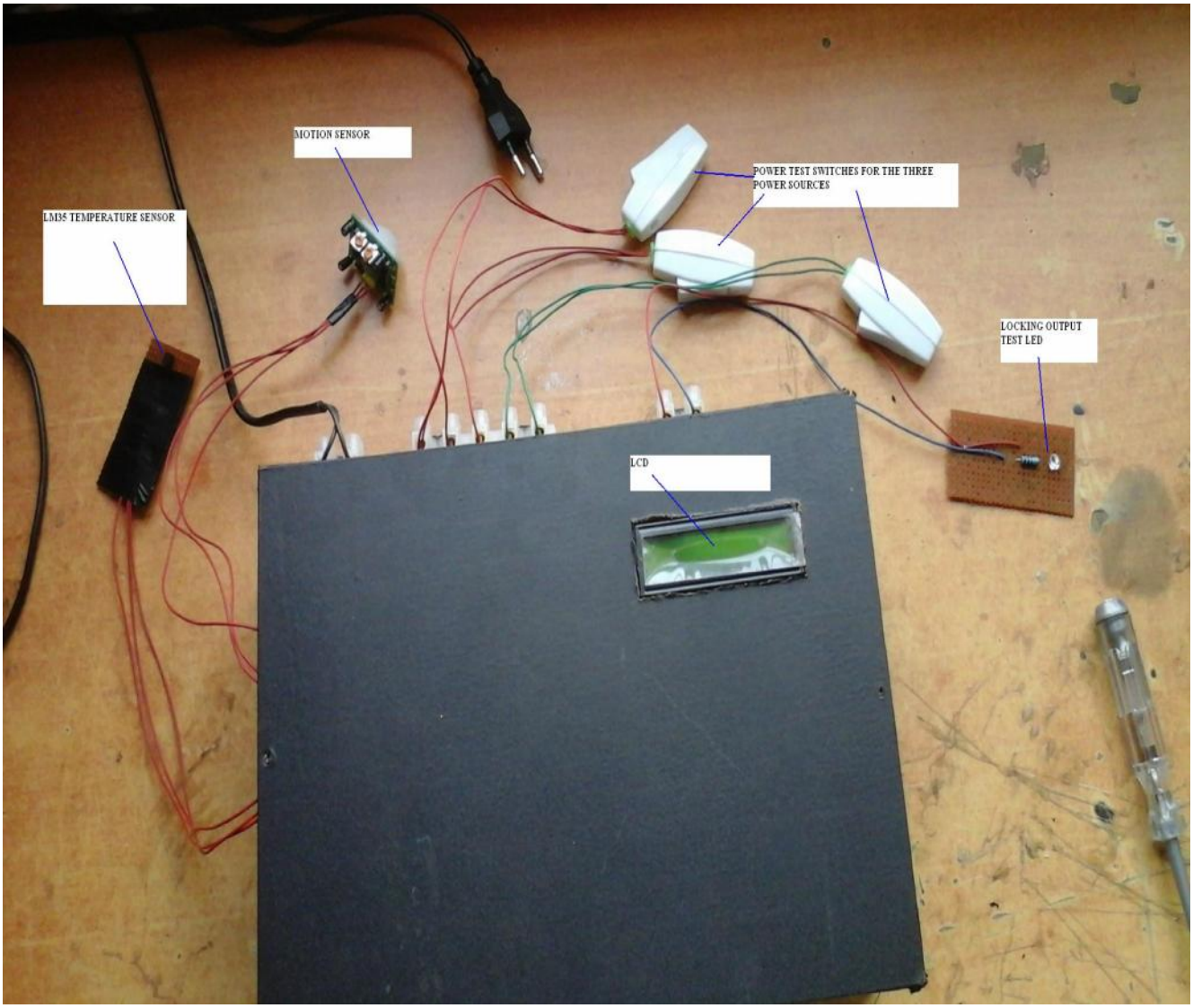

Fig 5.6. The Block Schematic layout diagram

The components of the artifact are designed in accordance with the block diagram design in chapter 4.

5.1.3 THE CIRCUIT DESIGN

a) The circuit

The interconnection of the various components of the artifact is shown in figure 5.2;

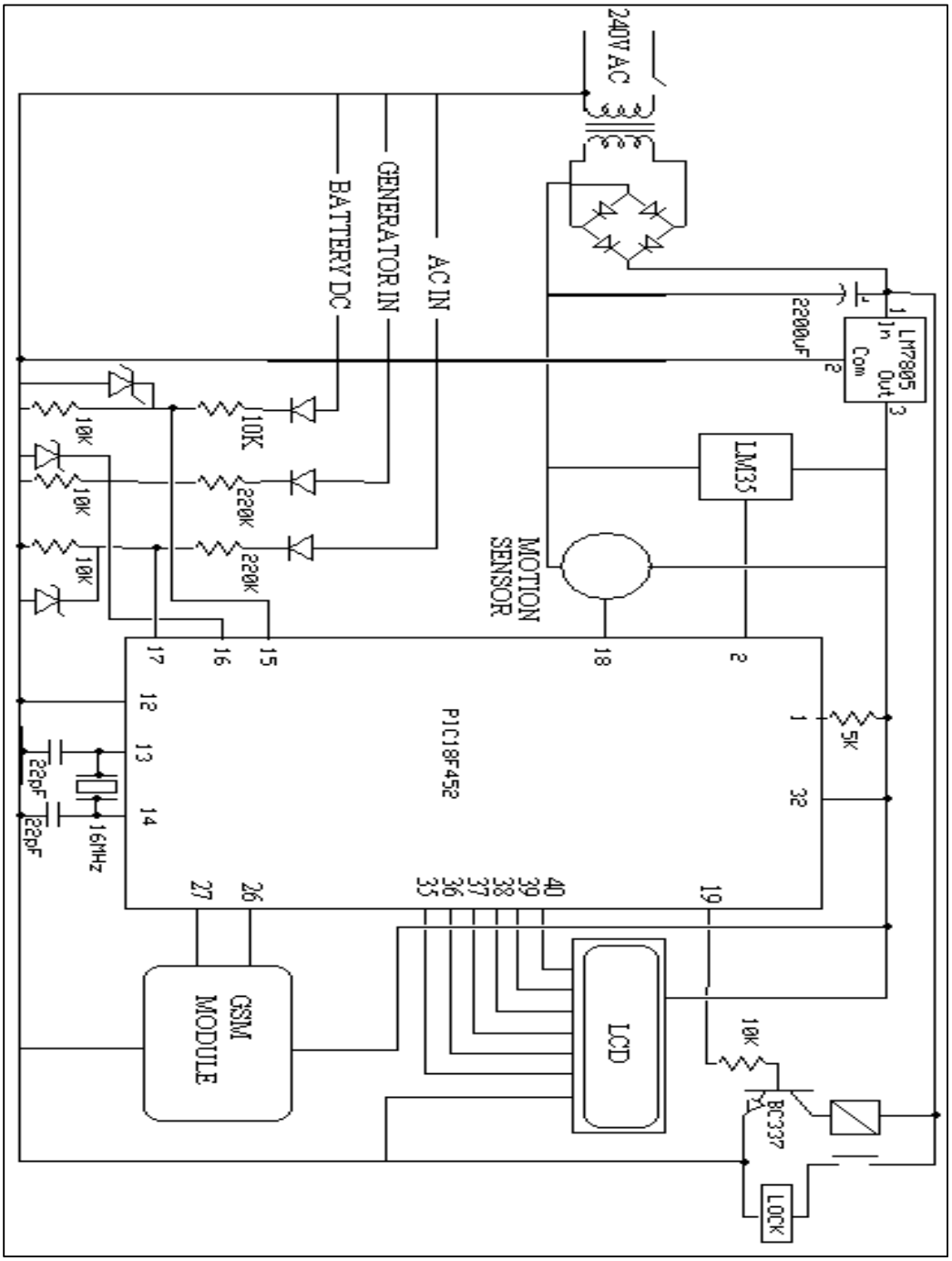

Fig 5.7. The Circuit Diagram

b) Circuit implementation Layout

The circuit layout design is shown in figure 5.3

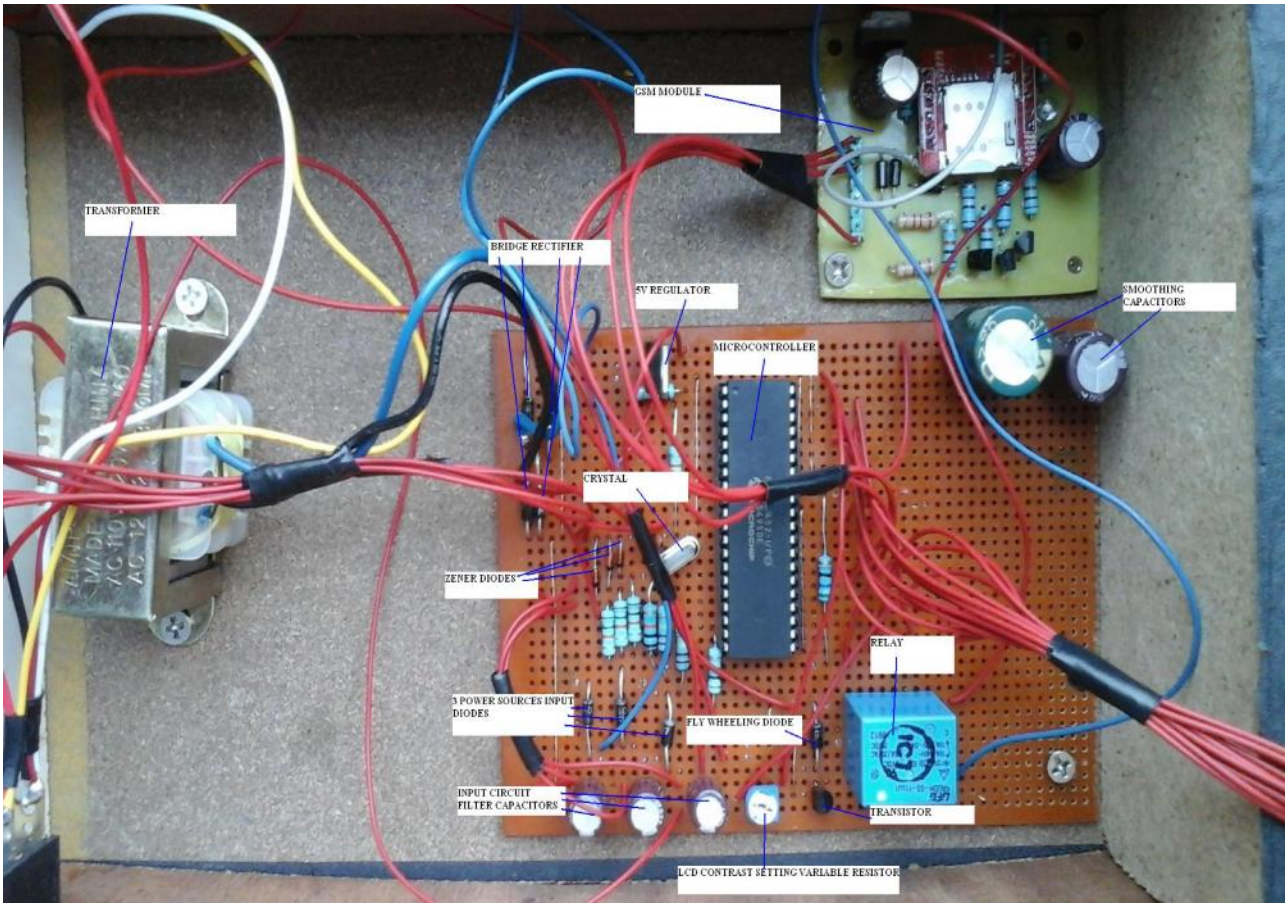

Fig 5.8. The circuit schematic diagram

c) Circuit Operation

When the switch is closed, the transformer steps down 240V ac to 12 V ac. This is then rectified by the four diode bridge rectifier after which it is smoothened by the 2200 uF capacitor. The 7805 IC is a voltage stabilizer IC. This is meant to ensure that the circuit is constantly supplied with 5 volts regardless of variation in the source voltage which ensures stable operation of the circuit.

The motion sensor on detecting motion generates an output voltage of 5 volts DC to the Microcontroller. The Microcontroller prompts the GSM module to send a text message to the security response team.

The LM35 temperature sensor is used to sense temperature by converting it to an analog voltage signal whose voltage is proportional to the temperature. This is fed to the Microcontroller internal analog to digital converter (ADC) module that converts the voltage to binary coded decimal (BCD) codes. The Microcontroller prompts the GSM module to send a text message to the HVAC maintenance team when temperature exceeds the set threshold.

The 220K and 10K resistor potential divider and the diode in each of the network converts the 240 volts ac input from the utility power and the generator power to 5 volts. This is stabilized by the 5 volts Zener diode.

The 12V or 48V battery bank power is converted to 5 volts by the use of diode and the two, 10K resistors. The three 5 volts outputs are fed to the microcontroller for monitoring.

When any of the power sources fail, the corresponding 5 volts input signal fails. The Microcontroller through the GSM module sends a text message to the Power maintenance team.

Access to the remote facility is availed by means of a magnetic lock which is activated by use of a coded short message. Once the code for unlock is received by the microcontroller, it will turn on pin 19 which will energize the relay through the transistor wired as a switch. The relay's normally closed contacts will unlock the door. Another coded short message is

used to activate the magnetic lock in order to lock the facility once the authorized personnel leave the remote facility.

5.2 THE SOFTWARE

The design of the Microcontroller software entailed determination of the flow or sequence of events, development of the control program using the appropriate Micro Basic high level program for PIC, assembly and storage of the program in Hexadecimal format in the Microcontroller memory.

The source code design consists of the main program and several sub procedures to handle the various parameters being monitored. This includes sub procedures for intrusion detection, High Temperature, AC mains failure, Generator failure and UPS failure.

a) The Main Program.

On start up the program begins execution of the main module. The main module begins by clearing the local alphanumeric display and printing the name 'GSM REMOTE MONITOR'. The program then moves on to display the current temperature reading on the local display. The temperature is displayed in the format TM: XX. The device will locally display all temperature readings but will only escalate if the temperature goes over the threshold.

The main program then proceeds to check if the temperature reading is above the threshold. If this is the case then the main program calls the sub-procedure 'TEMPS' which enables a text message to be sent to the HVAC team indicating that there is high temperature at the remote site.

The main program then moves to ‘MOTION START’ and checks whether there is a set bit on the intrusion register bit. If the bit is set indicating that an intrusion has been detected, then the word ‘INTRSN’ indicating intrusion detected is displayed on the local screen.

The program then moves to ‘POWER START’ portion of the program and checks the conditions for the three power inputs, which are the AC commercial power, the standby generator and the UPS DC power supply to the equipment. If there is failure in the AC mains then the message ‘AC F’ is displayed on the local display. A generator failure to kick in after AC mains failure is indicated by the message ‘GN F’ on the local display. A UPS failure will also be indicated on the local display as ‘UPS F’.

Once all the parameters have been checked and their status displayed on the local alphanumeric screen, the main program then moves to implement ‘GSM START’ to enable sending of text messages to the various response teams. The program will begin with the motion detector and if set will implement the sub-procedure ‘MTN’ which sends the text message to the security response team. After implementing the intrusion detection sub-procedure the main program then checks the status of the UPS and implements ‘BDC’ which is a sub-procedure for UPS failure and results in a text message to the power response team if there is failure in the UPS. The program then checks the status of AC mains power and if there is failure implements the sub-procedure ‘MAINS’ which results in a message on AC mains failure being sent to the power response team. If there is a mains failure, there will be a delay before the generator can come on. After this delay if the generator does not come on then the program executes the sub-procedure ‘GENR’ which will send a message on generator failure to the power response team.

After checking and reporting on all the parameters the main program then runs sub-procedure 'RID' which reads in any received text messages for access provision. If there are received messages then the microcontroller activates the magnetic lock to the open or close position depending on the command.

The registers are subsequently cleared and the program goes through a fresh loop.

b) Sub Procedure RID()

This sub procedure handles the read input data module and reads in the coded text messages for the activation of the magnetic lock. An input of the Ascii code for the letter 'A' results in a command to open the magnetic lock. An input of the Ascii code for the letter 'B' results in a command to lock the magnetic lock.

c) Sub Procedure MTN()

This sub procedure is called by the main program when there is a motion detected in the protected area and it sends the message 'SITE 4540 KITENGELA INTRUSION DETECTED' to the designated telephone number for the security response team. This message can be sent to more than one recipient by programming the desired recipients' telephone numbers in memory.

d) Sub Procedure BDC()

This sub procedure is called by the main program when a UPS power input failure is detected at the remote facility. It sends the message 'SITE 4540 KITENGELA UPS FAILURE' to the appropriate response team telephone number. Multiple recipients can be programmed if required.

e) Sub Procedure MAINS()

This sub procedure is called by the main program when AC mains supply failure is detected at the remote facility. It sends the message ‘SITE 4540 KITENGELA MAINS FAILURE’ to the power maintenance response team. It is also possible to program multiple recipients for this escalation.

f) Sub Procedure GENR()

This sub procedure is called by the main program if there is an AC mains failure at the remote facility and the standby generator does not start supplying AC power after a predetermined delay. The sub procedure sends the message ‘SITE 4540 KITENGELA GENERATOR FAILURE’ to the power maintenance response team. Multiple recipients can be programmed.

g) Sub Procedure TEMPS()

This sub procedure is called by the main program when the temperature at the remote facility exceeds the set threshold. In this research the high temperature threshold is set at any temperature above 30 degrees. The sub procedure will send the message ‘SITE 4540 KITENGELA HIGH TEMPERATURE XX DEGREES’. This message can be sent to multiple recipients.

The source code in micro basic language for PIC is attached in appendix 1.

5.3 TESTING

Testing of the circuitry was carried out after the assembly of all the components. The input power was traced through the circuit to ensure all the components were powered. The alphanumeric screen was incorporated to ensure that local tests were successful before attempting to transmit.

The software functionality was also tested by simulating various conditions in the monitored parameters and monitoring the output both on the local display and on the programmed mobile devices. For the purpose of functionality testing three different mobile devices were used to monitor intrusion, high temperature and power failure alarms.

5.4 RESULTS

The results obtained both on the local device display and the remote cell phones were captured in the attached screenshots. For the purpose of this research the artifact is assumed to be installed in a remote telecommunications site in Kitengela with a site identity code 4540.

The screenshots indicate various conditions at site which will be transmitted to remote field maintenance teams.

Fig 5.9. A Screenshot of the device start up screen

Fig 5.10. A Screenshot of Temperature at Site

Fig. 5.11. Screenshot showing temperature level and Intrusion detected

Fig. 5.12. Screenshot showing temperature and AC mains failure.

Fig. 5.13. Screenshot showing temperature, AC and Generator failure.

Fig. 5.14. Screenshot showing temperature and UPS failure.

Fig. 5.15. Screenshot showing temperature and multiple source power failure.

The screenshots of messages received by remote field response teams are indicated in screenshots from the cell phones used in monitoring intrusion, high temperature and power failure.

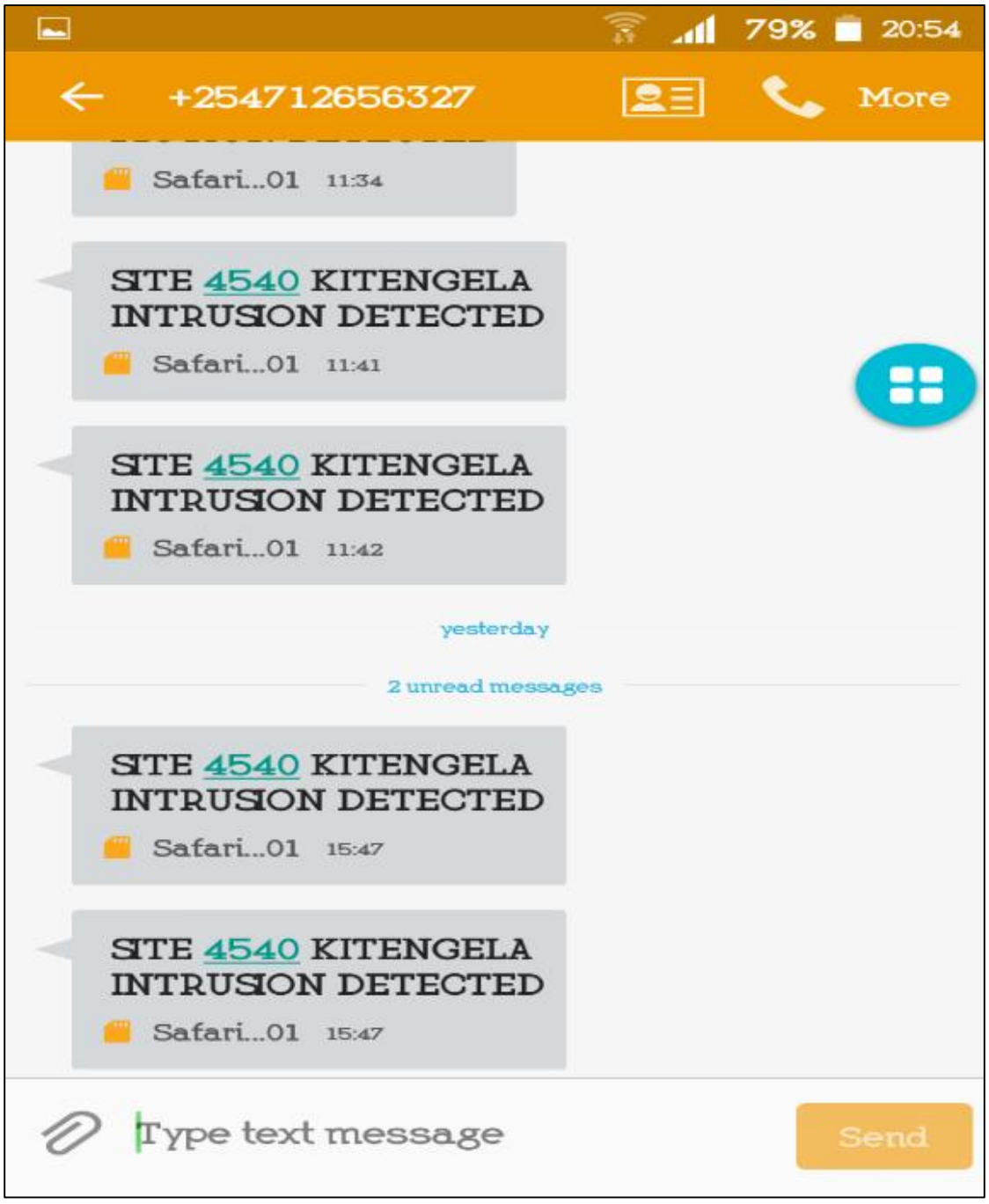

Fig. 5.16. Screenshot showing Intrusion detection text messages.

Fig. 5.17. Screenshot showing Power Failure text messages.

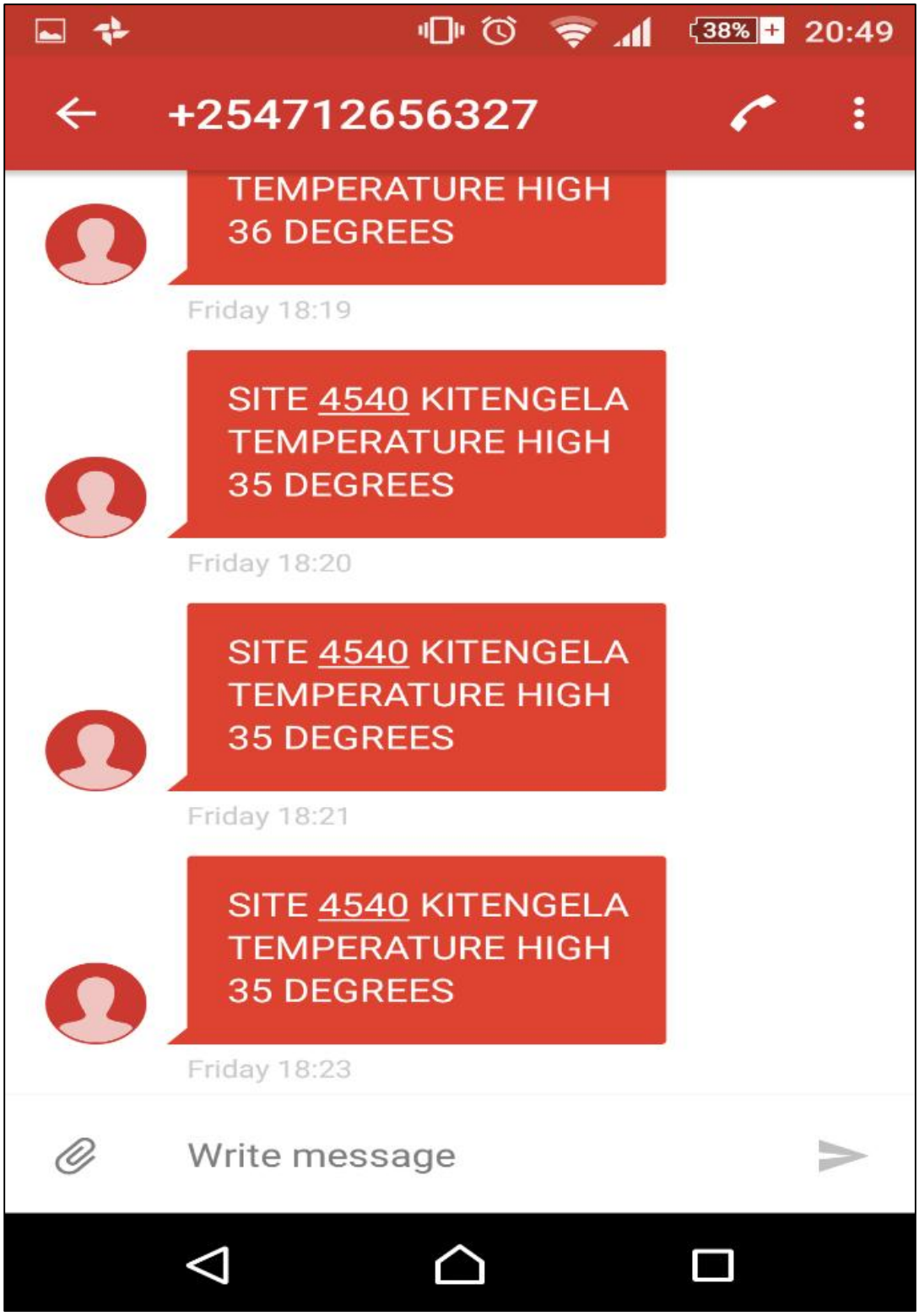

Fig. 5.18. Screenshot showing High Temperature text messages.

6. CONCLUSIONS AND FURTHER RESEARCH

6.1 CONCLUSIONS

Due to the remote and distributed nature of mobile telecommunications sites, there is a critical need for comprehensive remote monitoring systems to be put in place. It is not practical to have all these geographically distributed sites manned as the cost of maintenance would simply skyrocket and operators would not break even. Mobile telecommunications operators therefore deploy field teams strategically with each team covering a defined geographic area and responding to a number of sites. Depending on the terrain and dispersion of these sites, appreciable time may elapse between alarm occurrence and response. In event of multiple sites failures under the same field team, prudence in prioritization will be critical.

Ideally, once a remote site is installed it would only require scheduled preventive maintenance owing to the built in redundancies in most installed systems. Site visits for corrective maintenance are a costly affair for any telecommunications operator. This situation is further exacerbated by the expanding number of sites needed to continually optimize the mobile network and deliver newer technologies. The corrective maintenance effort is however rewarding especially where response to outages happens before total service outage occurs and where service restoration takes place within such time as to maintain agreed service level agreements with clients.

One crucial component of response to service outage is the time taken for the outage report to reach the field response team. In this regard, the goal of the researcher was achieved in this research project as evidenced in the immediate reception of customized text messages to every monitored condition.

Secondly the research achieved discrimination of site failure alarms to the appropriate response team such that each field team receives notification of outages related to their respective line of maintenance. Another advantage of this discrimination of alarm information is the ability of raising for example the security staff without the knowledge of other teams to ensure collusion of staff with unscrupulous people to vandalize remote site equipment and facilities is kept in check.

6.2 LIMITATIONS

This research basically addressed the issue of transporting remote site alarms directly to the field staff using an overlay system to the existing channels. The developed artifact can only be used to query the state of various monitored parameters as well as reporting on the same. The system cannot be used to carry out any corrective or preventive maintenance offsite.

6.3 FURTHER RESEARCH

Due to their remote and unmanned state, mobile stations are normally designed with several redundancies to forestall total failure. In most cases therefore field response units attend to partial failures which have not resulted in total network outage. Sometimes where total outage has occurred, it's due to failures in automatic transfer to standby units. An AC power failure coupled with a failure in the automatic transfer switch to the standby generator will result in the last defense i.e. the UPS supporting the load. Since the UPS is not designed to hold the site for long, total outage may result if the field response team does not get to site in time.

This could be alleviated if the monitoring system had an interactive capability and is connected to such basic components on site to allow their remote activation through short messages.

7. REFERENCES

Adepetun, A. (2014, December 17). Network Inventory Management System for Telecommunications. *The Guardian*.

Aistė Andrijauskaitė et al. (2009). SCADA SYSTEM IN GPRS NETWORKS:.

Azeti. (2016). Telecom Site Management. *Telecomms site Management*.

Communications Authority Kenya. (2016). *First Quarter Sector Statistics Report for the Financial Year 2015/2016.* Nairobi: Communications Authority of Kenya.

Flood, J. (1997). *Telecommunication Networks.* London: Institute of Electrical Engineers (IEE. Retrieved from https://books.google.co.ke/books?id=GR-1UXIYIvwC&printsec=frontcover#v=onepage&q&f=false

Hajela, S. (1996, October). Alarm Management inTelecommunications Networks. *Hewlett-Packard Journal* .

Institute, B. C. (2013). *The top causes of downtime explored.* Retrieved from http://www.continuitycentral.com/news06645.html.

Intelitower. (2011). Monitoring of Remote Stations. http://www.intelitower.com/assets/pdf/brochure-intelitower.pdf.

John. L. Zyskind; Jonathan A. Nagel & Howard D. Kidorf. (2006). Optical Fiber Telecommunications III.

Kothari, C. (2004). *Research Methodology.* (R. Illustrated, Ed.) New Age International.

Kumar, D. R. (2008). *Research Methodology.* New Delhi: APH publishing Corporation.

Marier, K. (2014, February 1). How Remote Monitoring Can Combine Services and Surveillance. *Security Magazine*.

Misra, K. (2004). *OSS for Telecom Network- An introduction to network management.* London: Springer.

Mukunzi, S. (2011, March 15). GSMA – Green Power for Mobile (GPM) 7th Working. In S. Mukunzi (Ed.), *Sustainable Green Energy*. Mombasa: GSM Association. Retrieved from http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/06/Sustainable_Green_Energy_Safaricom_Experience.pdf.

O'Driscoll, G. (2014). Essential Home Automation Functions. In *Manage your Smart home with an App.* (p. 20). https://books.google.co.ke/books?id=t6PmBQAAQBAJ&pg.

OpManager. (2016). *https://www.manageengine.com/network-monitoring/what-is-snmp.html*.

Schmerbeck, W. (2005). Cost/Benefit analysis of High performance controllers in low end telecommunications power systems applications. *INTELEC.* Berlin.

Telford, T. (2007). Information Technology in the construction Industry. In *Construction Law Handbook* (p. 430). https://books.google.com/books?isbn=0727734857.

Westell. (2015). Remote Site Management. *Westell*.

Winters, N. (2005). Telemetry. *Tech Target*.

APPENDIX

1. SOURCE CODE

```
SUB PROCEDURE RID()              'READ MESSAGE

  WHILE (UART1_Data_Ready() = 0)     ' If data is received,

  N1 = UART1_Read()                  ' read the received data,


  WHILE (UART1_Data_Ready() = 0)   ' If data is received,

  N2 = UART1_Read()                  ' read the received data,


  WHILE (UART1_Data_Ready() = 0)   ' If data is received,

  N3 = UART1_Read()                  ' read the received data,


  WHILE (UART1_Data_Ready() = 0)   ' If data is received,

  N4 = UART1_Read()                  ' read the received data,


  WHILE (UART1_Data_Ready() = 0)     ' If data is received,
```

```
N5 = UART1_Read()              ' read the received data,


WHILE (UART1_Data_Ready() = 0)   ' If data is received,

N6 = UART1_Read()              ' read the received data,


WHILE (UART1_Data_Ready() = 0)   ' If data is received,

N7 = UART1_Read()              ' read the received data,


WHILE (UART1_Data_Ready() = 0)   ' If data is received,

N8 = UART1_Read()              ' read the received data,


WHILE (UART1_Data_Ready() = 0)   ' If data is received,

N9 = UART1_Read()              ' read the received data,


WHILE (UART1_Data_Ready() = 0)   ' If data is received,

N10 = UART1_Read()              ' read the received data,
```

```
  WHILE (UART1_Data_Ready() = 0)   ' If data is received,
  N11 = UART1_Read()               ' read the received data,


  WHILE (UART1_Data_Ready() = 0)   ' If data is received,
  N12 = UART1_Read()               ' read the received data,


END SUB
```

SUB PROCEDURE MTN()

```
 UART1_Write_Text("0722699096")
 UART1_Write(34)     '  "
 UART1_Write_Text("SITE 4540 KITENGELA")
 UART1_Write_Text("INTRUSION DETECTED")
END SUB
```

SUB PROCEDURE BDC()

```
 UART1_Write_Text("0764591332")

 UART1_Write_Text("SITE 4540 KITENGELA")

 UART1_Write_Text("UPS FAILURE")

END SUB
```

SUB PROCEDURE MAINS()

```
 UART1_Write_Text("0764591332")

 UART1_Write_Text("SITE 4540 KITENGELA")

 UART1_Write_Text("MAINS FAILURE")

END SUB
```

SUB PROCEDURE GENR ()

```
 UART1_Write_Text("0764591332")

 UART1_Write_Text("SITE 4540 KITENGELA")

 UART1_Write_Text("GENERATOR FAILURE")

END SUB
```

SUB PROCEDURE TEMPS()

```
UART1_Write_Text("0722591332")       ' 0722591332

UART1_Write_Text("SITE 4540 KITENGELA")

UART1_Write_Text("TEMPERATURE HIGH")

UART1_Write(TEMP )

UART1_Write_Text(" DEGREES")

END SUB
```

MAIN:

```
    Lcd_Init()                    ' Initialize LCD

    Lcd_Cmd(_LCD_CLEAR)           ' Clear display

    Lcd_Cmd(_LCD_CURSOR_OFF)

    Lcd_Out(1,1,"GSM REMOTE")

    Lcd_Out(2,1,"MONITOR")

    DELAY_MS (30000)              '3000

    Lcd_Cmd(_LCD_CLEAR)
```

REP:

Lcd_Out(1,1,"TM:"): Print TM on LCD

TEMP=ADRESL

Lcd_Chr(1,4, ((TEMP div 10)

Lcd_Chr(1,5, (TEMP)

IF TEMP>30 THEN

IF TT=0 THEN

TT=1

TEMPS()

END IF

END IF

""""""""""""ADC END""""""""""""

''''''''''''**MOTION START**''''''''''''''''

```
  IF PORTC.3=1 THEN
    Lcd_Out(1,7,"INTRSN")
    MT=1
  END IF
''''''''''''''MOTION END'''''''''''''''
''''''''''''''POWER START'''''''''''''''
  IF PORTC.0=0 THEN          'DC
    Lcd_Out(2,1,"UPSF")
    DCC=1
  END IF

  IF PORTC.1=0 THEN          'MAINS
    Lcd_Out(2,6,"AC F")
    AC=1
  END IF
```

```
 IF PORTC.2=0 THEN           'GEN
    Lcd_Out(2,11,"GN F")
    GN=1
 END IF
''''''''''''''''POWER END''''''''''''''''
''''''''''''''''GSM START''''''''''''''''
   IF MT=1 THEN
    IF CMT=0 THEN
       CMT=1
       MTN()
    END IF
   END IF
  IF DCC=1 THEN
   IF CDCC=0 THEN
      CDCC=1
```

```
    BDC()
 END IF
END IF


IF AC=1 THEN
 IF CAC=0 THEN
    CAC=1
    MAINS()
 END IF
END IF


IF AC=1
DELAY_MS (30000)
 IF GN=1 THEN
  IF CGN=0 THEN
    CGN=1
    GENR()
```

```
 END IF

END IF
```

RID()

```
IF N1=65 THEN          'A...  UNLOCK
   PORTD.0=1
END IF

IF N1=66 THEN          'B...  LOCK
   PORTD.0=0
END IF

INC(CM)
INC(CM2)

DELAY_MS(1000)
```

```
  IF CM2>4 THEN      '5
    CM2=0
    PNDEL()
  END IF

  IF CM<30 THEN      '5
    GOTO REP
  END IF
 TT=0
MT=0
DCC=0
AC=0
GN=0
CMT=0
CDCC=0
CAC=0
CGN=0
```

```
    GOTO REP


END.
```