DESIGN AND IMPLEMENTATION OF THE TELECOMMUNICATION AND UTILITY CABLE TAMPERING MONITORING SYSTEM

by

Patrick Mabadie

211113360

Submitted in fulfilment of the requirements for the

Magister Technologiae: Engineering: Electrical

Department of Process Control and Computer Systems

Faculty of Engineering and Technology

VAAL UNIVERSITY OF TECHNOLOGY

Vanderbijlpark

Supervisor: Prof. MO Ohanga

9th March 2019

DECLARATION

I, Patrick Mabadie, student number 211113360, hereby declare that the dissertation entitled Design and Implementation of The Telecommunication and Utility Cable Tamper Monitoring System is the result of my own research and presents my own work and that all the resources that I have used or quoted have been indicated and acknowledged by means of complete references. I further declare that I have not previously submitted this work, or part of it, for examination at Vaal University of Technology for another qualification or at any other higher education institution.

Patrick Mabadie

09th March 2019

Date

ACKNOWLEDGEMENTS

My gratitude to my family and friends for their doubtless faith and massive support, and also thank GOD for my ability and determination.

I would like to express my deepest gratitude to my supervisor Prof. Marcel Odhiambo Ohanga and Prof. Ezra Kirunda for their commitments to this research. I would like to thank them for their continued support, guidance and invaluable input towards the completion of this research.

ABSTRACT

The telecommunication and utility cable monitoring system was implemented to protect the cable tampering. Cable tampering occurs despite the fact that methods have been developed, to solve and decrease cable tampering cases such as cable tampering prevention campaigns at the national and international level, organizing security patrols, replacing existing cable with fiber cables and I-Watch system installation. The objective of the research was to design and implement a cable tampering monitoring system which is able to monitor, detect, pinpoint the location and give the distance from the sensor at which the cable tampering took place. The system is an improvement on the traditional cable anti-theft monitoring system, the method of tracking resonance signal frequency was implemented. The system incorporates a sensing circuit which detects a change on the capacitance value of the cable and converts it into an equivalent frequency value, Field-Programable Gate Array (FPGA) board is utilized to convert the frequency into the cable length (the distance from sensor of cable which was taken away), after detecting an anomaly on the cable (tampered with) the output of the system is divided into two parts which are display mode and messaging mode. For display mode, the system uses a Liquid Crystal Display (LCD) which displays the GPS Coordinates of the location where the cable tampering took place and the distance from sensor of the cable which has been tampered with. In the messaging mode, the FPGA activates the GSM module and the module sends alert flag message to the user when the cable is tampered with.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

GLOSSARY OF TERMS

AC	Alternative Current
ADC	Analog to Digital Converter
ASCII	American Standard Code for Information Interchange
AVR	Automatic Voltage Regulator
BW	Bandwidth
CAT	Cable Anti-Theft System
CN	Capacitance
CO_2	Carbone Dioxide
CRO	Cathode Ray Oscilloscope
CTMS	Cable Theft Monitoring System
DC	Direct current
EAGLE	Easily Applicable Graphical Layout Editor
ESD	Electrical Discharge
FPGA	Field-Programmable gate array
GPS	Global position system
GPRS	General Packet Radio Service
GSM	Global system mobile
GUI	Graphical User Interface
IMEI	International Mobile Equipment Identity
LCD	Liquid crystal display
LED	Light Emitting Diode
I_{in}	Current signal with a variable frequency
LN	Inductance
MAX3238	Serial Module
MATLAB	MATrix LABoratory and the software
MCU	Microcontroller Unit
MHz	Mega Hertz
NIOS II	32-Bit Embedded-processor Architecture
SIM	Subscriber Identity Module
SMS	Short Message Service
OH	Overhead
PC	Personal Computer

PCB	Personal Computer board
PIC	Plastic Insulated Conductor
PROTEUS	Application for schematic capture, simulation and PC Board layout design
QUARTUS II	Programmable logic device design software
RF	Radio Frequency
RTL	Register-Transfer Level
RS232	Serial Communication Port
SRAM	Static Random-Access Memory
THR	Threshold
TDR	Time Domain Reflectometer
TRI	Trigger
TX	Transmit
U	Voltage signal
UART	Universal Asynchronous Receiver Transmitter
UFL	Upper Flammable Limit
URL	Uniform Resource Locator
VCC	IC power Supply
VHDL	VHSIC Hardware Description Language

CHAPTER ONE: INTRODUCTION

1.1 Introduction and Background of the Study

Cable theft phenomena concerns power and telecommunication lines in numerous places on the globe. Cables being tampered with, not for their original purpose but to sell the material, particularly copper used in making the cables. However, cable theft has spread over the years; it has turned out to be an important issue that results from the high cost of the metal. Cable theft is prevalent not only in emerging economies/countries but also in developed countries. For instance, in the United States of America, the telecommunication service provider has a habitual problem with copper cable theft in some pole-mounted cables of their access network (Berinato, 2007). The transport police agents, who maintain the security of the rail network, declared cable theft as among the highest concern in the United Kingdom (Andre, 2012).

However, the issue of cable theft is most severe in megalopolis. 190,000 Incidents of cable theft over a year were recorded in China, about 53,000 in 2005 alone (Andre, 2012). In 2006, Eskom, the Electricity utility provider in South Africa suffered cable theft, which cost about ZAR20 million. Meanwhile Transnet Freight Rail in 2006, lost cables valued at ZAR5.5 million (Andre, 2012). Construction building sites in South Africa have been targeted by armed gangs in such a way that the cables are tampered with even before its installation.

East of Johannesburg, in Springs, the Telkom services were disrupted because of some multiple incidents of cable theft in the area. More than 1,000 residences and companies were affected by this crime. Telkom's underground infrastructure cables were cut and removed by thieves on Wednesday, 6 June 2012 (Andre, 2012; Staff, 2012 & Hess, 2012). These particular cables supply power to seven street cabinets in adjoining areas.

According to Broun (2004), electricity thefts can take many forms, which can be stealing of electricity supply (illegal connections), fraud (meter tampering), unpaid bills and irregular billing. The consequences of all these types of theft are the reduction in incomes for the Electricity and Telecommunication service providers and the need to charge customers more. The increase in electricity theft in over 102 countries between 1980 and 2002 is evidence of the cable theft (Smith 2004).

1.2 Problem Statement

Telecommunication and utility copper cable theft is an extensive problem that results in high income losses to the communication and utility service providers totalling several billions of Rands per year (Comins & Rizwana 2010). The effect of cable theft increases the disruption of

the services. Cable monitoring systems are important because they will provide solutions for cable tampering/theft and improve the data services.

1.3 Aim and Objectives of the Study

The main aim of this study is to design and implement cable tampering monitoring system that is able to pinpoint the location where the tampering might take place, and provide the distance from sensor (cable length) which was taken away. The aim further extends to the investigation of the performance of cable theft monitoring solution.

The purpose of this study is to design and implement a cable monitoring system, investigate the level of performance of the cable monitoring system, especially to determine if the implemented cable monitoring system can detect an anomaly during cable tampering. In addition, give the performance of the system with respect to the tampering location and the position of the sensor.

The main objective of this study is design and implement a telecommunication and utility cable tamper monitoring system that is able to pinpoint the location of cable tampering. This objective is further divided into the following sub-objectives:

(i) To design and implement system's prototype.

(ii) To investigate the performance level of the effect of the distance on the monitoring system and its accuracy.

(iii) To improve the reading accuracy of the cable monitoring system in such a way that it detects any short and open circuits on the cable by using a sensing circuit.

1.4 Layout of the Dissertation

Chapter 1, introduces the thesis and highlights the motivation and importance of the research. It discusses aim, objectives and concludes with the road map of the dissertation. Chapter 2, discusses previous work and results achieved, provides an analysis of the problem and the proposed solution to the cable tampering monitoring system, the problem to be solved is the presented as four separate sub-problems the determinations and proposed solution conclude the chapter. Chapter 3, describes the capacitance current resonance and discusses the work of the principle references in this study. Chapter 4, describes the analysis of the proposed solution and different components which was used in the design. Chapter 5, presents the methodology and design to achieve the aim of a cable tampering monitoring system using the equations to determine the distance from sensor being tampered with, pinpoint the location where the

tampering took place and alert the user. Chapter 6, presents the implementation of the cable tampered monitoring prototype with FPGA, sensing circuit and GSM module. Chapter 8, discuss the tests done on the prototype and list the results achieved. Chapter 8, provides an analysis of the simulation test results to determine if the objectives of the research were achieved. Chapter 9, concludes the research and it summarises and reviews all the work done, discuss the implications of the findings and concludes with suggestion for further research work.

1.5 List of Publications

Conference papers:

1. Patrick Mabadie and Marcel Ohanga Implementation of current capacitance resonance circuit to monitor telecommunication and utility cable tampering. ICTAS2019, March 6th, 2019. IEEE International Conference on Information Communications Technology and Society (IEEE ICTAS 2019) Blue Waters Hotel, Marine Parade, Durban.
2. Patrick Mabadie and Marcel Ohanga. Design and Implementation of Telecommunication and Utility Cable Tampered Monitoring System. 3rd VUT Interdisciplinary Research and Postgraduate Conference 2018 17-18th October 2018 – Quest Conference Centre.
3. Patrick Mabadie and Marcel Ohanga. Design and Implementation of Telecommunication and Utility Cable Tampered Monitoring System. SAIEE, Africa Research Journal, Research Journal of the South Africa Institute of Electrical Engineers

CHAPTER TWO: REVIEW OF CABLE MONITORING SYSTEM METHODS

2.1 Introduction

This section provides a brief review of the different cable monitoring systems and their respective methods of detection (Current detection method, Voltage detection method, Capacitance detection method, Signal detection method and the Wireless signal transmission method) and then focuses on the method (Capacitance detection method) which closely meets the requirements of the project objectives. This chapter reviews the following existing solutions:

(i) Voltage Detection Method.

(ii) Current Detection Method.

(iii) Capacitance Detection Method.

(iv) Signal Transmission Method/Power Line Carrier Wave Communication.

(v) Wireless Signal Transmission Method.

This chapter reviews technologies based on the existing solution mentioned above and points out the deficiencies in each method within each category. Detecting and locating faults on a cable is important and has been done using several existing and developing strategies. The most common strategy of testing cables is, to measure the resistance from end-to-end (Furse, Chung, Dangol, Nielsen, Mabey & Woodward, 2003). This strategy can be utilized to identify cold solder joints, bad crimps, carbonization of the cable or connectors, and foreign matter on or near the cables. This strategy can be utilized on a fueled airplane (unlike high voltage tests), but it is difficult to pinpoint the faults location. In addition, it is difficult to miniaturize and is costly.

2.2 Related Work

The detection and location of cable tampering is crucial in addressing the problem of cable theft. This section discusses most of the cable tampering monitoring solutions, available benefits and deficiencies. These once identified in most of research papers reviewed, has been categorized as followed:

2.2.1 Cable Theft Monitoring System (CTMS) Using Global System Mobile (GSM) Modem

This system is based on voltage detection method, it checks if the cable is tampered with or not by identifying whether the end of the cable is charged. It is basic and dependable, in any case with the shortcoming that it only works for long-term detection alarm cables. As for the street lighting cables, it fails to identify and check during the daytime without power.

Mohd Chachuli (2016) presented a cable monitoring system based on a voltage divider method. This system detects any change in the temperature in the circuit as well as the voltage drop over the cable. If there are any changes, the microcontroller sends information to the Global system mobile (GSM) module to notify the users via a message of the noted discrepancy. The same microcontroller can activate a buzzer for audible warning and a light warning to indicate that cable theft has occurred. This system locates the area where the tampering took place and the information is included in the message notification. If the temperature is between 10 and 40 degrees Celsius, and the voltage is being between 0 to 10 volts, the system will not set any alarm or message notification, but if the system is outside of this range, warning light will switch ON. A notification message will be sent through the GSM Module, and the temperature and the voltage detected will be displayed on the Liquid Crystal Display (LCD). However, the deficiency of this system is that it does not give the information of the exact location at which the cable tampering took place also the voltage detection method, only works for long-term detection alarm cables. For the street lighting cables, it fails to detect and check during the daytime without electricity.

2.2.2 Anti-Theft and Monitoring System of Street Lamp Power Cables

This system is based on the current detection method, it monitors the current leakage based on the following principle: To begin with it makes the three-phase four-wire cable go through the transformer for testing at the same time, concurring to conventional circuit judging, its normal value ought to be zero or a particular initial value (that is, the initial leakage value). it can make the leakage intentionally by the end of the line between the front lines and the earth, and its detection value should to be more than the initial value. So once the detection value return to zero or the initial value, it sends alarm flag promptly with the assumption that the cable is cut off. This approach is achievable in theory, but it is ordinarily not the same case in real situation. Here are the impediments in detail:

(i) It is difficult to find out the initial value of detection. The leakage of cables does exist, the damage caused by laying from time to time, and the value is subject to differ concurring to weather conditions (damp or dry). In other occasion, the leakage occurs after a long time rather than when installing. Therefore, it is difficult to determine a particular value, and it is continuously changing. As a result, it often gives the alert by mistake at the starting of installation and stops sending alarm signals if the initial value is turned up.

(ii) During the daytime when the electricity fails, the cable guard will not work.

(iii) This system is based on the principle of current capacitance resonance, which is a current signal indicating a variation of frequency. The current signal with a frequency varying is injected in the street lamp power system; from the received current signal, the circuit capacitance can be calculated using the resonance frequency. The resonance frequency obtained from the system enables the determination of the cable length, and the capacitance, and from that the detection of the point at which the cable has been tampered with can be determined.

2.2.3 An Anti-Theft Street Cable Monitoring System

This system is related to the current detection method and was presented by Deepak, Shudhanshu and Ankit (2013). This system is based on the principle of current capacitance resonance, which is a current signal indicating a variation of frequency. The current signal is injected in the street lamp power system, from the received current signal the resonance can be calculated. The resonance obtained from the system enables the determination of the cable length, as well as the capacitance, and from that the detection of the point at which the cable has been tampered with can be determined. The disadvantage of this system is that it only works when the light is ON and is influenced by voltage fluctuations, but this can also easily be influenced by the climate changes.

2.2.4 A Novel Anti-Theft Monitoring System

This system is related to the current detection method and presented by Xiaorui *et al.* (2014), the system is based on the current capacitance resonance, by injecting a variable frequency constant signal into the street lamp system. The signal goes through the cable up to its far end. In the situation that the cable is uniform the frequency signal is then absorbed at the far end of the cable but if the cable has an anomaly the signal will return where it is originated therefore, a judgement can be made as to whether the cable has been stolen or not. Figure 2.1 shows the simplified street lamp branch, which is created based on an adjustable anti-theft measure schematic diagram. This circuit is composed of a variable capacitance (C_n), an inductance (L) which is connected in series with the capacitor (C), the resistor (R), and the (Z_{in}) which represent the impedance of the system. By injecting a signal with variable frequency into the monitoring circuit, the phase difference between the signal voltage (U) and the signal current (I_{in}) can be measured. When the phase difference is zero, which is the resonance, this signal frequency is the resonance frequency of the system.

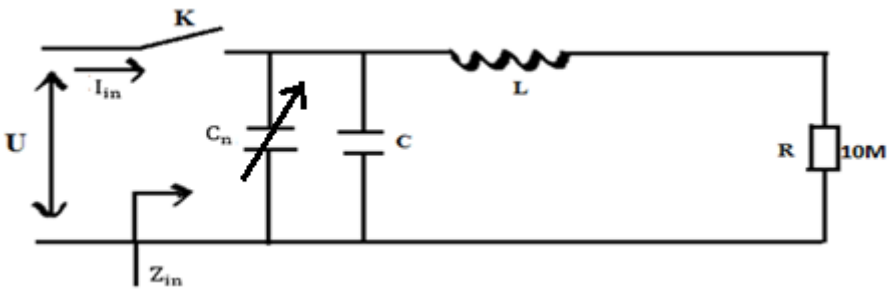

Figure 2.1: Current capacitance resonance simplified circuit (Xiangjun, *et al.,* 2008)

The capacitance of the cable can be calculated through the resonance measurement method, and the location of the breaking line can be detected. The deficiencies of the system are mentioned as follow:

(i) The leakage current measurement method is affected easily by the climate condition and is operated only when the street lamp is ON.

(ii) Working current measurement method is affected by the voltage fluctuation, the reliability of the method is limited.

2.2.5 Anti-Theft Monitoring and Location System for Cable of Street Lamp

This system is related to the capacitance detection method, Yuanyuan *et al.* (2011), presented a system to monitor cable theft by tracking the resonance frequency. Figure 2.2, illustrates the system; which is able to locate where the cable-theft has occurred. The system is composed of an inductance $\{L_n\}$ which is connected in parallel with the measured capacitance $\{C_n\}$, the voltage signal return $\{U\}$; and the current signal $\{I_{in}\}$. This particular current with a variable frequency is inserted into the cable anti-theft system; from which the voltage signal return $\{U\}$ is obtained. A comparison is made between the phases of the return voltage and the current signal. If there is no difference between the two signals it indicates that there is resonance; and the uniform signal obtained is the angular frequency and is also the resonance of the system.

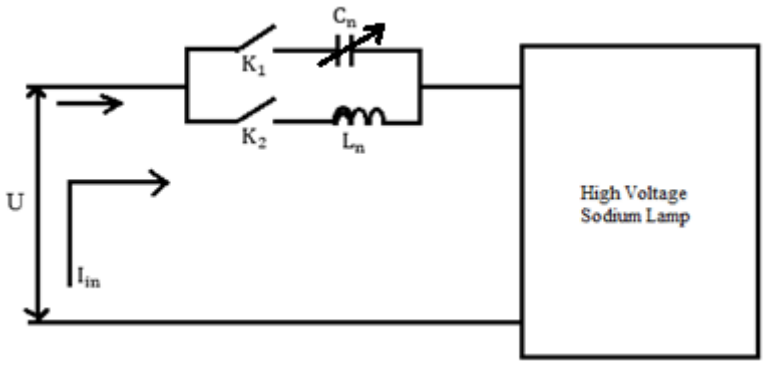

Figure 2.2: The Cable Anti-Theft monitoring system principle (Yuanyuan, *et al.*, 2011).

If there is a difference between the return voltage signal and the current signal, the conclusion is that the cable has been tampered with. The stolen street lamp cable length can be calculated by taking the measurement frequency. However, this system has location faults within a certain range.

2.2.6 Anti-Theft and Location Method Based on Pulse Transmission Attribute of Power Cable

The system is based on signal transmission and power line carrier wave communication method, the system introduced by Xiaorui *et al.* (2014) is a power cable monitoring system based on the propagations of low voltage pulses in the cable. This system works in three phases:

(i) Firstly, all the known faults like low resistance and break-line are analysed theoretically. A pulse signal of a low voltage is introduced into the cable conductor's head, the returned signal is detected by amplitude observation, and transmission waveform of the low voltage pulse is significantly different in terms of polarity and amplitude between tampered cables and the resistance fault.

(ii) Secondly, based on the common faults, an identification strategy is made on the reflected pulse and threshold value, which is the maximum value that can be obtained in terms of pulse amplitude.

(iii) Finally, the impedance mismatch: the fault location is determined by measuring the time difference between the reflected pulse and the original pulse. This particular method is mainly used for low resistance such as short-circuit and open circuit fault detection.

This system uses the Direct Current (DC) impedance measurement, the system needs an extra installation of a DC load at the end of the cable street lamp; and taking into consideration the fact that the cable is buried under ground, it suffers from influence such as substantial rainfall. The DC impedance is not infinite which causes a high false alarm rate. This same system also uses power wave carrier receiver equipment which is connected at the end of the cable. The system is costly. The cable is affected by its capacitance which limits the transmission range and it cannot locate cable theft when it occurs.

2.2.7 Compact Copper Cable Anti-Theft System Solution

This system is based on the wireless signal transmission method, Bahrin and Muhammad (2016), proposed an anti-theft monitoring kit for cables, specifically for telephone lines, electrical cables, other types of communication cables, and relates precisely to the equipment for cable theft detection by sensing the cables vibration. The cable anti-theft (CAT) device

consists of a microcontroller and vibration sensor which has been adjusted to detect the vibration pattern of the theft attempts with several techniques such as theft attempt using dagger, jigsaw and cutter. The device contains a General Packet Radio Service (GPRS) and GSM to determine the location of where the cable is tampered with and to receive a SMS with an indication of the location of the incident as well as the cable information. However, the deficiency of this system is that it can easily be influenced by the climate changes.

2.2.8 Industrial Real-Time Measurement and Monitoring System

This system is based on the wireless signal transmission method, Wen-Tsai *et al.* (2011), presented an industrial real-time measurement and monitoring system which is based on an embedded system with Zigbee. Zigbee embedded system is the main component of the improvement in the industrial safety quality, in addition to the existing performance of the monitoring functions. This system is composed of a wireless transmission technology which allows remote monitoring, industrial applications, and some measurement items which are:

(i) Length filtering;

(ii) Ground vibration sensing;

(iii) Carbon dioxide concentration.

This system is able to monitor all parameters mentioned above with the help of some sensors. Mendoza *et al.* (2005), presented a real-time monitoring system based on Field-Programmable Gate Array (FPGA). This is a system that acquires data from different kinds of sensors, transfers the data by radiofrequency to a computer which has an interface module, and is situated at 900m radius. The system allows the sensors to perform in a large area. It is also able to monitor crop local environment and physiological status. This system was built on a chip approach, using different types of sensors and compared with some greenhouse commercial monitoring systems conditions.

2.2.9 GSM-based remote sensing and control system using FPGA

This system is based on the wireless signal transmission method, El-Medany, (2008), presented a remote sensing and control system which is based on GSM and uses FPGA. The authors implemented a remote home security system, which is composed of a Global System for Mobile (GSM), Very High-Speed Integrated Circuit (VHSIC) Hardware Description Language (VHDL) and this is implemented in hardware using Field Programmable Gate Array (FPGA). The system works as a remote sensing for the electrical appliance at home and checks whether it is ON or OFF, then sends data to the owner of the house via SMS. The advantage of this system is that it can achieve multi-inputs and outputs control. Figure 2.3 illustrates the remote

sensing and control system architecture, which gets data from the sensors for different appliances such as lights, heat, doors, etc. Data gathered from the sensors is converted to digital signal, processed by the FPGA, and SMS is sent to the owner of the house.

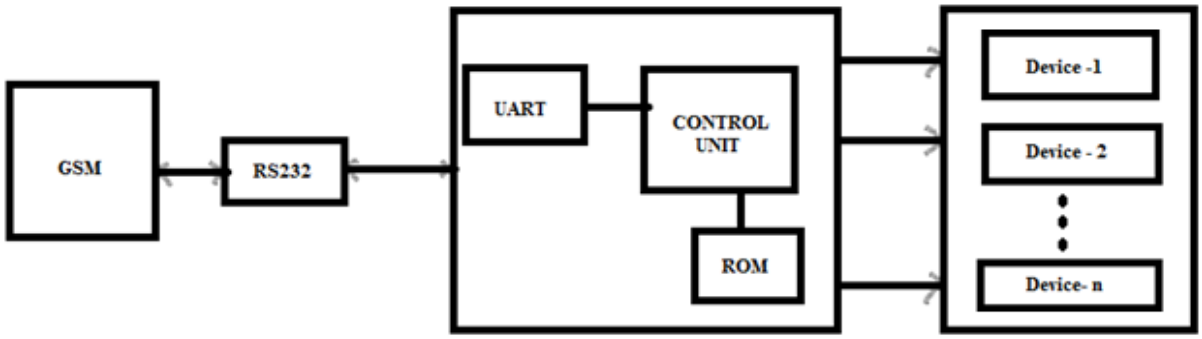

Figure 2.3: Architecture of the remote sensing and control system (El-Medany, 2008)

Zang (2008), presented a cable guard, which is commonly used in the cable guard technology. The system mainly works on the signal transmission and signal detection, the cable guard is based on the power line carrier communication method. This method works as follows: It is a power line which carries simultaneously data and electric power, the power line is transformed into a data line using the superposition of low energy information signal to a power wave (Galli, 2014). When the frequency of the electricity is between 50 to 60 Hz, the data is transmitted in KHz to avoid any interferences with the data. The challenge of this method is that the power wiring is unshielded and untwisted, so it acts as an antenna and emit radio energy which interferes with other users of same frequency band (Schwager, 2014).

2.2.10 Detection of Low-Voltage Power Cable Guard Alarm Mechanism

This system is based on the wireless signal transmission method, using GPRS/GSM innovation or wireless information radio that, introduce launchers at the cable end such that power failure and power login record can be reported and the cable default can be additionally detected by the main station. Nevertheless, the deficiencies are higher costs, strong reliance on higher wireless communications, and issues of battery power line carrier. Zhen Yu (2009), presented a system based on the cable guard alarm technology. This system detects low-voltage power cable guard alarm mechanism and uses impedance measurement of alternating sampling algorithm. In addition, it has a combination of power line carrier and a new mechanism for an integrated cable guard alarm system. This mechanism is based on fuzzy logic to judge the quality of the current and calculate the protected setting value. It gives the alarm detection signal, through the electric current dynamic analysis when the cable is tampered with or stolen. Sulaiman *et al.* (2016), presented a system which is a Compact Copper Cable Anti-Theft System Solution (CAT). It is a first entry level deterrent system which protects

telecommunication overhead (OH) cable from theft. This system is composed of GSM and GPRS module and vibration sensor which has been calibrated to detect the vibration pattern such as theft, using tools such as Jigsaw, Dagger and Cutter. The system is composed of a lithium ion battery to power the device. When the cable is tampered with, the system notifies the alarm and GSM notification. Debbarma (2014), implemented a system which is able to monitor flood. This system uses sensors and processing in Field-Programmable Gate Array (FPGA) board. The sensors measure parameters such as:

(i) Water pressure;

(ii) Water level;

(iii) Flow temperature.

Data collected from the sensor is converted to digital data, processed by the FPGA board then the data is sent to a computer which compiles the data and detect if there will be a flood or not. This system has been implemented using Xilinx Spartan 3E and FPGA start kit board. El-Medany & El-Sabry (2008), presented a temperature remote sensing system, which is based on FPGA. The system is composed of FPGA, GSM and VHDL. The main function of this system is to control the greenhouse climate such as: inside temperature, Carbon dioxide (CO_2) and relative humidity which improves the soil status and the crop production. The system has two units; the control center and the system board illustrated in Figure 2.4. The control center is composed of two units; the mobile phone which is connected to the FPGA via a serial communication port (RS232) and the Computer. The system board is composed of three units; the sensor circuit, the GSM module and the main controller (FPGA). If any humidity or temperature exceeds the threshold level, a message is sent through the GSM network.

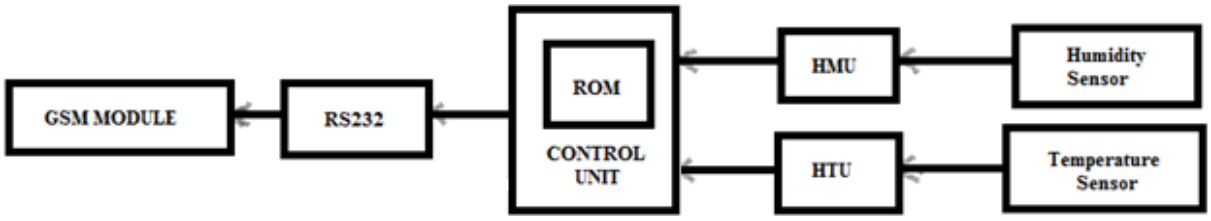

Figure 2.4: Temperature remote sensing system composition (El-Medany, 2008)

Chung *et al.* (2009), presented a system which is able to detect lengths of open and short-circuit using capacitance inductance sensor circuit. The researchers analysed and tested inductance sensing circuit and capacitance to find the best performance of this system at finding open and short circuit. This system is composed of different 555 timer circuit, Schmitt Trigger oscillator, two invertors and three gate oscillators. The system is able to indicate the location of open circuit and short circuit on wires with least error. The deficiency is that the power line carrier

method requires an installation of a power wave carrier receive device at the end of a cable, and it is costly. This method is affected by the capacitance of the cable; therefore, its transmission range is limited. This method does not detect the location of the breaking line.

2.3 Proposed Solution

The proposed solution is to design and implement a cable monitoring system capable to detect cable tamper, indicate the distance from sensor cable and the location at which the cable has been tampered with. The reason for choosing the modified capacitance was that it meets the aim and objective of the research closely and it will improve the efficiency and performance of the cable monitoring system, by adding a sensing circuit which is a time domain reflectometer capable of locating discontinuities such as faults in electric cables, to addressed the challenge of a cable theft monitoring system.

The proposed solution is different from the other in that:

(i) The cable theft monitoring system uses a sensing circuit and FPGA technology, which uses microcontroller technology, will detect the point at which the cable is tampered with, which is not addressed by any of the current systems of anti-theft cable monitoring systems.

(ii) The system will detect the location at which the cable has been tampered with.

The cable tampering problem has been attempted before but with no solution to detect the location at which the cable has been tampered with. Several proposed cable theft monitoring systems with different existing solutions have been reviewed in this section. It becomes important to compare their efficiencies and performances to determine which approach results in better cable theft monitoring system performance. It is noticeable that the implemented cable monitoring system lack the precision when it comes to detecting the exact location where the cables have been tampered with and determining the distance from sensor of the stolen cable.

2.4 Chapter Conclusion

This chapter presented numerous cable tampering monitoring existing solutions that can lead to a considerable cable saving. The methods that has been presented in this chapter result in high detection of cable tampering and pinpoint the location of cable tampered. Most of them however, failed to address the issue of pinpointing the location at which the cable has been tampered with, and to accurately determine the length of affected cable. The main objectives are to develop a system that detect tampering on a cable, determine the length of tampered cable and in addition, the specifically locate the point where the cable is being tampered with.

CHAPTER THREE: AN OVERVIEW OF CURRENT CAPACITANCE RESONANCE USING TIME DOMAIN REFLECTOMETER (TDR)

3.1 Introduction

Time domain Reflectometers (TDR) have been around for a long time and are the quickest, and most precise way to pinpoint cabling problems. Historically, the TDR was reserved for certain companies and high-level engineers (Raymond & Woodward, 2000). This was due to the complexity of operation and high cost of the instruments. The TDR has been significantly underutilized. Riser-Bond Instruments recognized these deficiencies and developed the first "little TDR" in the early 1980s (York, Evans, Pokusevski & Source, 2001). The simplified digital TDR has presently become a standard device for the first level technician. Riser-Bond Instruments' completed the production line with the concept that the equipment should be as simple as possible, accurate and user friendly.

3.2 Principle of the Current Capacitance Resonance

Due to recent developments and innovation in the electronic industries, the operation and interpretation of a TDR have been significantly simplified. Because of its capacity to distinguish cable issues, the TDR is presently regaining notoriety throughout communications industries (Smail, Hacib, Pichou & Loete, 2011). If a cable is metal and it has at least two conductors, it can be tested by a TDR. TDRs will troubleshoot and measure all sorts of twisted pair and coaxial cables, both airborne and underground. TDRs are utilized to find and distinguish deficiencies in all sorts of metallic combined cables. It can also find major or minor cabling issues including; sheath deficiencies, broken conductors, water damage, loose connectors, crimps, cuts, smashed cables, shorted conductors, framework components, and a variety of other fault conditions. In addition, TDRs can be utilized to test reels of cables for shipping damage, cable deficiencies, cable utilization, and inventory management (Furse *et al,* 2003). The speed and exactness of the time domain reflectometer makes it today's favored strategy of cable fault location. Because of the fact that today's instruments are more user friendly, a great understanding of the fundamental principle and applications of a TDR is a productive investigation system. Like all modern equipment, getting to know the instrument and its operation makes the TDR a more profitable tool.

A TDR transmits a small rise time pulse along the cable pair. If the cable pair is of a uniform admittance and properly terminated, the whole transmitted pulse will be absorbed in the far-end termination and no signal will be reflected toward the TDR. Any impedance discontinuities

will cause some of the incident signal to be sent back towards the source. This is similar in principle to radar. An increment in the impedance (an open cable pair) makes a reflection that fortifies the original pulse. A decrease in the impedance (a solid short) makes a reflection that opposes the original pulse (Waddoups, 2001).

The resulting reflected pulse that is measured at the output/input of the TDR is plotted as a function of time, and since the speed of signal propagation is moderately steady on a cable pair, the total time of the pulse down and back can be examined as a function of cable length. Because of its sensitivity to impedance varieties (Zhengya, 2003), a TDR may be utilized to identify cable impedance mismatch characteristics, such as: an open cable pair, a shorted cable pair, a grounded cable pair, a splice, a load coil including a smart coil, a capacitive construction in a section of cable, the starting of a horizontal or bridged tap, the end of a horizontal or bridged tap, series resistance, water in a section of air core Plastic Insulated Conductor (PIC) cable, and to estimate cable lengths (Jani, 2003). The average impedance of a telephone cable pair is 100 Ω. When utilizing a TDR planned for telephone cables the base line is 100 Ω. A few TDRs indicate the impedance by coordinating the display line to a reference on the screen.

3.3 Principles of Operation

The TDR operates on the same principles as radar. A pulse of energy is spread down the cable. When that pulse reaches the end of the cable, or a fault along the cable, a portion or all of the pulse energy is reflected back to the instrument. The TDR measures the time it takes for the signal to travel down the cable, see the anomaly, and reflect back. The TDR records data within this time and shows the data as a waveform and/or distance reading.

The TDR dispatches a short rectangular step of voltage down the cable. The wave travels to the far end of the cable, where it is reflected back at the end of the cable. TDR requires a fast-rise time pulse generator and quick voltage sampler to identify the reflected signal, and it is moreover exorbitant and difficult to miniaturize (Kueck, Kirby, Overholt and Markel, 2004). Capacitance measurement have been utilized for locating anomalies on cables, however previous literature has not discussed on how to locate cable tampering. The capacitance of an open circuited cable and inductance of a short-circuited cable are linearly proportional to their lengths. There are numerous methods of measuring capacitance, but the one which match closely the research objectives is a 555-timer circuit which was used to detect the distance from sensor cable tampered. (Edang, 2001). Any conductor has a capacitance with respect to ground or another conductor. The capacitance will depend on the area and physical shape of the

conductors and the permittivity of the dielectric isolating the conductors from ground. A long wire can be thought of as a series of these localized capacitors, and the bulk capacitance of an open circuited wire is directly proportional to its length. Additionally, short-circuited cable behaves like a series of inductances at low frequencies, and the bulk inductance is directly proportional to the length.

3.4 Capacitance and Inductance of Wire and Sensors

The measurement of the cable length is done using different methods, capacitance, inductance and sensor method, it is imperative to understand the range and variation of these values for realistic cable types. This chapter describes these values both analytically and experimentally. Expression 3.1 presents the mathematical model for calculate the capacitance of a conductor Where (C) is the capacitance values of any two conductors, (d) is the distance between the conductor and ground, (S) is the area across the two conductors and (Ɛ) is the permittivity of the dielectric separating the conductors (Ɛ=$\varepsilon_r\varepsilon_0$; ε_0=8.854E-12 F/m). In this case ε_r is the relative permittivity to the permittivity of air ε_0. For two parallel plates, the well-known equation for capacitance is given in equation (3.1) as:

$$C = \varepsilon\frac{S}{d} \text{ in Farads (Amin and Wollenberg, 2005)} \quad (3.1)$$

The capacitance and inductance values have been modeled and calculated (Amin and Wollenberg, 2005). For two circular parallel conductors (circular wires) the capacitance (C) and inductance (L) are given by:

$$C = \frac{\pi\varepsilon}{\cosh^{-1}(\frac{D}{d})} \text{ in Farads (Netl Modern Grid Strategy, 2008)} \quad (3.2)$$

$$L = \frac{\mu}{\pi}\cosh^{-1}\frac{D}{d} \text{ high frequency, Henry (Patrick and Fardo ,2009)} \quad (3.3)$$

$$L = \frac{\mu}{\pi}\left[\frac{1}{4} + \cosh^{-1}\frac{D}{d}\right] \text{ low frequency, Henry (Willis and Schrieber, 2012)} \quad (3.4)$$

where D is distance between the two centers of the conductors and ε is the permittivity of the separator. μ is magnetic permeability of the dielectric (μ=$\mu_r\mu_0$, μ_0=4πE-7 H/m). μ_r is the relative permeability. μ_r and ε_r of polyethylene are about 0.994~1.0017 and 2.5~2.7, respectively.

Twisted pair wire has about 20% greater capacitance than simple parallel wire due to extra length from twists (Park, Yang and Lee, 2011). This total capacitance is given by:

$$C_{Total} = \frac{\pi\varepsilon_0}{\cosh^{-1}(\frac{D}{d})} + \int_a^b \frac{\varepsilon_0 dx}{D-\sqrt{D^2+x^2}} + \int_a^b \frac{\varepsilon_0 dx}{D+\left(\frac{1.0}{\varepsilon_r}-1.0\right)\sqrt{D^2+x^2}-\frac{\sqrt{d^2+x^2}}{\varepsilon_r}} \text{ (Tichelman, 2007)} \quad (3.5)$$

where (a) is the radius of internal conductor, and (b) and (c) are the inward and external radius of the shield (Willis and Schrieber, 2012). Capacitance and inductance values of coaxial are:

$$C = \frac{2\pi\varepsilon}{\ln\frac{b}{a}} \text{ in Farads (Nieuwenhout, Dogger and Kamphuis, 2005)} \quad (3.6)$$

$$L = \frac{\mu}{2\pi}\left[\ln\frac{b}{a} + \frac{1}{4} + \frac{1}{4(c^2-b^2)}\left(b^2 - 3c^2 + \frac{4c^4}{c^2-b^2}\ln\frac{c}{b}\right)\right] \text{Henry (Rahimi and Ipakchi,2010 (3.7)}$$

ε is the permittivity of separators between the internal conductor and the shield. Figure 3.1 shows the capacitance values of five distinctive open circuited for airplane wires as a function of length measured using a Liquidity Coverage Ratio (LCR) meter which is an electronic testing device used to measure inductance (L), Capacitance (C) and Resistance (R) of any electronic equipment.

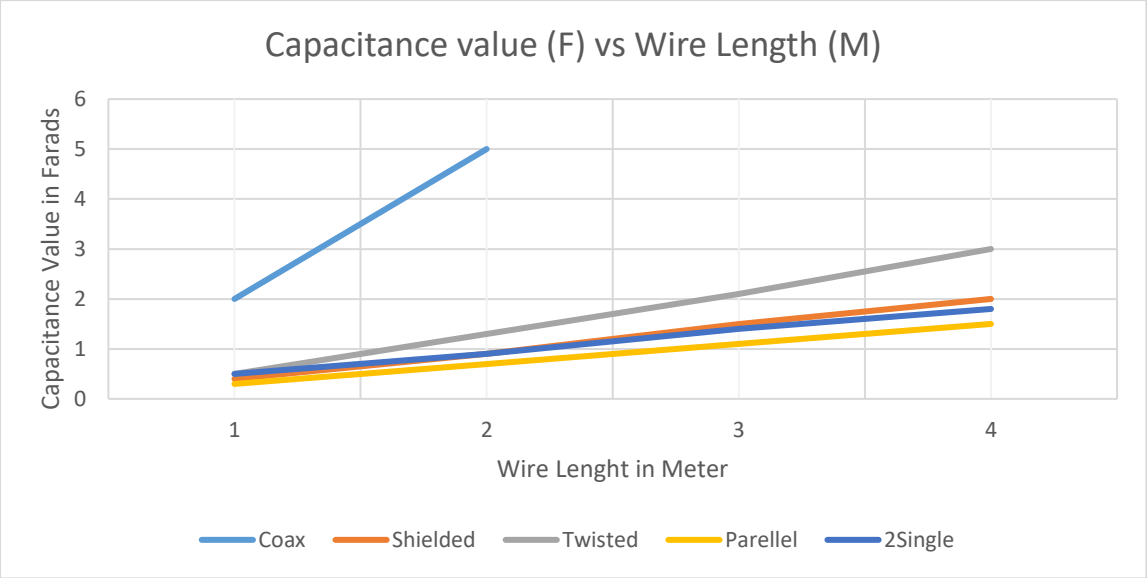

Figure 3.1: wire length vs measured capacitance of 5 different open circuited for airplane wires using LCR meter.

Table 3.1 gives the specifications on the type of wires, military part numbers, and the measured capacitance and inductance per unit length for each wire.

Table 3.1: Measurement results of capacitance and inductance of wire

Wire type	Part Number	Line Type for Figures	Pf/m	Uh/m
Coax	C4931-22l		339	0.161
Twisted Shielded Quadruple	M27500-22SC4S23		106.5	0.517
Twisted shielded triple	M27500-24SC3S23		100.5	0.55
Twisted pair shielded	M27500-2408T23		102.4	0.544
Thick twisted triple	M81381-11-12		90.29	0.467

Figure 3.2 shows the inductance values of the same wires when short circuited. The coaxial cable is seen to have the largest inductance per unit length followed by shielded twisted pair cable. inductance value of parallel individual wire (single wire) is similar to twisted pair cable, but slightly lower. Among the same type of wire, the thicker wire (lower gauge) has larger inductance per unit length. The lowest inductance value is found from the single parallel wires in a bundle, since the distance between the wires is small, within a bundle of wire (often 20-150 wires), the inductance could vary due to the wire not staying in the same part of the bundle, and subsequently vary the distance between two wires forming a test pair. This was found not to be large. Variations of about 4 pF out of 350 pF and 0.01 µH out of 9.20 µH for 392 inches (9.95 m) long M22759/16-22-90 in a bundle of 20 wires was measured (Li, Qiao, Sun,Wan and Zhang, 2010).

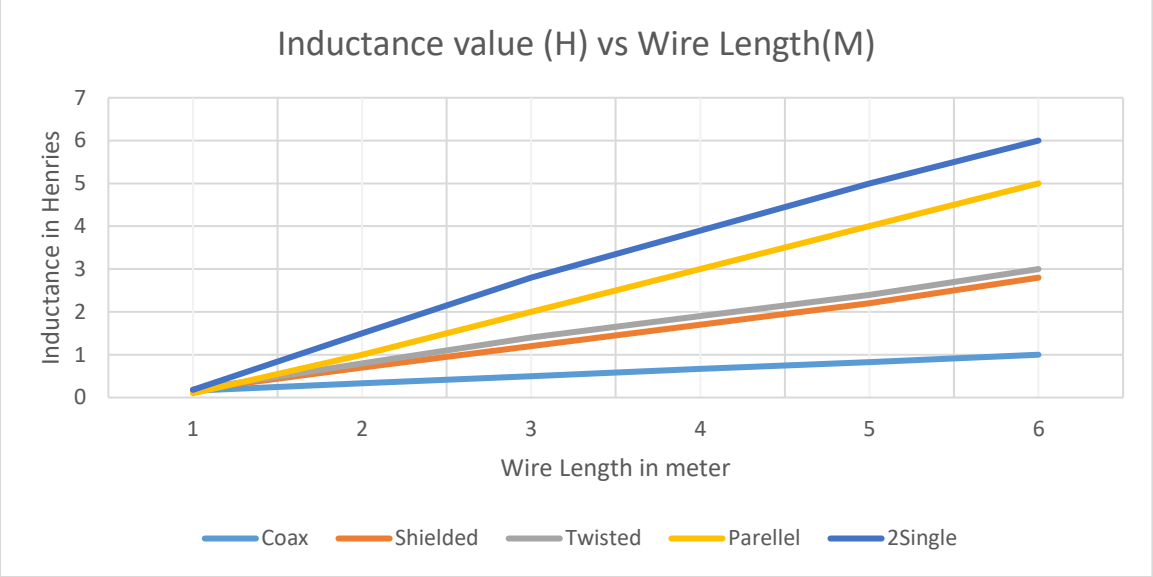

Figure 3.2: wire length vs measured inductance of 5 different short-circuited wire cable LCR meter

Figure: 3.2 shows the measured inductance value of the same wire types when they are short circuited. The coaxial cable has the slightest inductance per unit length. From Figures 3.1 and 3.2, it can be seen that a wire with higher capacitance value has lower inductance value. Figure 3.2 shows result of five different types of cables that have been shorted. The inductance value from the five different types of wire are linear and increase accordingly. Clearly the capacitance and inductance can be utilized to measure the length of wires and the distance to faults. There are various circuits for measuring these values (Tichelman, 2007) they are not all similarly effective.

3.5 Capacitance and Inductance Sensors

The following section discusses the capabilities, points of interest and disadvantages of a several sorts of capacitance sensors. Sensors for measuring capacitance and inductance can be broadly separated into two categories:

(i) One type of sensor uses the wire as an inductive or capacitive component in a resonator circuit. As example of such sensors the two-inverter oscillator, difference amplifier and 555 timer sensors.

(ii) Another type of sensor uses the capacitance or inductance of the wire as an impedance and measures the voltage drop between different impedances in the circuit. The voltage divider is an illustration of this class of sensor.

Few circuits are more vulnerable to stray capacitances or inductances, more or less precise, have ranges of measurement that are more or less effective, and in common work better for measuring wire length or distance to fault than other methods.

3.5.1 The Two-Inverter Oscillator

A two-inverter oscillator is a constant multi-vibrator (Li, Xiaoguang, Jian and Ketai, 2011). It comprises of two inverters and a Resistance Capacitance (RC) Network, as shown in Figure 3.3 the output of each inverter is either logic 0 or logic 1, each corresponding to a static voltage.

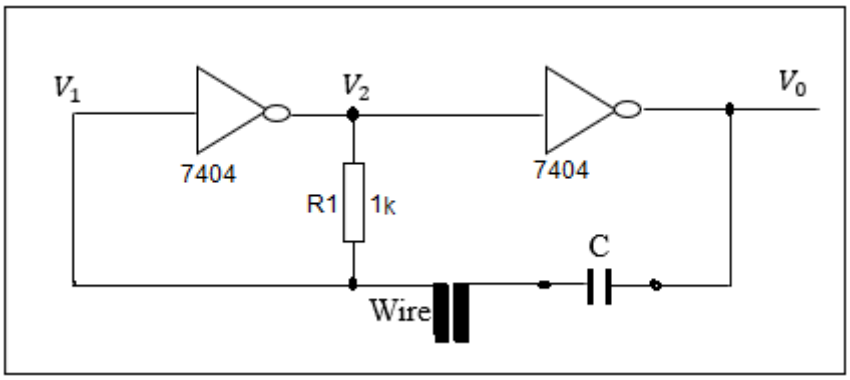

Figure 3.3: Two Inverter Oscillator for open and short circuit wire (Han and Lim, 2010)

The input V_1 can vary gradually between certain range, because it is the voltage of the insulated gate. No current flows into the input. The only possible current path is between nodes V_2 and V_0. The current indicates that when V_1 is logic 1, V_2 and V_0 will be logic state 0 and logic state 1, respectively. Then V_1 is greater than the inverter switching voltage. The voltage over R_1 produces a current (i), which charges the capacitor, in this case the wire, causing voltage accross the capacitor (V_c) to rise. Thus V_1 drops. When it is lower than the inverter switching voltage, the inverter switch states. The respective logic levels of V_2 and V_0 are now 1 and 0. The current

(i) reverses, and v_c drops until V_1 rises over the inverter switching voltage. then the inverters once more switch states. Thus, the RC circuit which acts as an oscillator will result to the frequency generation and the expression is given as:

Open circuit:

$$F(Hz)=\frac{(C_w+C)}{(5*C*C_w*R)} \text{ (Cho, } et\ al.,\text{ 2007)} \quad (3.8)$$

Short circuit:

$$F(Hz)=\frac{(1+L_w*C_w)}{(5*R*C_w)} \text{ (Cho, } et\ al.,\text{ 2007)} \quad (3.9)$$

where C is the capacitance, C_w is the capacitance due to the open circuited wire, L_w the inductance due to the shorted wire. The value chosen during the experiment for the oscillator are R = 1KΩ, V_{cc} = 3.2V, C = 50 pF

3.5.2 Differential Amplifier for Open and Short Circuit

A non-inverting or inverting operational amplifier circuit has a gain defined by the feedback resistor (R_f). The change in output voltage due to the change in capacitance is very small in certain cases, Figure 3.4 shows the simplified difference amplifier.

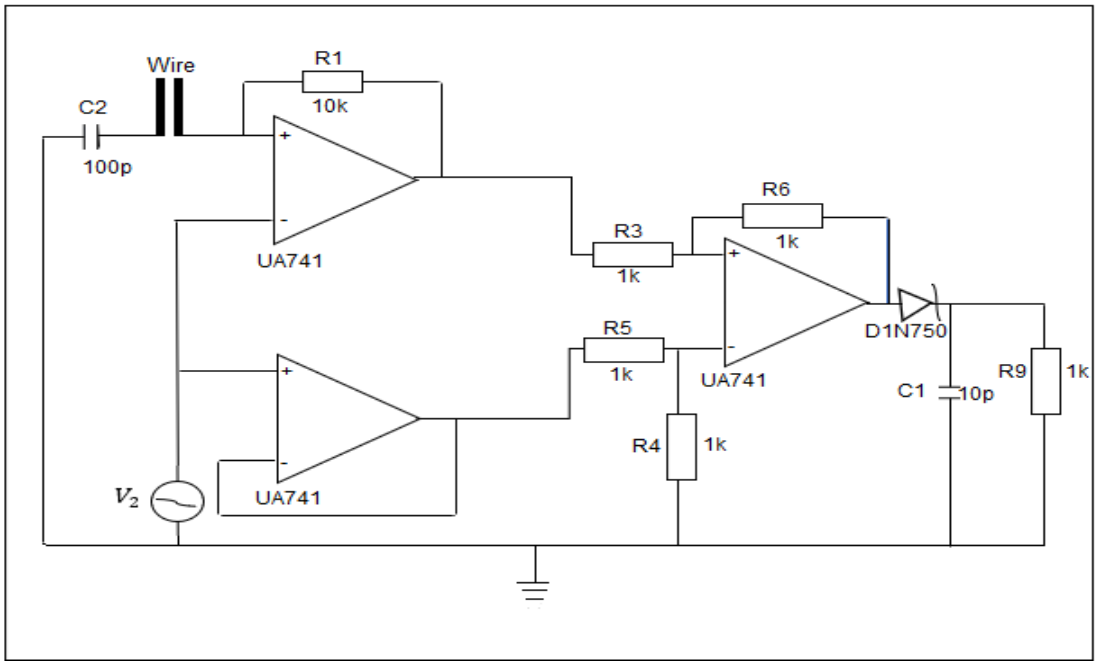

Figure 3.4: Difference amplified sensor for open and short circuit wire (NSTC, 2000)

The amplifier output is fed to the non-inverting terminal of the differential amplifier and the follower output (which is the same as the input voltage) is fed to the terminal of the differential amplifier, the final output can be obtain using the equation below:

Open Circuit

$$V_0(V) = \frac{V_{in} * R_f * \omega * C * C_w}{C_w + C} \text{ (Aranguren, 2002)} \quad (3.10)$$

Short Circuit

$$V_0(V) = \frac{V_{in} * R_f * \omega * C^2}{L_w * \omega^2 * C - 1} \text{ (Gandla, Waleed, Al-Assadi, Sedigh and Raghu, 2008)} \quad (3.11)$$

where R_f is the feedback resistance, C denotes the reference capacitance, C_w represents the capacitance due to the open circuited wire, L_w means the inductance due to the short-circuited wire, V_{in} is the input voltage, V_0 the output voltage

3.5.3 555-Timer Circuit for Open and Short Circuit Measurement.

A 555-Timer connected as an Astable multi-vibrator is a well-known strategy for finding faults on open circuited wire (Edang, 2001). The frequency output for open circuited wires is given by the equation 3.12.

$$F(Hz) = \frac{1.433}{[(R_a + 2R_b)C]} \text{ (Inyiama and Obota, 2013)} \quad (3.12)$$

The values of the resistors (R_a and R_b) and the capacitance (C) can be adjusted to test short circuited wires as shown in Figure 3.5. The values used are R_a = 1kΩ and R_b = 10MΩ to get a 50% oscillation duty cycle, the values are obtained from the work presented in reference (Edang, 2001).

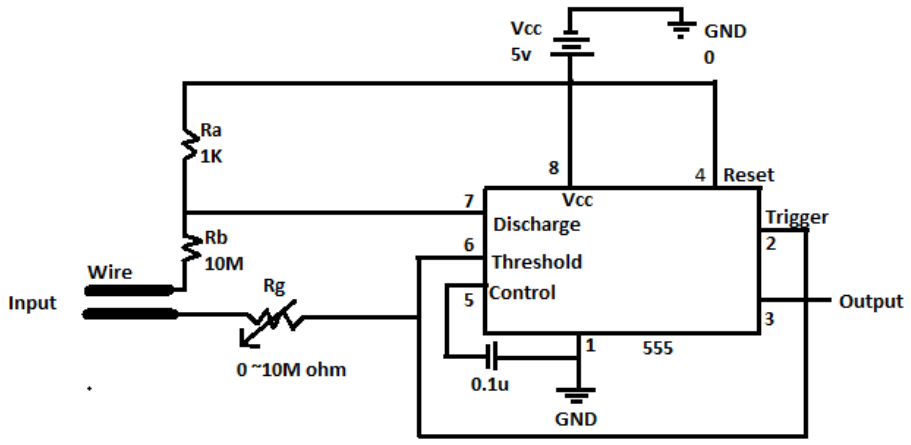

Figure 3.5: Sensing Circuit for fault detection on wire (Fujiyama Hiroyuki, 2006)

This circuit detect an open and short circuits because a short-circuited wire produces DC output with the timer for open circuited wire (Edang, 2001), and an open circuited wire produces DC output with the timer circuit in Figure 3.5 for short circuited wire. The period of the output is

plotted in Figure 3.6, and both open and short-circuited setups are shown to be exceptionally linear. The maximum length that was tested was 60 meters long. In theory this circuit can locate faults on wires up to almost 1000m long. When speckled the value of R_a and R_b to get the best output possible in Figure 3.5.

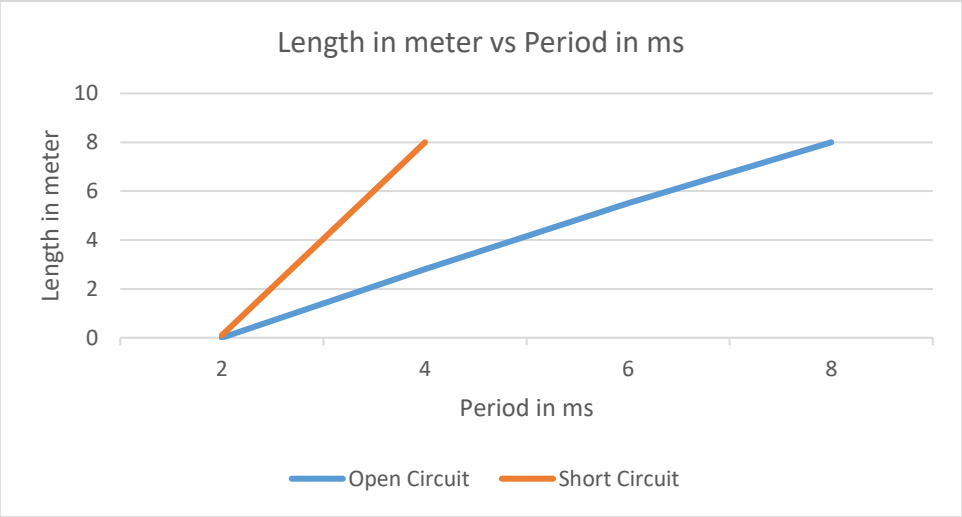

Figure 3.6: Time output period vs length of the twisted pair shielded wire

According to Chung, Amarnath, Furse & Mahoney (2009), the analysis done on the three different methods of detecting open and short circuit:

(i) Two Inverter Oscillator Sensors
(ii) Differential Amplifier
(iii) 555-Timer Circuit

The most efficient circuit is the 555-Timer Circuit hence, it is used in this research project. The 555 timer and differential amplifier can locate both open and short-circuited wires with the slightest error. Most extreme errors for the open and shorts circuit were 5.3 cm and 20 cm, and for the differential amplifier were 7.93 % and 28.43 %, respectively (Chung *et al.,* 2009). Calibration of these systems can be done by measuring wires of the type that will later be tested and storing the coefficients of a linear fit to that data. If no calibration is done, and the average values are utilized, error of order 1~5cm for open and 1~20cm for short would be seen. Hence it is strongly recommended that the type of wire and its gauge be known and utilized for calibration.

3.6 Conclusion

This chapter presented an overview of the current capacitance resonance method. The reason of choosing this method. The next chapter will give information about the proposed solution. All the component of the proposed solution will be presented, explained and analysed.

CHAPTER FOUR: COMPONENT DESCRIPTION OF THE TELECOMMUNICATION AND UTILITY CABLE TAMPER MONITORING SYSTEM

4.1 Introduction

This chapter decomposes the proposed solution into components (modules), the modules are analysed and the function of each modules is presented.

4.2 Modules of the Proposed Solution

The proposed solution is broken down into modules the following:

(i) Sensing circuit
(ii) FPGA Board
(iii) GSM Module
(iv) GPRS Module
(v) RS232 connector
(vi) PC Server

4.2.1 Sensing Circuit

The sensing circuit detects the capacitance value when the cable is tampered with and convert it into the exact equivalent frequency value and sends to the FPGA board. The input of the FPGA is the output of the sensing circuit. The sensing circuit is used to detect and locate open circuit along the cable, in case of cable tampering the sensing circuit sends a signal using the 555-Timer Reflectometer Circuit to the FPGA board.

The sensing circuit is a modified version of the time domain reflectometer which is a dominant technique (Scott, Wraith & Dani, 2002). A short pulse is generated from the circuit and propagated down, if the cable is of uniform impedance and is properly terminated, then there will be no reflection. The pulse generated is absorbed at the far end of the cable, instead if there are impedance variations which are caused by the tampering with the cable, then the generated pulse is reflected back to the source, information such as: sign, magnitude, capacitance value, phase delays of the signal and frequency can be obtain and interpreted. The obtained results are used to determine the distance from sensor cable tampered with. TDRs are widely used especially in aviation and naval craft troubleshooting (Edang 2001).

4.2.2 FPGA Board

The FPGA board uses a processor to convert the frequency value gathered from the reflectometer (sensing circuit) into equivalent distance from sensor cable. This device acts like a remote monitoring for cable tampering. It uses a frequency counter to convert frequency to a

length (distance from sensor) when the cable has been tampered with. The FPGA also compile data received from the sensing circuit and the GPRS and send an alert message through GSM wireless network to the user mobile El-Medany *et al.* (2008).

When the cable has been tampered with, the sensing circuit detect it and send data to the FPGA. Once the FPGA receives the data it converts the frequency into the distance from sensor (length) and activates the GPRS to get the coordinates where the cable is tampered with. The FPGA display the distance from sensor cable tampered and the location on the LCD screen and instantaneously sends instant messages to the users' mobile with the respective data mentioned herein. 7-Segment display is used to display the counter clock (Frequency). From the sensing circuit when the cable is tampered with and, the LCD screen, display data received from the sensing circuit as well as from the GPRS when a cable has been tampered with.

4.2.3 Global System for Mobile (GSM) Module

The GSM module receives data from the FPGA then send it to the respective user. The GSM module is used to send instant messages and alerts to the users or the person in charge of the system. The message contains information about the cable which has been tampered with, the distance from sensor cable tampered with and the location where the anomaly took place (Cao, Xu, Liu, Ye & Xu 2011).

4.2.4 General Packet Radio Service (GPRS) Module

The GPRS module is used to get the GPS coordinates of the location at which cable tampering took place. These coordinates are sent to the FPGA immediately after a cable has been tampered with.

RS232 Connector: The RS232 is used as a connection between the sensing circuit and the FPGA and between the FPGA and the GSM module. The device provides an easy and quick communication with the FPGA board (Mackay, Wright, Reynders & Par, 2004). Data is composed of the GPS coordinates of the location where the cable tampered occurred and the length of cable taken. This data is stored only after an anomaly has been identify on the cable (Henle, Kuvshinoff, 1992). Alarm Indicator: The alarm is triggered ON when cable tampering has been detected by the sensors and the data transfer to the FPGA. Once the cable is tampered with, the safety level which is programmed at FPGA controller, should be able to decode the information and activate the port in which the buzzer is connected to start the alarm sound (Chenebert, Breckon & Gaszczak, 2011). Power Supply Module: The foundation of a reliable system is a good power supply, because of the peak current needed from the GPRS module,

sensing circuit, FPGA board and the other modules. Designing a good power module must be taken into consideration (Malmstadt, Enke & Crouch, 1981).

4.3 Chapter Conclusion

This chapter presented and analysed a telecommunication and utility cable tampering monitoring system. The proposed solution is designed to improve on an existing system, the system was decomposed into modules and analysed. The function of each module was presented for clarification of the proposed solution.

CHAPTER FIVE: DESIGN OF THE TELECOMMUNICATION AND UTILITY CABLE TAMPER MONITORING SYSTEM

5.1 Introduction

This chapter presents the design of the proposed solution and is divided into five major sections. The first module, is the Sensing circuit together with its subsection; the second part describes the FPGA module with all its subsection; the third module presents GSM module, the fourth part illustrates the GPRS modules with its subsection and the fifth part details the RS232 and the final part explains PC server. The availability of the resources (components) has been specified and the system output specifications and the circuit design are given.

5.2 Research Design

Monitoring performance improvements and cable theft monitoring system accuracy requires the utilization of effective strategies. Assumption in the proposed research:

(i) The combination of the sensing circuit with the current capacitance resonance method will improve the cable tampered monitoring system and the detection of the distance from sensor.

(ii) The combination of the FPGA and the GPS will give accurate coordinates of the location where the tampering took place.

(iii) The sensing circuit will be able to detect the change in the capacitance value of the cable and proceed the information to the FPGA.

The reason for choosing the FPGA is because it has been proven to be a better piece of equipment than a basic microcontroller. Thus, the FPGA board replaced the microcontroller in building the prototype.

This project explored the results of combining the current capacitance resonance method with a sensing circuit. The importance of adding a sensing circuit to the current capacitance resonance is to detect cable tampering. The two combined system together were tested by simulation on software such as PROTEUS. Information were gathered and calculations done in parallel with the simulation, to observe the optimized reading accuracy. In addition; to the cable monitoring system, which uses the current capacitance resonance method, the substitution of the microcontroller by the FPGA gate was done and the monitoring performance simulated by the software mentioned above. Different data was gathered and calculation done, as well as observations done to determine the changes in monitoring performance of the cable tamper monitoring system.

A Quantitative experimental approach was used in this research, various cable length were analysed. Simulation of the cable theft monitoring was implemented and determination of the performance of the current capacitance resonance measurement in combination with a sensing circuit and FPGA gate. The monitoring of performance and reading accuracy was analysed and compared with the simulation against the objectives. MATrix Laboratory and the software (PROTEUS), application for schematic capture, simulation and PC Board layout design (PROTEUS) simulation was used in the project. After having the PC Board layout done, the components were assembled to build the prototype.

5.3 Sensing Circuit

The sensing circuit is used to locate faults in a metallic cable; a short pulse is generated and propagated down the cable. Thereafter the reflected signal returns to the generator, interpretations are done based on the phase, delay and the frequency of the received or returned reflected signal.

The sensing circuit acts like a sensor to detect the capacitance value of the cable and to convert it into the exact equivalent frequency value and send it to the FPGA board. The input of the FPGA is the output of the sensing circuit. The Sensing circuit in this project was used to detect and locate anomaly on the cable, in case the cable is tampered-with, the sensing circuit sends a signal using the 555 timer Reflectometer circuit to the FPGA board.

The sensing circuit in this system is a reflectometer sensing circuit. It has a capacitance sensor which detects the capacitance value of a cable and converts it into an equivalent frequency value and sends it to the input of the FPGA board. Figure 5.1 (Fujiyama Hiroyuki, 2006), shows the 555-timer arranged with multi-vibrator to compose the reflectometer circuit which senses and detects the location of open circuit and short circuit on a cable. The circuit is adapted to the test open and short circuit cables, the value of the two resistances R_a = 1 kΩ, R_b = 10MΩ, C_1 = 0.1uF, C_2 = 11.373Pf~568.650pF are chosen to find 50 % oscillation duty cycle.

The cable is connected to the sensing circuit. When the cable is tampered with it will be in the open circuit mode and the capacitance or Electrical Discharge (ESD) effect occurs.

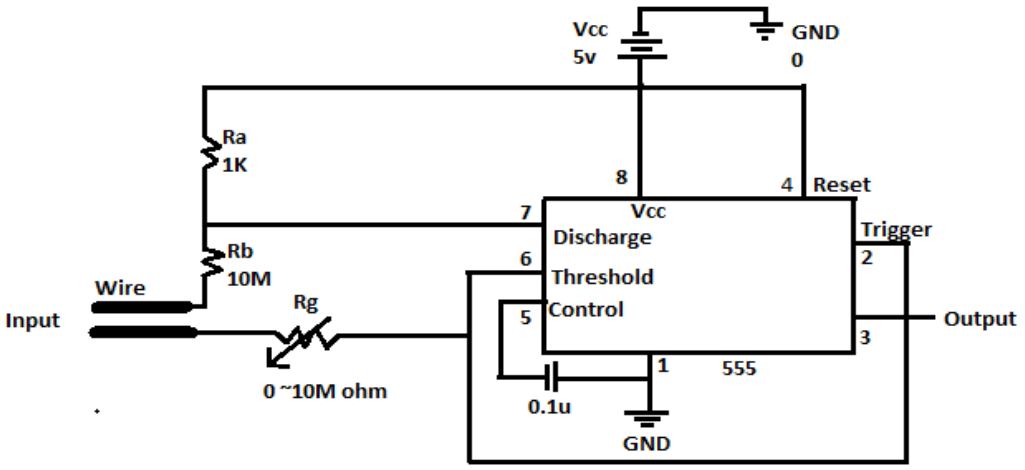

Figure 5.1: Sensing circuit (Fujiyama Hiroyuki, 2006)

Equation 5.1 gives the approach of the relation of proportionality between the distance from sensor and the capacitance value.

$$\frac{\text{Distance from tampered sensor,L2}}{\text{Original Distance from sensor,L1}} = \frac{\text{Original Cable Frequency,f1}}{\text{Frequency of tampered cable,f2}} \quad (5.1)$$

The sensing circuit detects the capacitance value of the cable and converts it into an equivalent frequency. The device launches a short step of voltage, this voltage travels down the cable till the end and reflects back to the source. If the capacitance value C_1 correspond with the return value C_2 then no tampering was detected but if there is a difference between the capacitance C_1 and C_2, the returned value (C_2) is converted to a frequency using equation 5.2:

$$F(Hz) = \frac{1.433}{[(R_a+2R_b)C]} \text{ (Inyiama and Obota, 2013)} \quad (5.2)$$

5.3.1 Relationship between Capacitance Value (Frequency) and Distance from Sensor

A live copper cable is connected to the sensing circuit. When the copper cable is open after being tampered with, the capacitance effect occurs. The capacitance value of the cable is proportional to the distance from sensor cable. If the value of the cable capacitance increases, the distance from sensor increases as well and vice versa. Based on the equation 5.1 the distance can be calculated and hence the distance from the tampered sensor is determined.

According to Meier & Jhangiani (2007), the reflection is caused by the mismatch on the impedance. The slight change in the dielectric constant from the AC signal between modules can change the result of the characteristic impedance and the impedance mismatch. Even though the power loss caused by the reflection is an occurrence which is applicable to all AC systems measurement errors, power loss becomes remarkable when the cable in the system is greater than 1/100 wavelength of the signal traveling through the cable. The Radio Frequency

(RF) signal having a shorter wavelength, is more vulnerable to power loss due to reflections rather than lower frequency signal. The relationship between the wavelength and the distance from sensor cable is illustrated by equation 5.1. The comparison between the propagation characteristics of 1 MHz sine wave and a 1 GHz sine wave. The wavelength of the two signals can be calculated using the equation 5.3.

$$\lambda = (V_f)\frac{v}{f}m \text{ (Zeng, YI \& Lui, 2008)} \quad (5.3)$$

where,

λ = the wavelength of the signal

v = high velocity

f = the frequency, and

V_f = the velocity factor of the cable. {Taking in consideration the type of cable in both systems with a velocity factor of 0.66}.

The result of the above example with a 1MHz of frequency is

$$\lambda_1 = 0.66\frac{3\times10^8}{1\times10^6}m = 198m,$$

and result of a 1GHz signal is given by equation 5.3.

$$\lambda_2 = 0.66\frac{3\times10^8}{1\times10^9}m = 0.198m.$$

The signal which has a frequency of 1GHz, is $1/5^{th}$ of the distance from sensor cable (Meier & Jhangiani, 2007), meaning that five cycles of that particular signal propagates along the cable at any time. This small wavelength signal adopts the waveform when the propagation takes place along the cable and reflects at junctions with different type of impedance.

5.4 FPGA Module

In this project the FPGA is responsible for transferring data from the sensing circuit to the GSM module, and convert data (frequency values) to corresponding distance from sensor. The component is used in the design to analyze the data coming from different inputs (components) such as GSM, GPRS and the Sensing circuit. Input coming from the sensing circuit (frequency value), is converted to an equivalent distance from sensor by the FPGA, then sent to the LCD. Input coming from the GPRS (GPRS coordinates) are gathered by the FPGA, then sent to the LCD. Input coming from the GSM (distance from sensor and GPRS coordinates) are gathered

by the FPGA then sent to the users as well as to the Computer Server to keep historical records of the cable tampering. The FPGA module configuration follows the following steps:

Step 1: Design a frequency counter on Quartus II. Quartus II is a programming architecture used on the FPGA module.

Step 2: The coding is compiled in Quartus II and error checking are done.

Step 3: If there is an error while compiling the Program the system restarts from step 1, if there are no errors while compiling the program them it moves to step 4.

Step 4: Load the program into the selected Device (FPGA);

The steps that have been stated above are shown in the flow diagram in Figure 5.2.

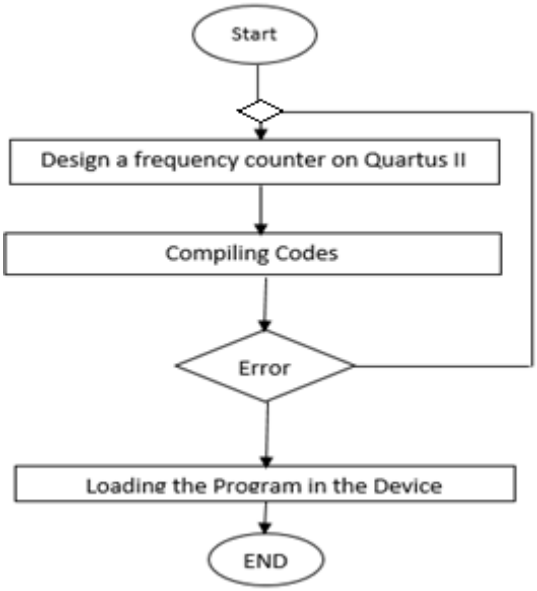

Figure 5.2: Flow diagram of Quartus II

5.4.1 The Quartus II Configuration Code

Figure 5.2 shows Flow diagram of the design procedure for the FPGA, the steps of coding which is done in Quartus II and taking into consideration the error handler. Then the program load into the FPGA. Table 5.1 presents the pseudo codes on how the program works in the FPGA. The pseudo codes present information about input ports.

List of notations

Symbol	Meaning
FI1	FPGA input pin 1
FI2	FPGA input pin 2
FO1	FPGA output pin 1
FO2	FPGA output pin 2
VF	Velocity Factor of the cable
SL	Speed of Light

Table 5.1: Pseudo Code of Quartus II for FPGA module

```
1:      Begin
2:        Inputs: FI1, FI2, Result;
3:        Outputs: FO1,FO2;
4:        Initialize FO1,FO2,FI1,FI2;
5:        Declaration of constant VF=0.66, SL=3*10^8,
6:      While FP1≠0 do
7:        Obtain data from the sensing circuit
8:         Set  FI1 equal to output value of the sensing circuit
9:         Set Result = VF*(SL/FI1);
10:     Return Result
11:       Set FP2 equal to output value of the GPRS
12:       Display ("LAT"+FP2+"LON"+FP2+"DIS"+Result)
13:       Set FO1 =  FO2 = FP2 + Result
14:     End
```

A program was developed using Quartus II software. This program was built using Verilog Language for frequency counter. The purpose of this frequency counter is to detect and process the frequency received at the input of the FPGA. The frequency received is then converted into an equivalent distance from sensor cable using equation 5.4.

$$\text{Cut Cable Length, L2} = \frac{\text{Original Cable Frequency,f1}}{\text{Cut Cable Frequency,f2}} \text{X Original Cable Length, L1} \qquad (5.4)$$

One of the outputs of the FPGA displayed the information concerning the distance from sensor, the GPS coordinates of the place where the tampering took place, on the LCD panel of the FPGA device. The second program was developed using Nios II software and uses C language. This program is used to control the GSM and GPRS modules. The purpose of this program is to send SMS alert to the user mobile, (the PC server) and to request the coordinates from the GPRS of the location where the tampering took place.

The FPGA is connected with the Sensing Circuit in such a way that the output of the Sensing circuit is connected to the input of the FPGA through a RS232 which is illustrated in Figure 5.3. The other connections of the FPGA are the power supply, ground, LCD display and the outputs. The GPRS provides medium speed data transmission and is used to give GPRS location and coordinates of the location where the tampering took place. GPRS is connected with the FPGA through the serial port or RS232 and sends information to the GPRS Modem to regulate its data transmission is shown in Figure 5.4. The peak current of the GPRS is about 2 Amps when the Modem is starting to connect with the network, therefore the power module needs to provide a current for more than 2 Amps.

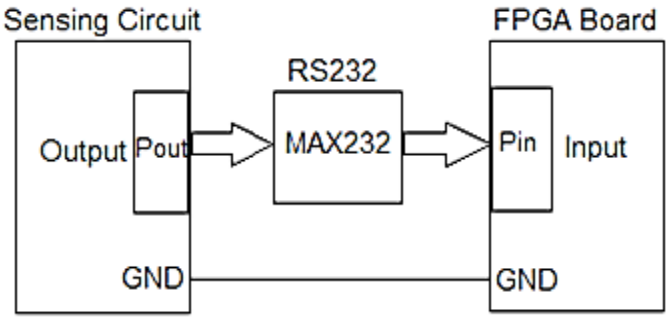

Figure 5.3: Connection between Sensing circuit and FPGA

Figure 5.4 shows the connection between the FPGA module and the GPRS modem, the TXD 0 interface which connects the FPGA and the GPRS module.

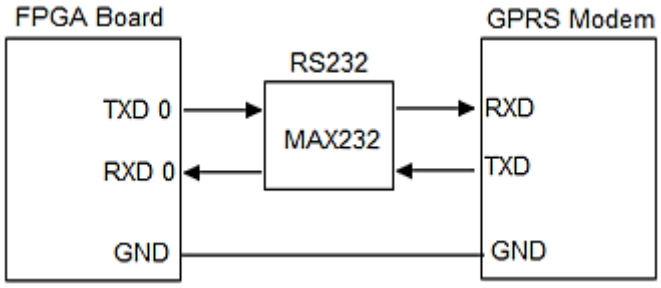

Figure 5.4: Connection between the FPGA and the GPRS Modem

5.5 GSM Module

The GSM is triggered by the FPGA, this GSM sends data such as the distance from sensor and the GPRS coordinates to the users of the system.

Configuration follows the following steps:

Step 1: Design of a program for GSM on Nios II.

Step 2: The coding is compiled in Nios II and the error checking is done.

Step 3: If there is an error while compiling the Program the system restarts from step 1; if there are no errors while compiling the program then it moves to step 4.

Step 4: Load the program into the selected Device (FPGA).

Step 5: Check if the data has been transmitted. If not, the program then moves to step 1.

The steps 1-5 are shown in the Figure 5.5 and Nios II configuration Code shown in Table 5.2.

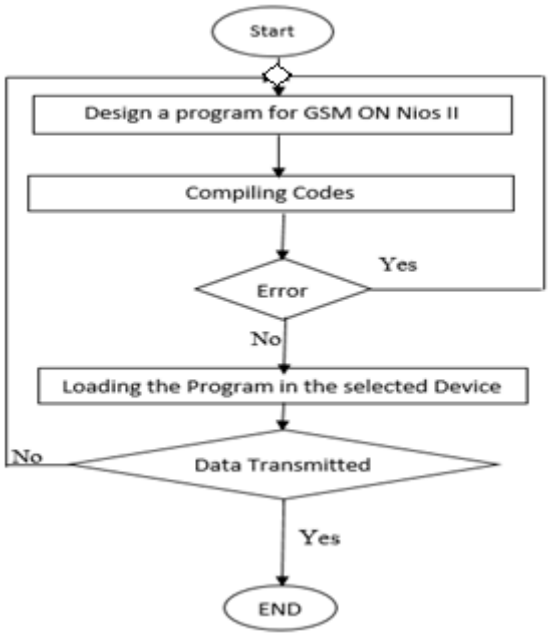

Figure 5.5: Flow Diagram of the Nios II

Table 5.2.: Pseudo Code of Nios II for GSM module

1:	Start
2:	Activate Port 1
3:	Initialize Input value
4:	Establish Handshake connection
5:	Ready for connection
6:	getting data from the FPGA // Cable Length and GPS coordinates
7:	Transfer data to the receiver
8:	Data transferred
9:	End

The GSM works as follows. If the FPGA received a none zero frequency value from the sensing circuit, it converts it to distance from the sensor then trigger the pin of the GSM module through the RS232, a process of transforming input data into an appropriate format to be transmitted (modulation) begins. The data with the header (start), the body (the data itself) composed of the distance from sensor cable and the GPS coordinates and the tail (end) is then transmitted over the network to the receiver. The data transmitted is then demodulated to the original at the receiving end (users).

The GSM device is used to send data to the system users as well as to the computer server. Figure 5.6 represents the connection between the FPGA and GSM.

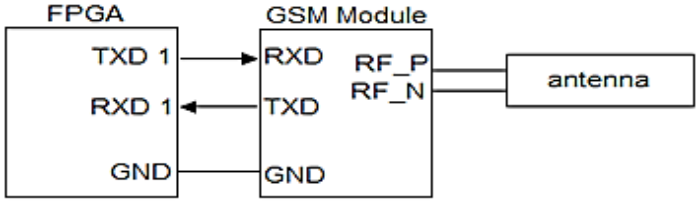

Figure 5.6: Connection between the FPGA and the GSM module

5.6 GPRS Module

The GPRS is used in the design to get coordinates (location) where the cable has been tampered with. Once the FPGA receives a capacitance value from the sensing circuit it converts it into a distance from sensor and simultaneously activates a control in the FPGA which triggers the GPRS to get the Coordinates. Figure 5.7 (Agnihotri, 2010) shows the connection. GPRS hardware device is composed of different modules which are:

(i) Intelligent processing module.

(ii) Serial interface module.

(iii) Display module.

(iv) The remote communication module.

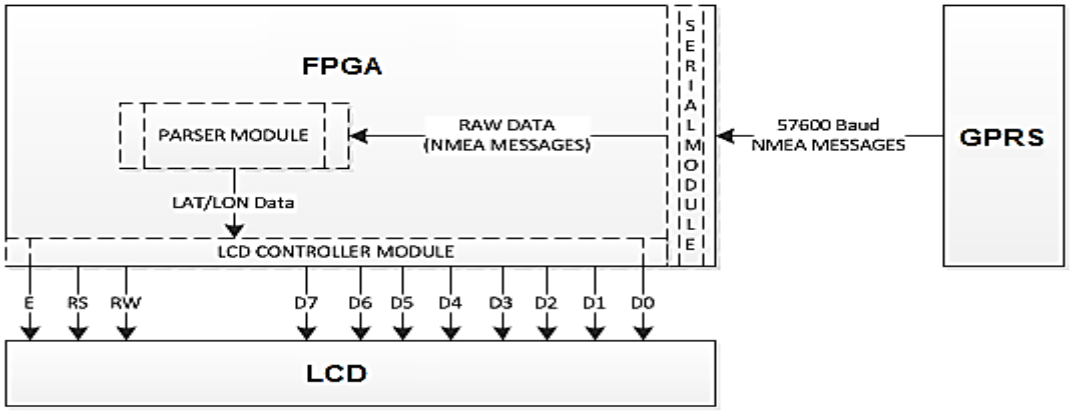

Figure 5.7: Connection between the FPGA and the GPRS (Agnihotri, 2010)

Figure 5.7 shows the block diagram of the GPRS modem. The intelligent module contains two chips (AT89C55 and X25045). The first chip is used to transmit data, analogue to digital conversion and display module. The second chip is responsible for storage of the data in case of power outages.

The Remote communication module contains a SIM card, serial module MAX3238 three parts and the GPRS wireless module. The GPRS wireless module is in charge of sending out data received from the remote monitoring center. The data is then sent to the intelligent processing module through the MAX3238, then the level conversion starts. SIM card function is to store data such as customer identification and customer information authentication encryption algorithm. The display module facilitates the understanding of the real-time situation. (Zhenyu & Jinling, 2004).

5.7 RS232

The component is used in the design to transfer data from a device to another. In this research, is used to transfer data from the sensing circuit to the FPGA, and from the FPGA to the GSM. When a connection between the sensing circuit and the FPGA is made, data is transmitted serially in one direction over a pair of wires. The data coming from the sensing circuit is called Tx (indicating transmission) while the data coming from the FPGA is labelled Rx (indicating reception). Each byte is transmitted sequentially (as long as the preceding byte has been transmitted). Data is sent from the sensing circuit to the FPGA using RS232, through the data transmit pin. The data carrier control detects and checks if a start bit is being transmitted from the sensing circuit to tell the FPGA that a byte of data is about to follow. The start bit lets the receiver synchronize to the data bits. This means that the receiver is allowed to create its own sample clock at the middle of each bit. There will be seven or eight data bits with the least significant bit (LSB) transmitted first, the reason being a choice can be made between seven and eight. The difference between the two is that seven bits is used to send text, and eight bits (ASCII) is used to send alphabet. The GSM modem works with the RS-232, the voltage level indicator. Its 'logic 1' varies from -3 to -15 volts and 'logic 0' from +3 to +15 volts.

5.8 Computer Server

The computer server is used for storing historical data when incidents occur on the cable, with a basic network control interface. It also contains a database which has a list of events recorded accordingly in terms of day month and year (Zhai & Cheng, 2011). The hardware server uses Intel Core i7 as the main processor to control the database and receives monitoring data from the FPGA device. GPRS module is used to give a real time monitoring location at which the cable was tampered with. The Server design uses a GSM module which has 8K SRAM and 64K flash memory to be able to receive data from the FPGA through the GPRS Modem. Figure 5.8 shows the block diagram of the connection between the server and the GSM modem. The PC server is a computer which is connected to the network and has a database which is used to store data coming from the system.

5.9 Components used to Design the Prototype

Components were selected to meet the design specification, in electronics part market, there are many types of modules which can be used in this research project but, all of them will not be used in this project. A specific selection will be done according to certain criteria such as: Functionality, availability, time, accessibility and cost.

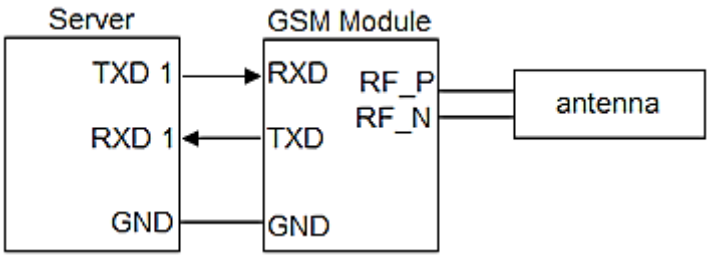

Figure 5.8: Connection between the PC server and the GSM module

There is a need of GSM and GPRS in the project. Many types of GSM and GPRS have been reviewed with the different criteria mentioned above and the one which meets the functionality is the SIM 900. This device is cost effective, available in South Africa and is the one which nearly meets the research objectives the device work with between 4.8 and 5.2 Volts power.

From all the Microcontroller reviewed (Altera, Atmel, EPSON, Intel, Panasonic, Xilinx etc.) the Altera DE2-70 is the one which meets the functionality of the Research Specification. The device is available in South Africa and easily accessible and most of all the device can work from 230 volts to 15 volts.

The RS-232 is used as the connection between the FPGA and the GSM module and has all the functionalities as the other connectors of the same type. Indeed, the RS-232 meets the functionalities of the research outputs.

5.10 Power Supply Module

The foundation of a reliable system is good power supply. Because of the peak current needed from the GPRS module, sensing circuit, FPGA board and the other modules. Designing a good power module must be taken into consideration and the isolated chips in order to reduce interferences. Figure 5.9 shows the connection of the power module as well as the connection with the GPRS modem and other modules. The power supply uses LM2596 and TPS79533 power chips; the LM2596 is a power management integrated circuit which delivers an output of 3 Amps. The LM 2596 has load regulation characteristics and a good linearity. The TPS79533 has a fixed voltage of 3.3 volts.

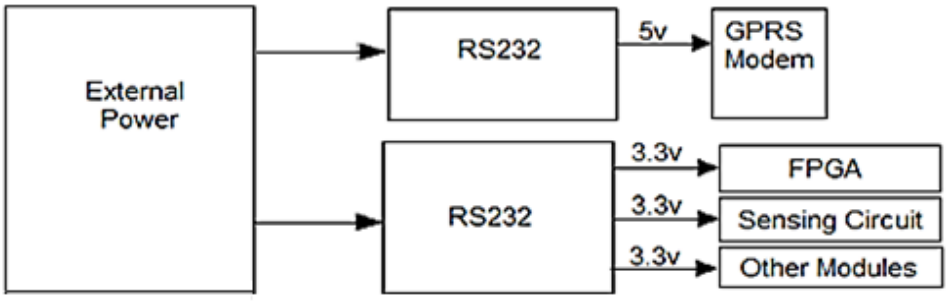

Figure 5.9: Power Supply connection with the components

5.11 Alarm Indication

The alarm is triggered ON when a cable tampering is detected by the sensors and the data is transferred to the FPGA. Once the cable is tampered with, the safety level which is programmed at FPGA controller, should be able to decode the information and activate the port in which the buzzer is connected to sound the alarm.

5.12 Design Set Up (The Telecommunication and Utility Cable Monitoring System)

Figure 5.10, shows the system set up which is composed of: the FPGA is the main controller which receives data from the sensing circuit when a tampering is detected on the cable. The output of the location where the tampering occurred is displayed on the LCD and 7-Segment sends instant messages through GSM Module to the user mobile phone and records the data in a database.

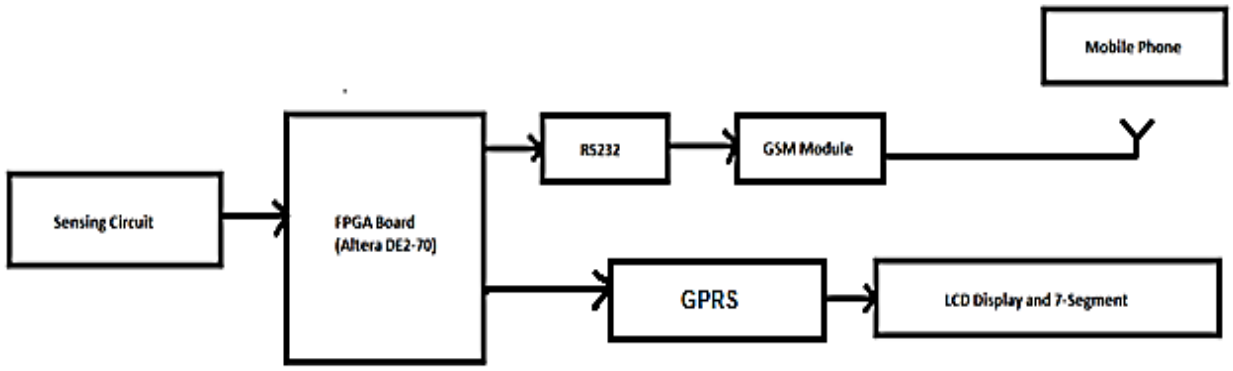

Figure 5.10: The Telecommunication and Utility Cable Monitoring System Set Up

The system Architecture is mainly based on three components. As shown in Figure 5.10, the controller (FPGA module), the GSM/GPRS module and the sensing circuit. The role of the controller (FPGA module) is to constantly check the inputs coming from the sensing circuit and prepare the message to be send through the GSM module. The role of the GSM module is for communication between the user and the controller (FPGA module) through the RS232 serial communication standard. The advantage of using FPGA as controller is that, the device is able to achieve multi inputs/outputs. The FPGA program code was written with a VHDL code for the Altera DE2-70 bus controller on Xilinx ISE suite 10.1. The voltage level of the FPGA and the Altera DE2-70 are similar so no need to make them compatible. The schematic diagram was done on Proteus version 8 after the simulation is carried out on a PCB, a sketch diagram of the prototype was produced and the prototype built.

5.13 Design of the Sensing Circuit using NI Multisim

The reflectometer system was used in the experiment, the circuit diagram is presented in the Figure 5.11 (Furse, *et al.,* 2003). The figure represents the reflectometer system before the modification.

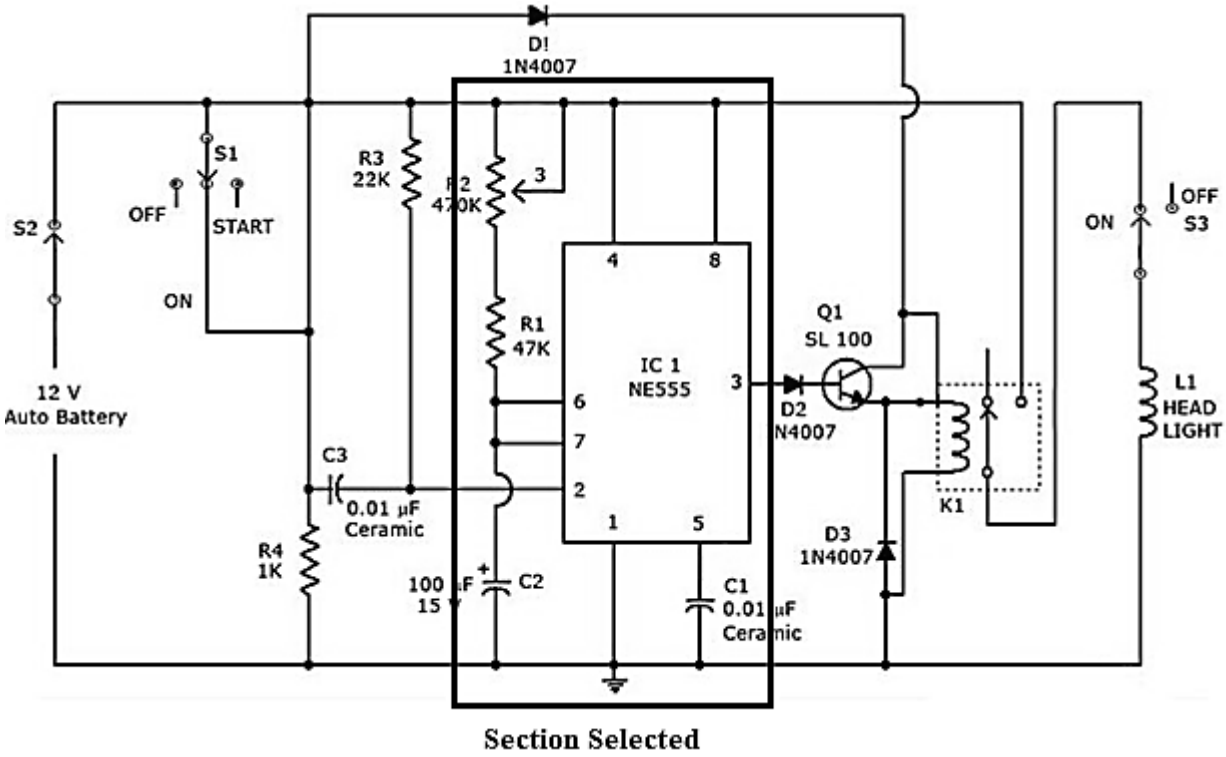

Figure 5.11: Circuit diagram of the Reflectometer before the modification (Furse, *et al,* 2003)

Figure 5.11 shows the diagram of the reflectometer; this circuit is not used fully in the experiment because the only important part of this circuit is the selected part. The section used in the experiment is shown in the Figure 5.12. The selected part is used as the sensing circuit in the experiment.

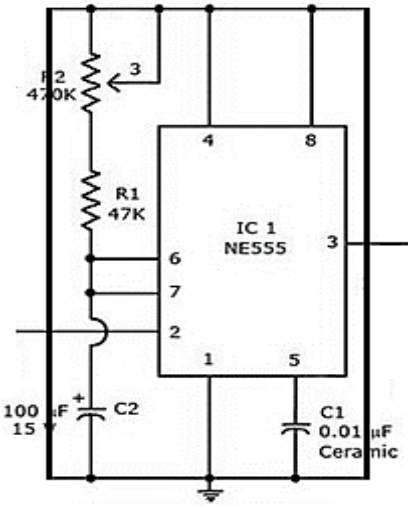

Figure 5.12: Sensing circuit implemented in NI Multisim

Figure 5.12 represents the implementation of the sensing circuit. It is a part of the reflectometer (sensing circuit) the reason why it has been selected is, some part from the reflectometer not needed were removed and the other components were added. Components such R_1, R_2, capacitors C_1, C_2 and the main components of the circuit 555 timer are used in the simulation. The values of the resistance and capacitance comes from the analysis done on the three types of sensing circuit done on chapter three. The circuit is supplied with a 9V and regulated by two resistors R_1 and R_2, which can be varied to get the best performance of the system. The circuit works as follows: data is received at the input (C_2) then goes through the circuit and output data are collected at the output which is connected to the oscilloscope read information such as duty cycle, frequency and time period.

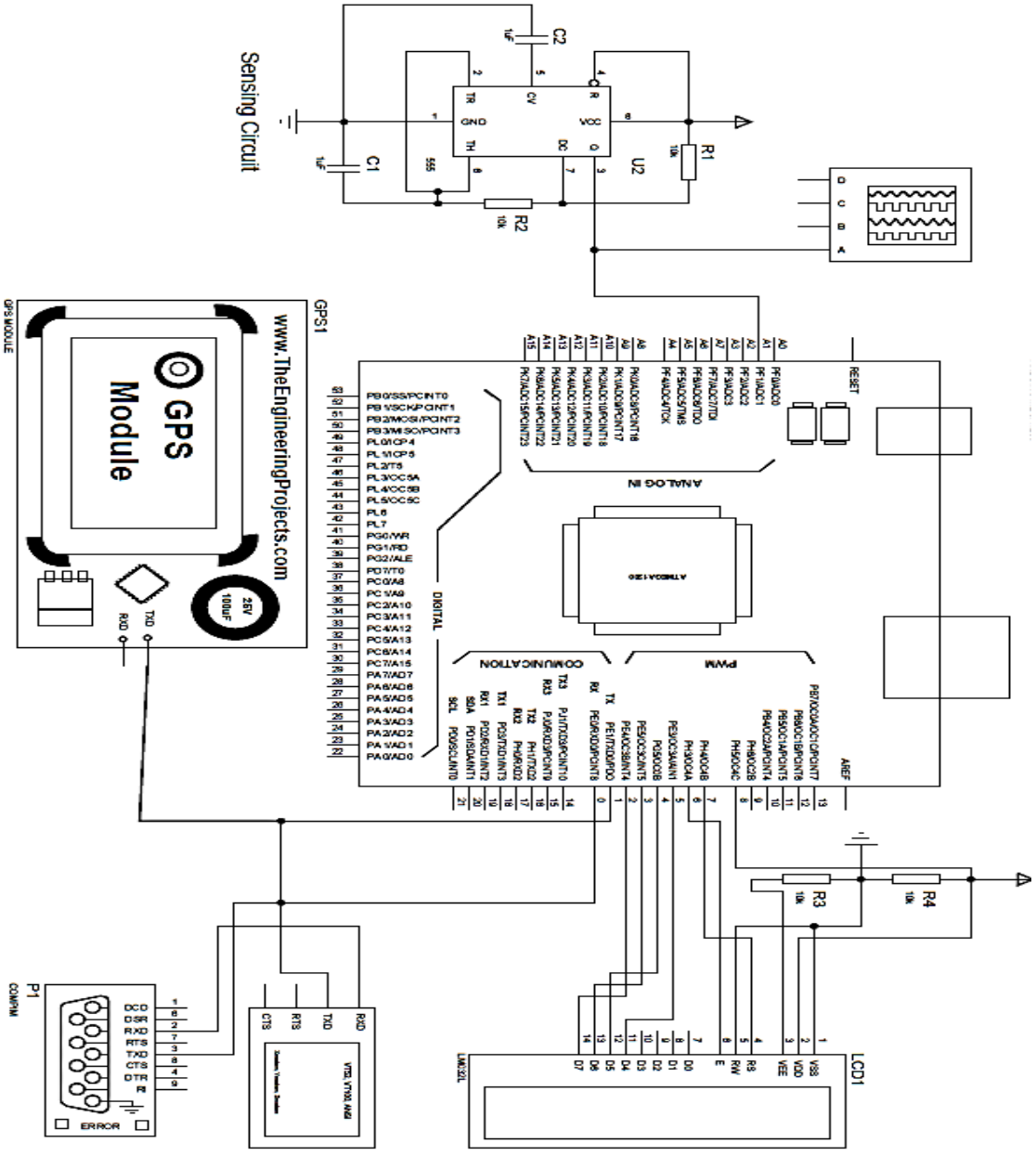

Figure 5.13: Schematic Diagram of the full system with components Values

Figure 5.13 shows the full schematic diagram of the prototype which is combined of the sensing circuit, the FPGA, GPS module and the LCD. The Figure 5.13 also shows the components assemblage.

5.14 Chapter Conclusion

This chapter summarised the design of the proposed solution. It presents information regarding the modules used in the research project, how the components were used, and their connections. It also explained how the components work, the type of systems each module runs with, the reason why some components were used instead of others; and how the components are being used in the design.

CHAPTER SIX: IMPLEMENTATION OF THE TELECOMMUNICATION AND UTILITY CABLE TAMPER MONITORING SYSTEM

6.1 Introduction

This chapter presents the implementation of the prototype. It summaries how the implementation is done and, gives the description of the tools used in the modeling. The hardware component is assembled to build up the prototype shows in Figure 6.1. The capacitor C_2 is varied, for the software simulation in an attempt to detect tampering on the cable and give the specific distance from sensor. These specifications were used to build the sensing circuit, hardware connection between the components were done.

6.2 Software Implementation

The software implementation of the sensing circuit was done on Proteus and the simulation results compared with the prototype simulation. The software simulation data was collected and compared to the prototype simulation. Proteus 8 was chosen because of the high feasibility rate and Real-time performance; the software provides well tools for writing simulations, modules are used and assembled together. Proteus a software which allows researchers to edit files, the GUI makes usage and debugging much easier than other simulators parameter. Proteus is a simulation tool that can be used to carry out system level performance testing.

Chung *et al*. (2009) presented a paper on the most effective way of detecting open and short circuit, from the experiment into two methods:

(i) One type of sensor uses the wire as an inductive or capacitive component in a resonator circuit. As example of such sensors the two-inverter oscillator, difference amplifier and 555 timer sensors.

(ii) Another type of sensors uses the capacitance or inductance of the wire as an impedance and measures the voltage drop between different impedances in the circuit. The voltage divider is an illustration of this class of sensor.

The results obtained from the experiments reveals that the 555-timer circuit is the most suitable to detecting open and short circuit on a wire. In Chung *et al*. (2009) paper there are various combinations of capacitance and resistance. However, the best combination is C_1 = 0.1µF, R_1 = 68kΩ and R_2 = 68kΩ in order to adapt the sensing circuit, so that is can test short-circuit and open-circuit on a cable, these values also were chosen to obtain a 50% oscillation duty cycle. If capacitance and resistance value are chosen different than the one given above, it circuits module a dc null at it output.

The implementation of the sensing circuit was done on Proteus 8, and the results are observed on the oscilloscope. Various capacitance values were set in the sensing circuit and frequency values are observed at the output of the circuit. Threshold (THR) and trigger (TRI) are connected together then connected the input (C_2) which from the sensing circuit, this input is connected to a capacitor which replaced the cable in the simulation. This capacitance value (C_2) is varied and frequency value read at the output (OUT).

6.2.1 Software Implementation of the Sensing Circuit Using Proteus 8

The output result of the simulation is observed on the oscilloscope, data such as period, duty cycle and frequency were observed. Figure 6.1 illustrates the Software implementation of the sensing circuit on Proteus 8, software which present real time information about the sensing circuit. Input data coming from the combination of Threshold (TH) and Trigger (TR) goes through the circuit, this data is converted into a frequency value and goes out from pin Q which is connected to the oscilloscope output data, to be observed on the particular oscilloscope.

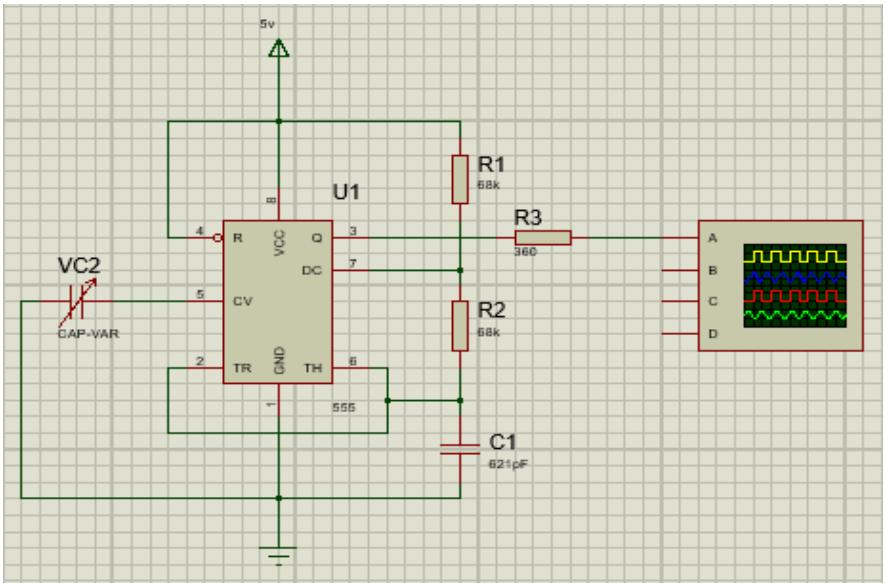

Figure 6.1: Software implementation of the sensing circuit on Proteus 8

6.2.2 Software Implementation of the GSM Module on Proteus 8

GPRS Module: The SIM 900 is a cellular modem, which is embedded in a 64 pins universal socket and offers a standard based quad-band GSM/GPRS. This GPRS module is composed of embedded transmission control/Internet protocol, stack for, internet connectivity and uses a UFL antenna connector which needs a subscriber identity module (SIM) socket. The GPRS module is able to transfer data at a speed of 115.2Kb/s and can be interfaced directly to a UART or a microcontroller using AT commands. It also has an LED to display the network status. The

GPRS is powered with a 5V which is regulated by an UA7805 and operates at 9600 Bd through a serial port of the master component which is the FPGA. The power consumption of this device is 0.56W at 5V. The FPGA sends an AT command to the GPRS module, requires the received signal strength indicator, to be greater than -89dBm to allow a good connection. In addition, it establishes the communication between the GPRS and the URL of the web server to upload and download data. If the signal strength is poor, all the data are stored the solid-state memory and the system tries to establish the connection each hour. Figure 6.2 illustrates the GSM module software implementation on the Proteus 8 software. Since there is no FPGA module on the Multisim software or any compatible package for it, an Arduino has been used for the simulation because it has similar characteristics with the FPGA board. Figure 6.2, shows the connection between the GSM module and the Arduino board, and the pin connection between the two components. On Proteus 8, are different commands to set up the GSM module, before being tested in the simulator (Proteus 8).

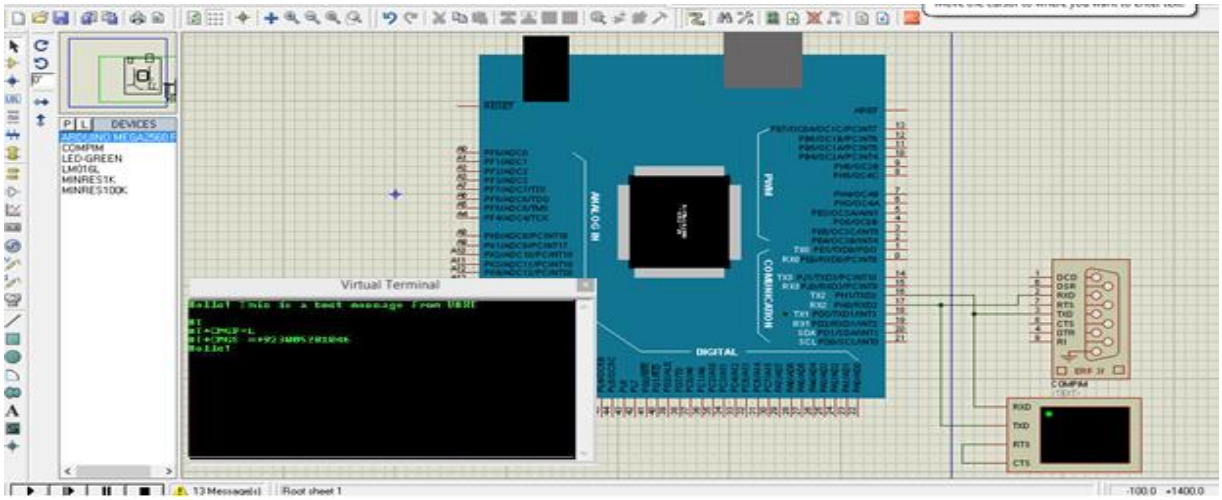

Figure 6.2: GSM module implementation on Proteus 8

6.2.3 Software Implementation of the Cable Tampering Monitoring System using Proteus 8

Figure 6.3 shows the system simulation on Proteus 8 software. The simulation is composed of different components such as the Arduino main component, since the FPGA is not part of the Proteus Package; the Arduino is the substitute of it. The RS232 which is the connector between the Microcontroller and the GSM module is represented in the circuit. The LCD connected to the microcontroller is well illustrated in the Circuit, and the Sensing circuit is connected to the microcontroller. All components are placed and connected together in the simulation. Arduino gets data from the sensing circuit and converts the frequency, sends it to the Microcontroller, which converts the frequency to distance and displays it in the LCD, activate the buzzer and

sends the SMS to the user. The section where the data is sent from the Microcontroller to the Computer Server is not shown in this simulation.

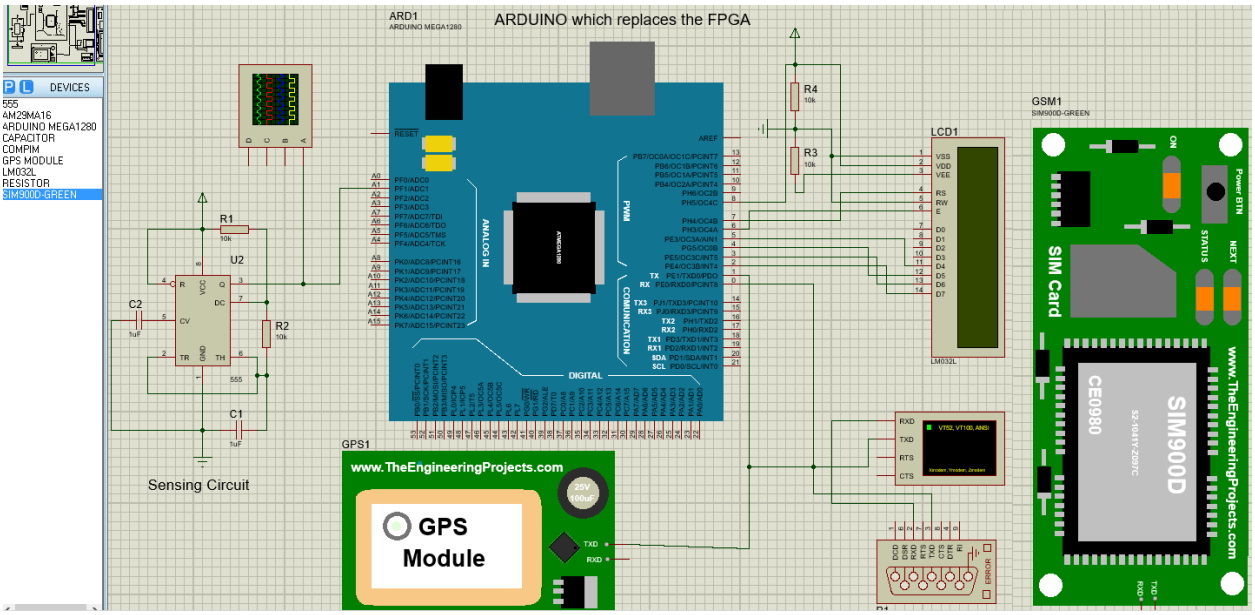

Figure 6.3: Software implementation of the System simulation on Proteus 8

6.2.4 Software simulation of the Sensing Circuit for 2-meter cable on NI Multisim

The sensing circuit input was 56.865 pF, this capacitance value was converted to a frequency value the results are shown in Figure 6.4, where it shows 15.001MHz. Then from the frequency calculation was done using equation 5.2 to get the distance from sensor.

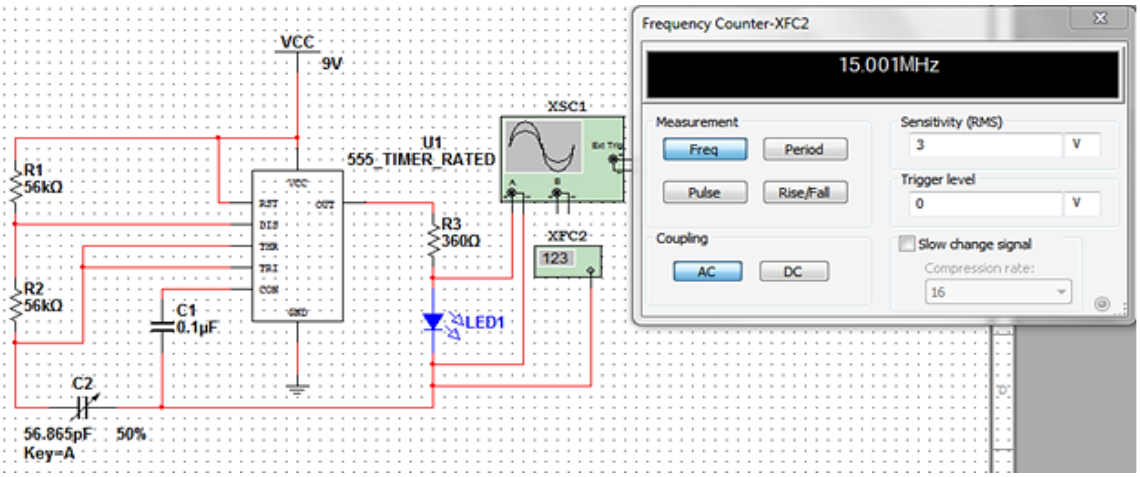

Figure 6.4: Software simulation of the sensing circuit for 2-meter cable on NI Multisim

Figure 6.4 show the layout of the sensing circuit, in NI. After switching ON the simulation, different information such as frequency are obtained from the output of the sensing circuit and the frequency value, is observed from the frequency counter. It also shows a real-time simulation of the system. The output of the sensing circuit is observed from data such as the frequency are measured from the output of the sensing circuit. Figure 6.4, also shows the value

of the capacitance 2 (C_2) which is varied. The reason why the capacitance is varied is that it simulates the tampering scenario replaces the cable tampered with. These values were selected to match different distance from sensor size which were from 2~20 meter, these particular values of distances from the sensor give specific capacitance value which was place in the capacitance C_2. The distance from sensor was replaced by the capacitance C_2 value starting from 2 meter which gives a capacitance value of 568.650 pF up to 20 meter which has the capacitance value of 56.865 pF. These capacitance values are converted by the sensing circuit to a frequency value, which then will be converted to a specific distance from sensor by the FPGA.

6.2.5 Results Obtained on Software Simulation

The software simulation test was done on the sensing circuit using National Instruments Multisim (NI Multisim) simulator. The simulation is tested using different capacitance values as inputs on (C_2) from the sensing circuit and corresponding frequency value are measured at the output of the sensing circuit, the results are shown in the Table 6.1.

Table 6.1. Results collected from the software simulation of the system

Software Simulation Values			
Input	Output		
Capacitance Values (pF)(C2)	Period Values (ns) Output of the Sensing Circuit)	Frequency Values (MHz) (Output of the Sensing Circuit)	Distance from sensor (m)
56.865	66.667	15	20
51.177	60	16.667	18
45.492	53.333	18.750	16
39.806	46.667	21.428	14
34.119	40	25	12
28.432	33.333	30	10
22.746	26.667	37.5	8
17.059	20	50	6
11.373	13.333	75	4
568.650	6.667	150	2

The distance from sensor shown in Table 6.1 is obtained by varying capacitance values, this capacitance value is then input to the sensing circuit and information such as period and frequency are measured at the output at the sensing circuit. This information is observed from the oscilloscope connected at the output of the sensing circuit.

The percentage error has been calculated using the equation:

$$\%\text{error} = \frac{|\text{PrototypeValue} - \text{SoftwareValue}|}{\text{SoftwareValue}} \times 100 \quad (6.1)$$

6.3 Hardware Implementation

This section presents information about the assembling process for the system hardware component, such as the execution of the sensing circuit, the connection between the GSM Module, FPGA, Sensing Circuit, GPRS Module and the PC Server. This process includes the construction of the circuit board and testing the circuit in real time. The set-up of the prototype was done in an analog and digital electronic laboratory. The required components such as capacitance, resistance and 555-timer were assembled, in the simulation when building the prototype. Values of the capacitors, resistors such as: $C_1 = 0.1\mu F$, $C_2 = 621\rho F$, $R_1 = 68k\Omega$ and $R_2 = 68k\Omega$ for the sensing circuit to be able to detect open and short circuit on the cable (Edang, 2001).

6.3.1 Schematic and PC Board Layout of the Sensing Circuit

In order to build the sensing circuit, the following procedures were used:

(i) A PC board was built using EAGLE version 7.5.0 software, with virtual components placed on it.

(ii) The layout of the circuit was printed out and ironed on the PC Board Figure 6.7.

(iii) Holes were drilled from the PC Board in order to place the components.

(iv) The components were placed and soldered on the board

(v) Tested were done to check any short circuit made when soldering the components

Figure 6.5 shows the schematic diagram of the sensing circuit; this circuit give the exact positioning of every components.

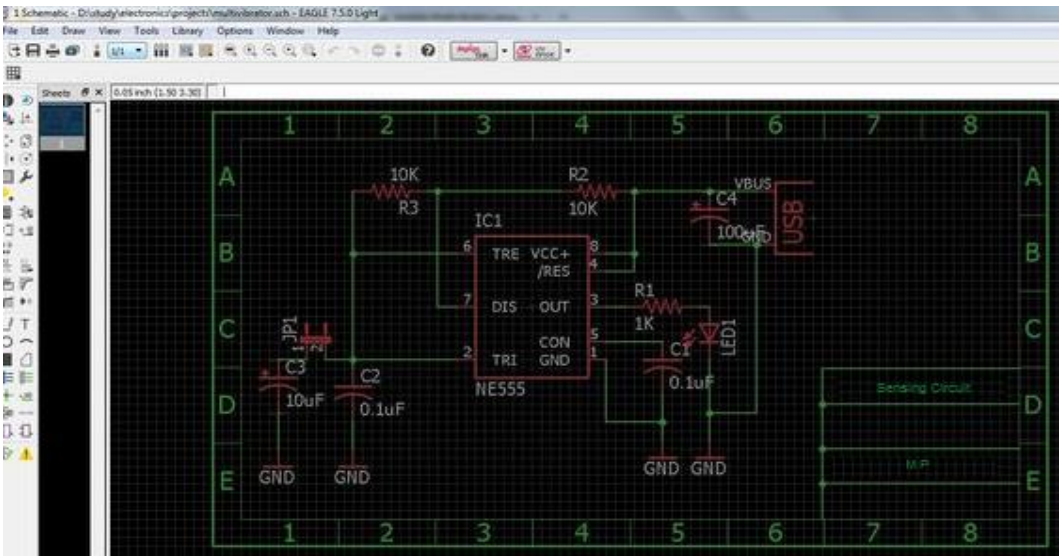

Figure 6.5: Schematic diagram of the sensing circuit using Eagle

Figure 6.5 shows the schematic diagram and the PC board of the sensing circuit. The current goes through routes and tracks of all the components, the schematic board shows the location

where the components are placed. The schematic diagram is the tool from which the PC Board is built. The sensing circuit was assembled from the schematic diagram, on the breadboard, then supplied with a voltage on the kit.

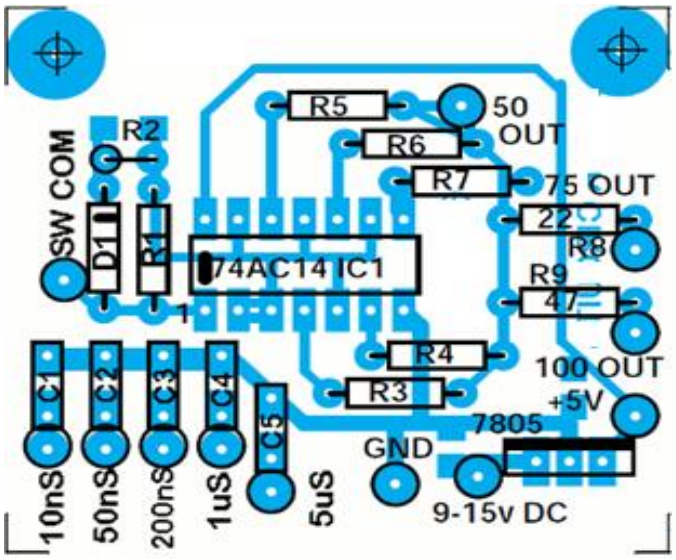

Figure 6.6: Layout of the sensing circuit print out

Figure 6.6, shows the print out of the sensing circuit before placing it on top of the board, before ironing it, then put the board in a substance for the tracks to remain on the board.

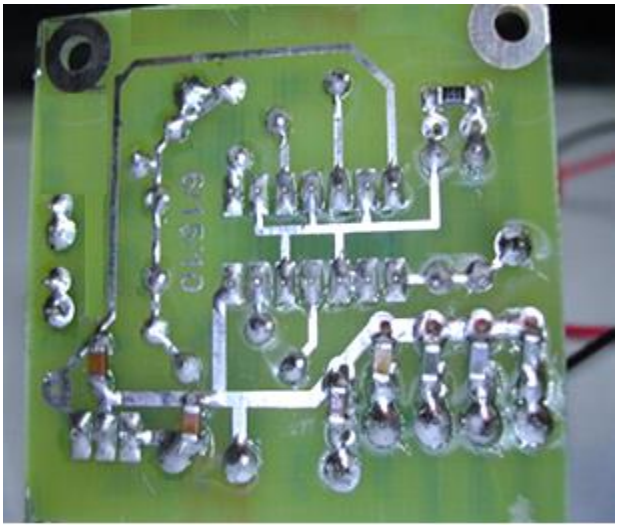

Figure 6.7: Sensing circuit schematic and the PCBoard

Figure 6.7 shows the final board of the sensing circuit, after soldering the components on the board.

6.3.2 Sensing circuit Assembling and Final Layout

After soldering, the components on the board there a need of checking if there any open or short circuit on the board, then test can be done on the system to confirm the software

simulations. Figure 6.8 shows the circuit diagram for the system hardware components, such as 555-timers, resistances and capacitances. This circuit includes the sensing circuit construction. The circuit is tested in real time, data gathered was sent to the FPGA device.

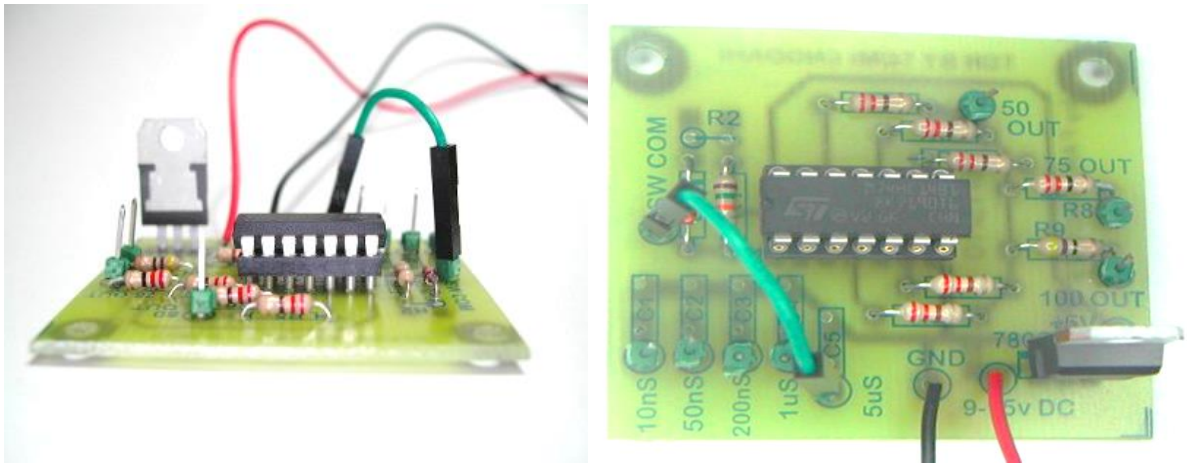

Figure 6.8: Sensing circuit assembling and board

Figure 6.8 shows the top view of the placement of the components on the PC Board. From this PC board information such as the value for each resistance, capacitance, and VCC are given to avoid any mistake when it comes placing the components the right place. The prototype of the sensing circuit was built in the Electronics Laboratory at Vaal University of Technology ready for simulation. Tests were done before building the prototype to avoid any error on the simulation.

6.4 Complete Setup of the Cable Tampering Monitoring System

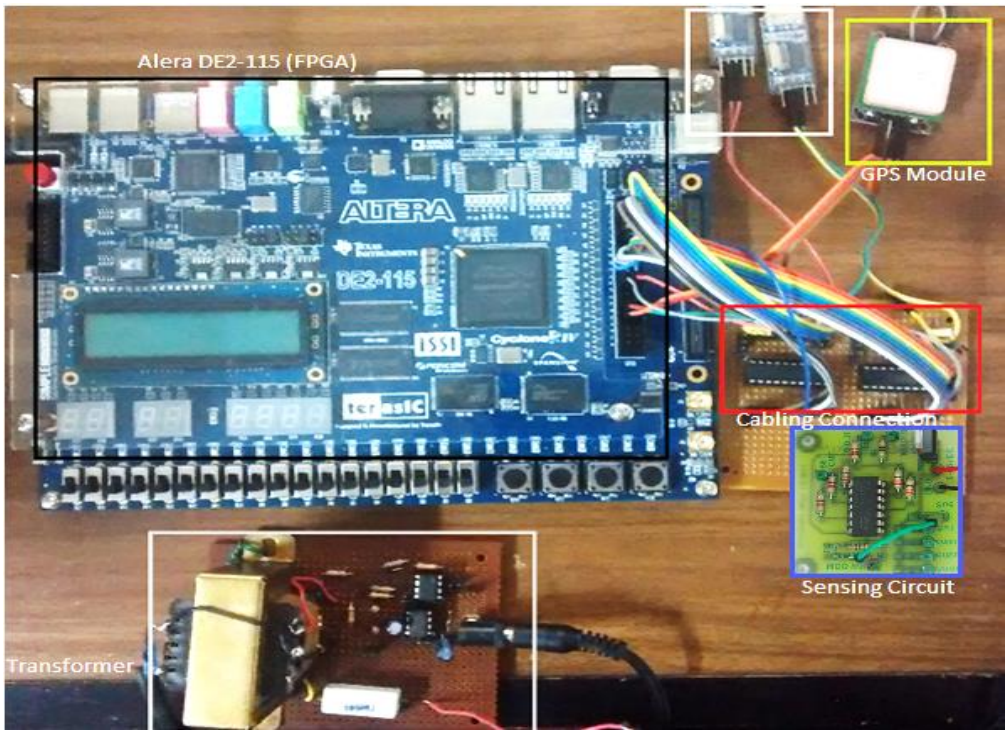

Figure 6.9: Hardware assemblage of the project

Figure 6.9 represents the full setup of the cable tamper monitoring system prototype that was implemented, the prototype consists of the sensing circuit, the FPGA and the GPS module. The prototype was tested in the simulation of the prototype chapter to verify if the design functioned as expected.

6.5 Chapter Conclusion

The overall software tests done were combined and presented in this chapter, which also presented information about the results obtained using software such as NI Multisim regarding the frequency and the capacitance, data gathered from the output of the sensing circuit. The hardware implementation was carried out as well after designing and building the sensing circuit, then assembled it with the FPGA board, GPRS modem, GSM modem and power supply. The correctness at hardware level was then verified.

CHAPTER SEVEN: TEST PROCEDURES AND TEST RESULTS

7.1 Introduction

This chapter presents the simulation tests for the verification of the implementation (prototype) in order to check if the design meets the specifications. Tests are designed to verify the functionalities of the prototype, the description of the tools used in the simulation. Simulation tests were carried out to test the objectives of the research, that is the accuracy of the prototype. Test if the prototype is capable to pinpoint the location of cable tampering, comparison between the prototype results and results obtained from the software simulation. The simulation test setup comprising the software, the hardware, the results obtained are documented from Figures 7.2 to 7.13.

There are three parameters such as: the distance from sensor at which was tampered with, the GPS coordinates of the place where the tampering took place and the functionality of the GSM Module when delivering the Message. The first parameter was the distance from sensor cable which was tampered with. The test was done in a range of 2 meter to 20 meters then displayed on the LCD of the monitoring system. The second parameter was the location of the place where the tampered cable took place. In order to get the proper reading of the location where the tampered cable took place. The third parameter was the performance of the GSM Module on how quick the alert can deliver to the user after the tampering took place. After the cable has been tampered with at certain points; the prototype detected the tampering cable with, different results in terms of distance from sensor and location. Hence comparison between the software and the prototype simulation was done. The test was repeated and measurement was also carried out. Analyses and observations were done; in order to obtain results which were then discussed; and then conclusions were drawn from the documented results.

7.2 Test 1: Simulation on a 2-meter distance from the sensor

The prototype experiment focuses on the measurement of the frequency generated by the sensing circuit for 2-meter cable. The output of the sensing circuit is a frequency which is based on the tampering on the cable. This output is connected to the oscilloscope channel and the reading of data such as frequency and period gathered were observed. Same procedure was done for cable length ranges from 4 to 20 meters.

7.2.1 Result Obtained from the Output of the Sensing Circuit

A 2-meter cable was used for test purpose, the capacitance value was detected by the sensing circuit and converted to a frequency value and results displayed by the oscilloscope. Figure 7.1

shows the output result of a 2-meter cable being tampered with and the frequency is 161.843 MHz with a period of 6.2 ns. After switching ON the simulation, the output waveform appears in a rectangular form. Different information such as period and frequency are obtained from the output of the sensing circuit by using the oscilloscope. Data such as the period, the voltage scale and the frequency are measured from the output of the sensing circuit.

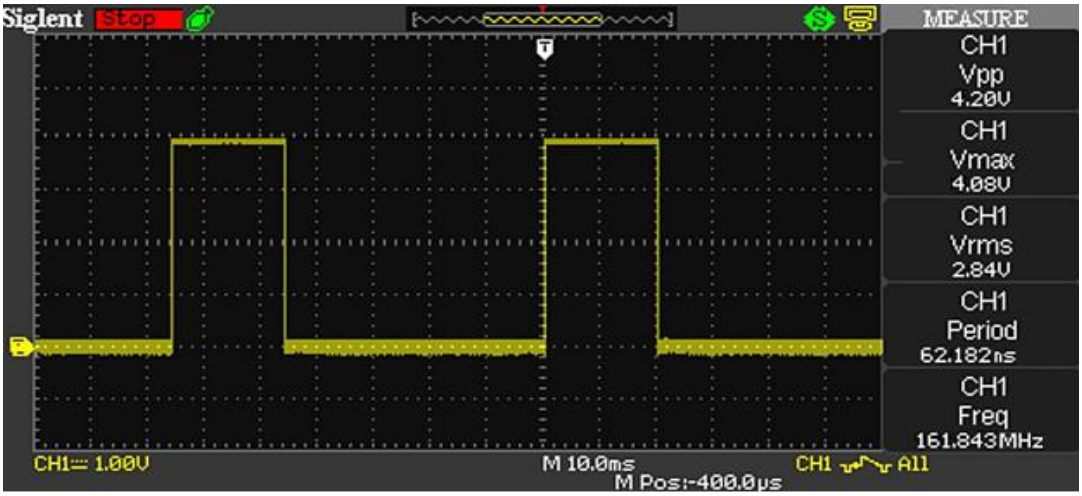

Figure 7.1: The sensing circuit output for 2-meter cable oscilloscope view.

Figure 7.1 shows the time HIGH (Th) period and the time LOW (Tl) period can be seen and calculation can be done to get the total time period (T) of a cycle as well as the frequency (F) and the duty cycle. Once the program codes are successfully inserted in the Altera De2-11, the frequency value is ready to be processed. Data such as the period and the capacitance value are recorded and captured in the Figure 7.1.

7.2.2 Results Obtained from the FPGA (Alter De2-11) from 2-meter cable

Once the FPGA has converted the frequency into the equivalent distance from the sensor, the FPGA request the GPS coordinates from the GPS Modem, and send the two data (distance from sensor and GPS Coordinates) to the LCD and the result is shown in the Figure 7.2

Figure: 7.2: System results display on the LCD.

Figure 7.2 shows information such as the GPS Coordinates (-26.7105365, 27.8625075) of the place where the cable tampering took place (Latitude and Longitude), including the distance from sensor which has been tampered with.

7.2.3 Result Obtained from the GSM for 2-meter cable

When the sensing circuit detects that one end of the cable is tampered with, it generates a frequency and sends it to the FPGA Board. The FPGA convert the frequency into a corresponding distance from sensor simultaneously. The FPGA board triggers the GSM program and sends the message to the user. This message contains the distance from sensor and the location where the anomaly took place Figure 7.3 shows the data which has been sent to the user on the mobile phone via GSM module as: the location where the tampering took place (GPS coordinates) and the distance from sensor cable which was tampered with.

Figure 7.3: The SMS received at the user mobile phone

7.3 Test 2: Simulation on a 4-meter Cable

The prototype was tested when tampering occurred for 4-meter from the sensor.

7.3.1 Result Obtained from the Output of the Sensing Circuit

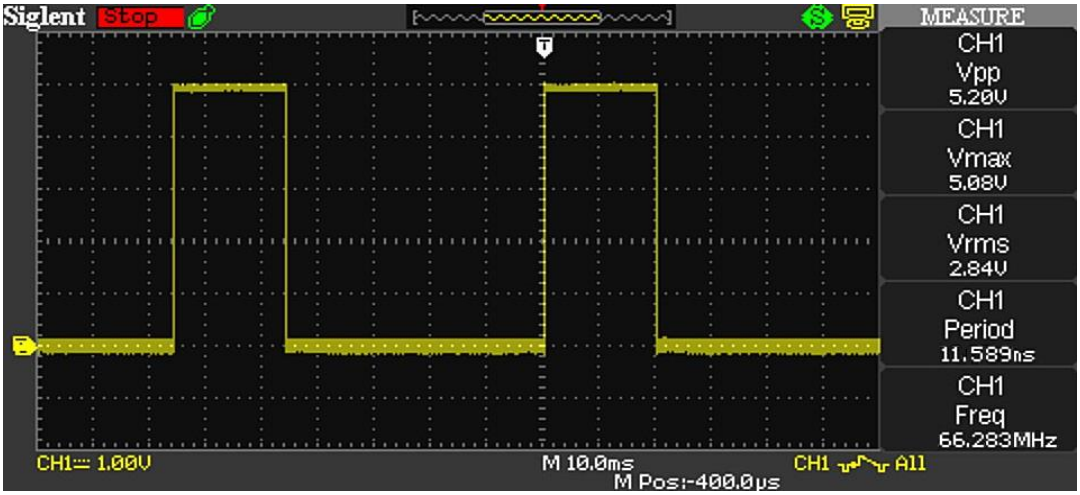

Figure 7.4: The sensing circuit output for 4-meter cable oscilloscope view.

7.3.2 Results Obtained from the FPGA (Alter De2-11) from 4-meter cable

Figure 7.5: System results display on the LCD.

7.3.3 Result Obtained from the GSM from 4-meter cable

Figure 7.6: The SMS received at the user mobile phone

7.4 Test 3: Simulation on a 6-meter Cable

The prototype was tested when tampering occurred for 6-meter from the sensor.

7.4.1 Result Obtained from the Output of the Sensing Circuit for 6-meter cable

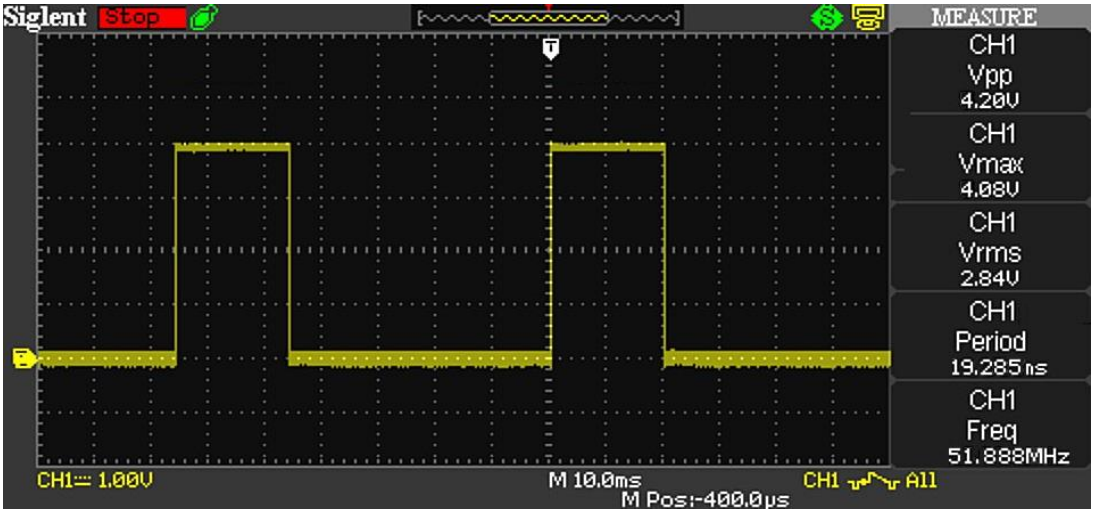

Figure 7.7. The sensing circuit output for 6-meter cable oscilloscope view.

7.4.2 Results Obtained from the FPGA (Alter De2-11) for 6-meter cable

Figure 7.8: System results display on the LCD.

7.4.3 Result Obtained from the GSM for 6-meter cable

Figure 7.9: The SMS received at the user mobile phone

7.5 Test 4: Simulation on a 8-meter Cable

The prototype was tested when tampering occurred for 8-meter from the sensor

7.5.1 Result Obtained from the Output of the Sensing Circuit

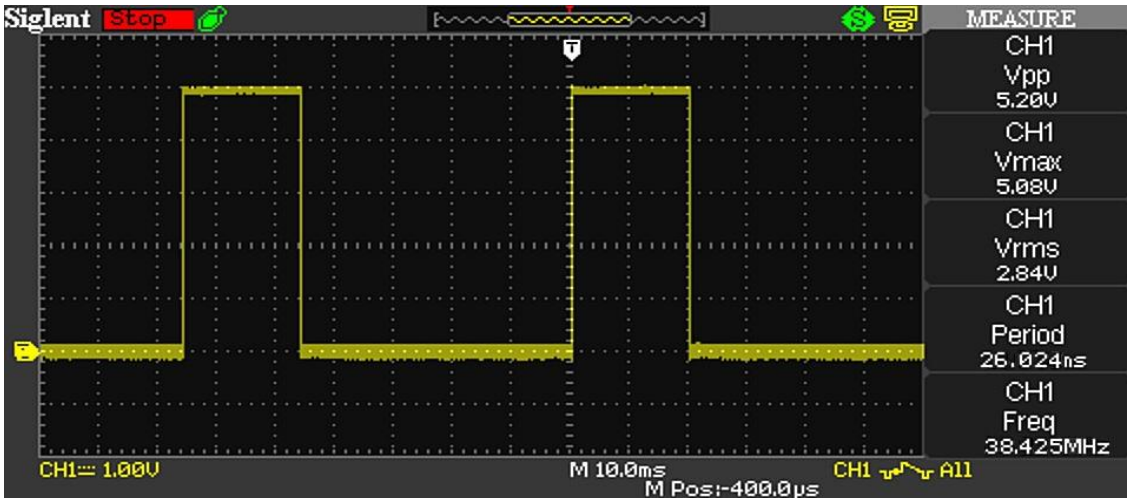

Figure 7.10: The sensing circuit output for 8-meter cable oscilloscope view.

7.5.2 Results Obtained from the FPGA (Alter De2-11) for 8-meter cable

Figure 7.11: System results display on the LCD.

7.5.3 Result Obtained from the GSM

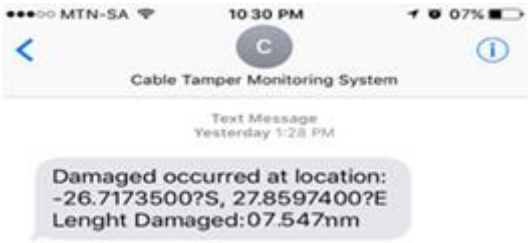

Figure 7.12: The SMS received at the user mobile phone

7.6 Test 5: Simulation on a 10-meter Cable

The prototype was tested when tampering occurred for 10-meter from the sensor.

7.6.1 Result Obtained from the Output of the Sensing Circuit

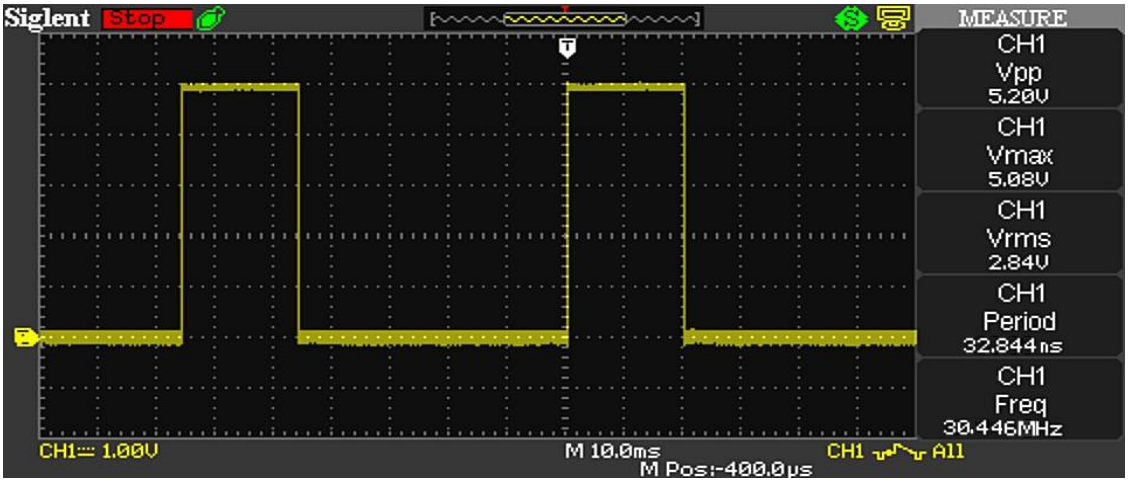

Figure 7.13: The sensing circuit output for 10-meter cable oscilloscope view.

7.6.2 Results Obtained from the FPGA (Alter De2-11) for 10-meter cable

Figure 7.14: System results display on the LCD.

7.6.3 Result Obtained from the GSM for 10-meter cable

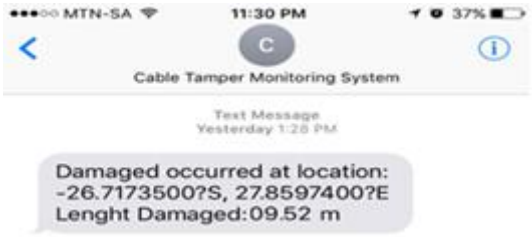

Figure 7.15: The SMS received at the user mobile phone

7.7 Test 6: Simulation on a 12-meter Cable

The prototype was tested when tampering occurred for 12-meter from the sensor.

7.7.1 Result Obtained from the Output of the Sensing Circuit for 12-meter cable

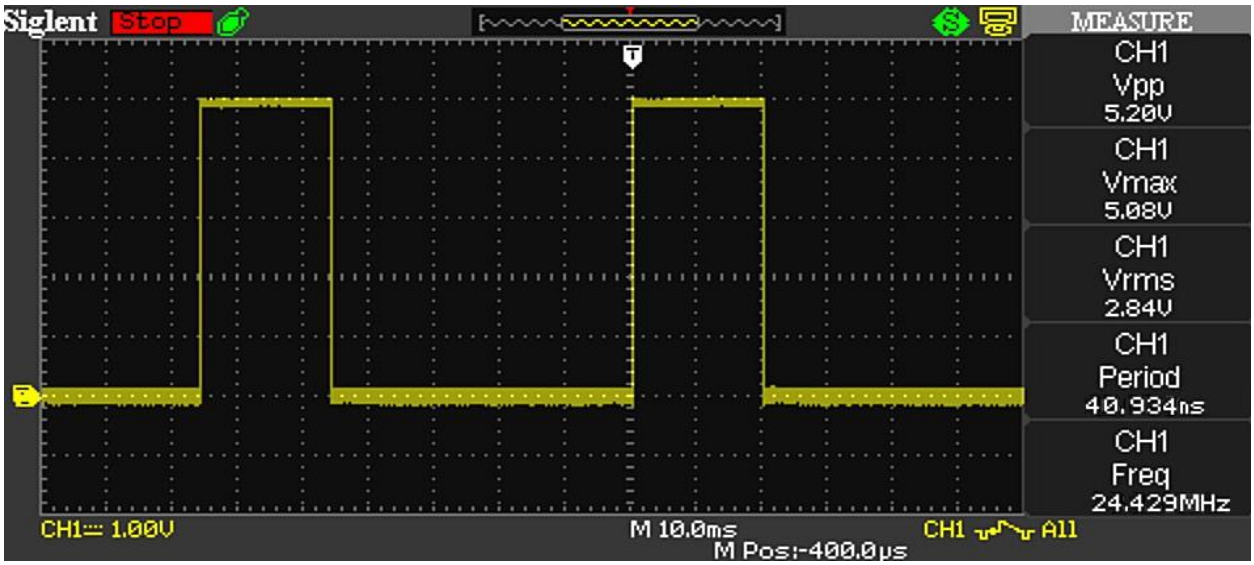

Figure 7.16. The sensing circuit output for 12-meter cable oscilloscope view.

7.7.2 Results Obtained from the FPGA (Alter De2-11) for 12-meter cable

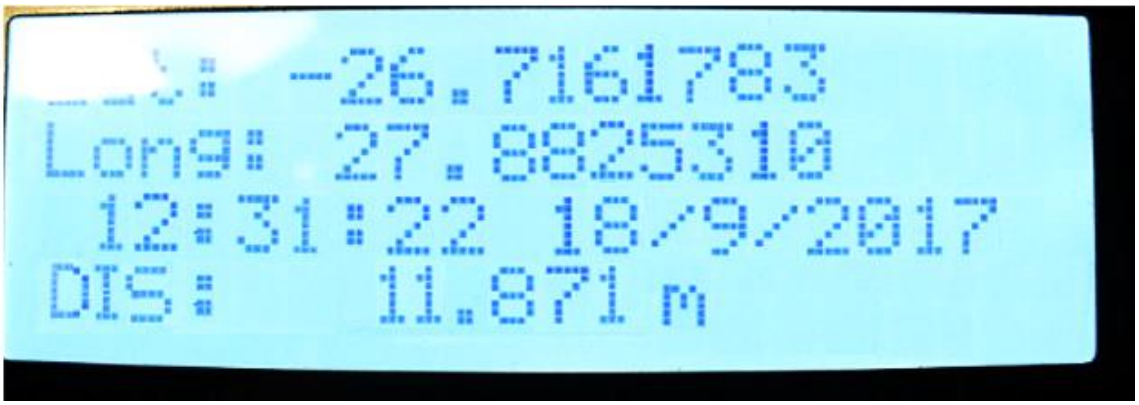

Figure 7.17. System results display on the LCD

7.7.3 Result Obtained from the GSM for 12-meter cable

Figure 7.18: The SMS received at the user mobile phone

7.8 Test 7: Simulation on a 14-meter Cable

The prototype was tested when tampering occurred for 14-meter from the sensor.

7.8.1 Result Obtained from the Output of the Sensing Circuit for 14-meter cable

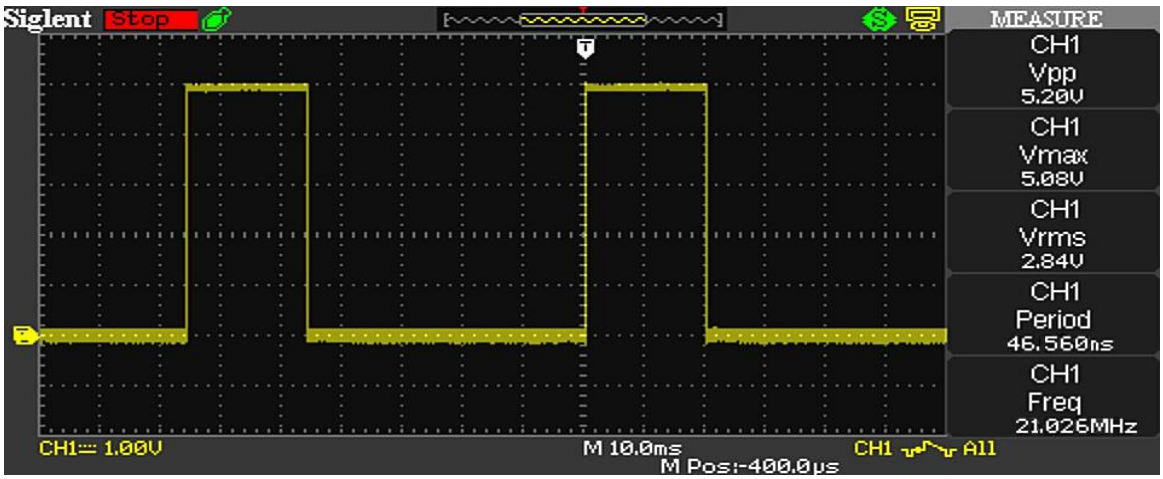

Figure 7.19. The sensing circuit output for 14-meter cable oscilloscope view.

7.8.2 Results Obtained from the FPGA (Alter De2-11) for 14-meter cable

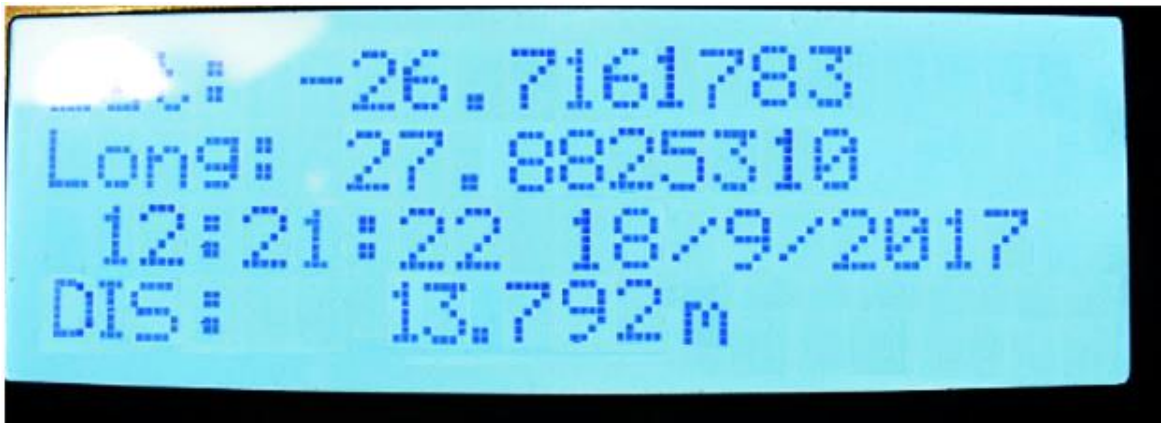

Figure 7.20. System results display on the LCD.

7.8.3 Result Obtained from the GSM for 14-meter cable

Figure 7.21: The SMS received at the user mobile phone

7.9 Test 8: Simulation on a 16-meter Cable

The prototype was tested when tampering occurred for 16-meter from the sensor

7.9.1 Result Obtained from the Output of the Sensing Circuit for 16-meter cable

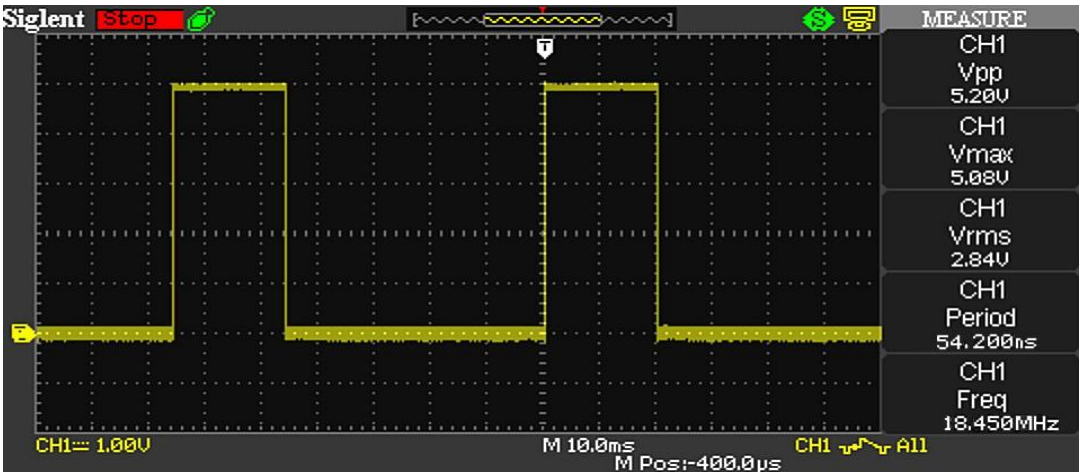

Figure 7.22. The sensing circuit output for 16-meter cable oscilloscope view.

7.9.2 Results Obtained from the FPGA (Alter De2-11) for 16-meter cable

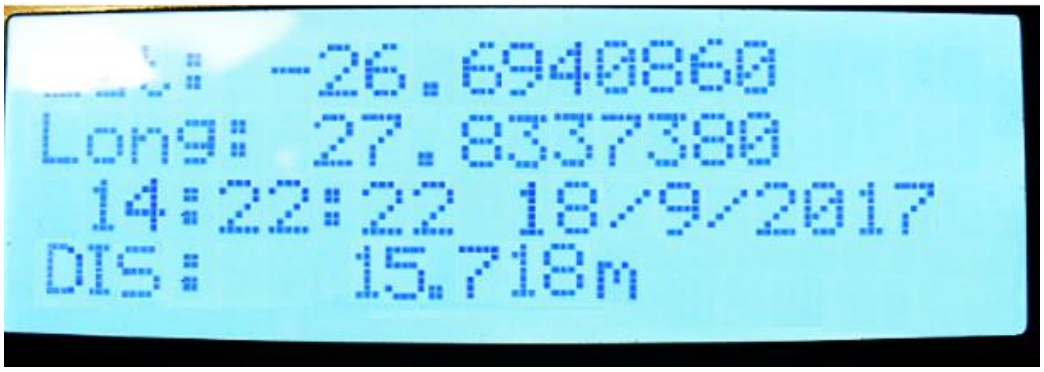

Figure 7.23. System results display on the LCD.

7.9.3 Result Obtained from the GSM for 16-meter cable

Figure 7.24: The SMS received at the user mobile phone

7.10 Test 9: Simulation on a 18-meter Cable

The prototype was tested when tampering occurred for 18-meter from the sensor

7.10.1 Result Obtained from the Output of the Sensing Circuit for 18-meter cable

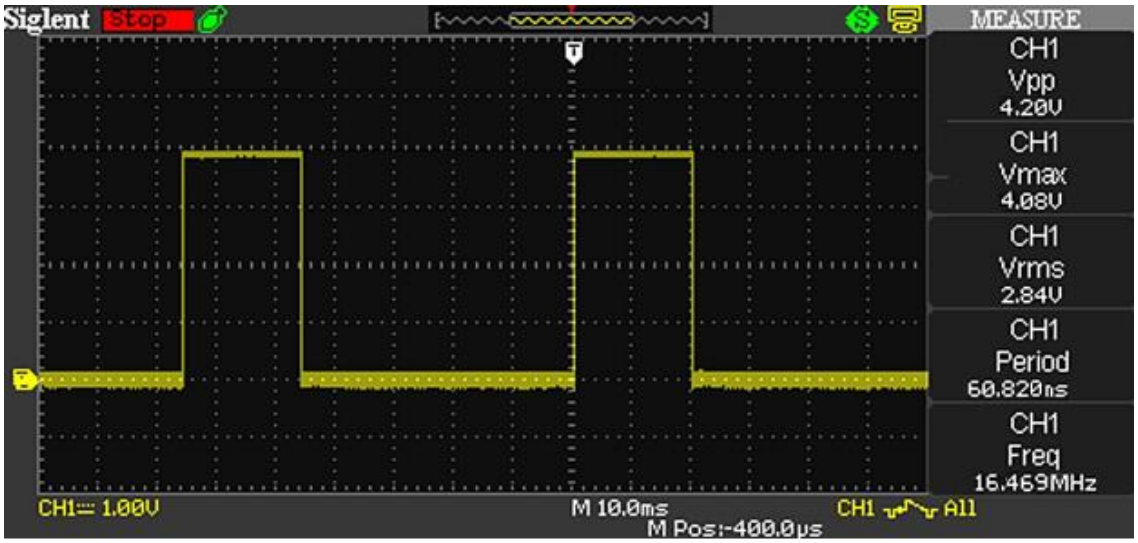

Figure 7.25. The sensing circuit output for 18-meter cable oscilloscope view.

7.10.2 Results Obtained from the FPGA (Alter De2-11) for 18-meter cable

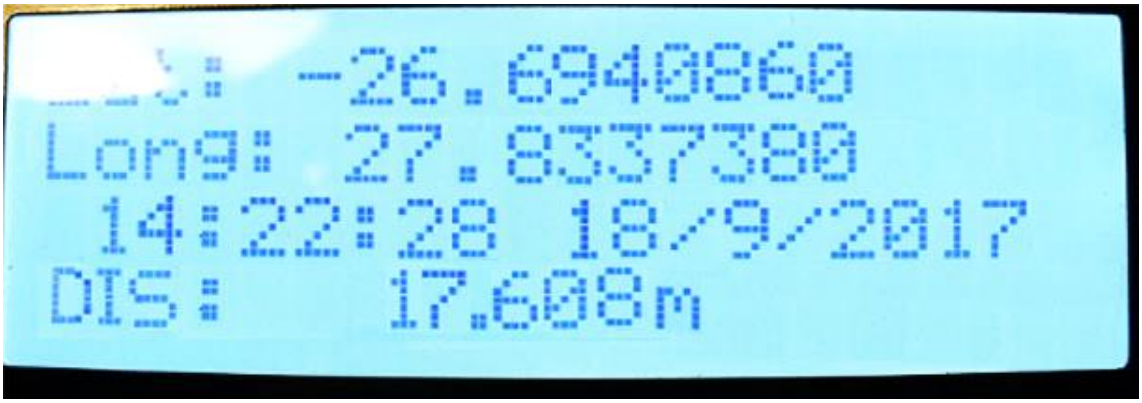

Figure 7.26. System results display on the LCD.

7.10.3 Result Obtained from the GSM for 18-meter cable

Figure 7.27: The SMS received at the user mobile phone

7.11 Test 10: Simulation on a 20-meter Cable

The prototype was tested when tampering occurred for 20-meter from the sensor

7.11.1 Result Obtained from the Output of the Sensing Circuit for 20-meter cable

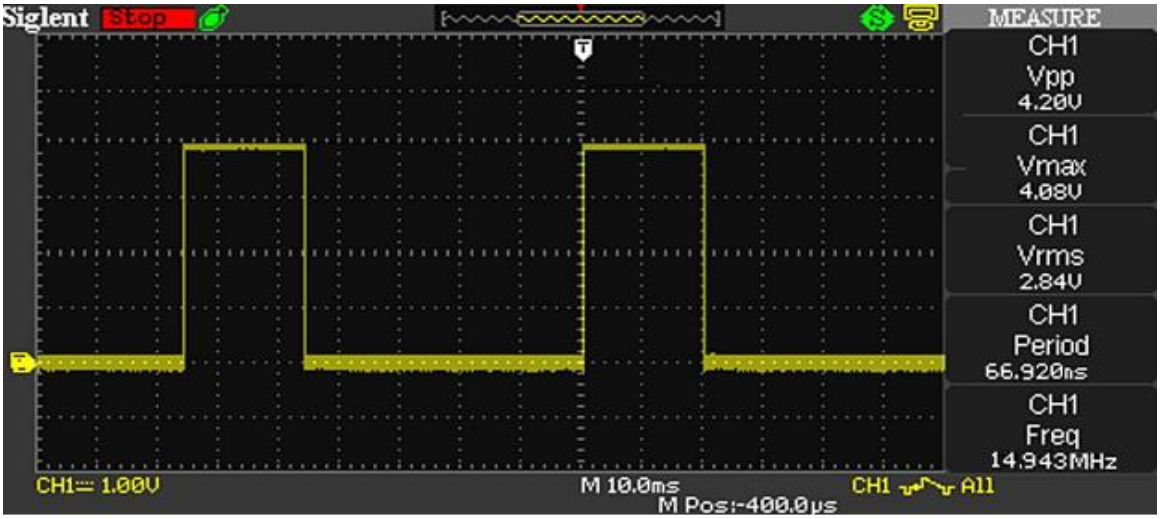

Figure 7.28. The sensing circuit output for 20-meter cable oscilloscope view.

7.11.2 Results Obtained from the FPGA (Alter De2-11) for 20-meter cable

Figure 7.29. System results display on the LCD.

7.11.3 Result Obtained from the GSM for 20-meter cable

Figure 7.30: The SMS received at the user mobile phone

7.12 Results Obtained when Testing the Prototype

Table 7.1 presents simulation data gathered from the prototype tests data such as: Capacitance, period, Frequency and the distance from sensor. In the same way as the simulation, data was read at the output of the sensing circuit. When the cable is tampered with a capacitance value is generated and sent down the sensing circuit, this capacitance value is converted into a frequency value which is output from the sensing circuit as well as the period. This frequency goes through the FPGA and the distance from sensor is output from the FPGA.

Table 7.1: Results collected from the prototype test of the system

Prototype Values				
Input	Output			
Cable Tampered (Meter)	Capacitance Values (pF) (Reading from the Multimer)	Period Values (ns) (Oscilloscope)	Frequency Values (MHz) (Oscilloscope)	Distance from Sensor (Meter) (Display on LCD)
2	536.621	62.182	161.843	1.803
4	13.102	11.589	66.283	3.361
6	16.740	19.285	51.888	5.590
8	22.602	26.024	38.425	7.547
10	28.525	32.844	30.446	9.525
12	35.551	40.934	24.429	11.871
14	41.305	46.560	21.026	13.792
16	47.072	54.200	18.450	15.718
18	52.795	60.820	16.469	17.608
20	58.12	66.920	14.943	19.407

Table 7.1 shows simulation results obtained when testing the prototype, 10 distinct tests were done on the prototype and the information about the capacitance, frequency, period and distance from sensor observed.

7.13 Comparison Between the Software Simulation and the Prototype Based on the Frequency Generated at the Output of the Sensing Circuit

The software simulation and the prototype results for the different frequency as have been obtained for the software simulation 150 MHz and the prototype test. The simulation record 150 MHz and prototype returns 161.84 MHz with a difference of 11.8MHz and the error of 7.372% with correlation therefore exists, the data used in this test is collected on the Table 7.2

Table 7.2: Error percentages of the frequency value between the prototype test and the software simulation.

Software Result	Prototype Result	Difference between the Software and the Prototype	Error
Frequency Values (MHz)	Frequency (MHz)	Frequency (MHz)	Percentage (%)
150	161.843	11.843	7.372
75	66.283	8.717	11.623
50	51.888	1.878	3.62
37.5	38.425	0.925	2.408
30	30.446	0.446	1.53
25	24.429	0.571	2.284
21.428	21.026	0.402	1.876
18.750	18.450	0.300	1.6
16.667	16.469	0.198	1.188
15	14.943	0.057	0.38

Table 7.2 shows that the measurement in the error column is small in the interval from 0.057 to 11.843 MHz of the frequency. According to the Table 7.3, the highest error encountered is 11.843 and the corresponding distance is 2-meter. The location where the cable has been tampered with can be found and the error are recorded.

7.14 Comparison Between the Software Simulation and the Prototype Based on the Distance from Sensor Generated at the Output of the FPGA.

The software simulation and the prototype results for the distance from sensor has been obtained for the software simulation 2-meter and on the prototype test 1.803-meter the difference between ideal solution and the prototype was 0.197-meter, with 9.85% correlation. The data used in this test is presented on the Table 7.3

Table 7.3. Error percentages of the distance from sensor between the prototype test and the software test.

Software Result	Prototype Result	Difference between the Software and the Prototype	Error
Distance from Sensor (meter)	Distance from Sensor (meter)	Distance from Sensor (meter)	Percentage (%)
2	1.803	0.197	9.85
4	3.361	0.639	15.975
6	5.590	0.410	6.833
8	7.547	0.453	5.7
10	9.525	0.475	4.75
12	11.871	0.129	1.075
14	13.792	0.208	1.486
16	15.718	0.282	1.763
18	17.608	0.392	2.178
20	19.407	0.593	2.965

Table 7.3 shows the results of the distance from sensor which were tested in the prototype, data was gathered and recorded with the percentage error. From the results observed from Table 7.3, the maximum error in terms of percentage is obtained from the distance from sensor (from 2-meter to 20-meters) is about 1 meter. On the prototype experiment, the longest distance from sensor tested is 20-meters, but on the calculation side the distance from sensor which can be tested is more than 1 kilometer. The difficulty of cable testing on long distances is due to the fact that the measurement value is not accurate when the cable is rolled together or bent. The cable cannot be rolled together when the test takes place because the capacitance value within the cable will not be accurate.

7.15 Comparison Between the Software Simulation and the Prototype Based on the Capacitance Value.

The software simulation and the prototype results for the capacitance value have been obtained and comparison was done. Data used in this test are presented in the Table 7.4

Table 7.4: Error percentages of the capacitance value between the software and the prototype simulation.

Software Result	Prototype Result	Difference between the Software and the Prototype	Error
Capacitance Values (pF)	Capacitance (pF)	Capacitance (pF)	Percentage (%)
56.865	58.12	1.255	2.16
51.177	52.795	1.618	3.065
45.492	47.072	1.58	3.357
39.806	41.305	1.499	3.63
34.119	35.551	1.432	4.029
28.432	28.525	0.093	0.327
22.746	22.602	0.144	0.634
17.059	16.740	0.319	1.87
11.373	13.102	1.729	13.197
568.650	536.621	32.029	5.633

Table 7.4 shows that the measurement in the error column is small in the interval from 0.093 pF to 32.029 pF of the capacitance. From the result, the highest error encountered is 32.029 pF and the corresponding distance is 2-meter this happens from the location where the cable has been tampered with and this is a small distance and the error is acceptable.

7.16 Comparison Between the Prototype and the Literature Review

From the projects reviewed in the literature it has been found that no system is able to detect the location at which the cable has been tampered with. It is noticeable that the implemented cable monitoring systems reviewed lack the precision when it comes to detecting the exact location where the cables have been tampered with and determining the distance from sensor of the stolen cable. However, the prototype build in this project is able to pinpoint the location where the tampering might take place, and provide the distance from sensor (cable length) which was taken away.

7.17 Error Margin Analysis

It is noticeable that the error margin in the simulation of the Project is considerable in term of percentage when testing small cable length example for 2 meters simulated in the software it gives 9.85 % error margin compared to the prototype and for 4 meter it gives 15.975 %. However, as the cable length increase the margin error decreases refer to Table 7.3.

7.18 Chapter Conclusion

This chapter has presented software simulation and test carried out on the prototype. The parameters observed are: the period, the frequency, the capacitance value, distance from the sensor, GPS coordinates of the location where the tampering took place and the SMS received by the users when the incident happened. Simulation were done on different size of cables from 2 to 20-meters cable (distance from the sensor), and results were observed on the output of the FPGA's LCD. By simulating the prototype, a verification was done and the implementation meets the design specifications.

CHAPTER EIGHT: ANALYSIS OF THE SIMULATION TEST RESULTS

8.1 Introduction

This chapter presents information about the analysis of the results achieved from the simulation tests of the prototype, to determine if the prototype performed as per the design. The analysis is done, according to the results obtained from the simulation, capacitance value, frequency value and corresponding distance based on the prototype tests. A comparison of the simulation results against the research objectives to determine if the objectives were achieved. The aim of this research was to design and implement a telecommunication and utility cable tampered monitoring system which is able to pinpoint the location of the cable tampered with, and to get the distance from tampered sensor cable. Proteus 8 software was used for modelling the prototype and design.

The system was built, tested and when the cable was tampered with at 2 to 20-meters, the prototype was able to detect and provide information about the distance from sensor been tampered with and the location where the incident took place and the results are shown in Table 7.1. The system was able to send the SMS to the users giving information about the size of the cable been tampered with and the coordinates of the place where the tampered with took place.

8.1.1 Prototype Objectives and Results

The objectives of the research were to design and implement a cable monitoring system, investigate the performance of the prototype, especially to determine if the implemented cable monitoring system can detect an anomaly on the cable (cable tampered with) and indicate the distance from the sensor and the location at which the tampering will take place. The result of the prototype shows that the system is able to detect and locate the place where the tampering took place and give the distance from the sensor as well as send an alarm message to the user via SMS.

8.1.2 Comparison Between the Simulation and the Prototype Based on the Frequency, Distance from sensor and Capacitance.

This section presents the comparison between the simulation and the software results based on the frequency generated from the sensing circuit, the capacitance, the frequency and the distance from sensor. It provides data gathered from the software and the prototype and analysis can be done. Frequency value is gathered from the prototype and the software results was plotted as shown in the Figure 8.1. Figure 8.1 also show that the prototype and the software

results are very close, the reason why the results are a bit different is because of the interference happening on the prototype.

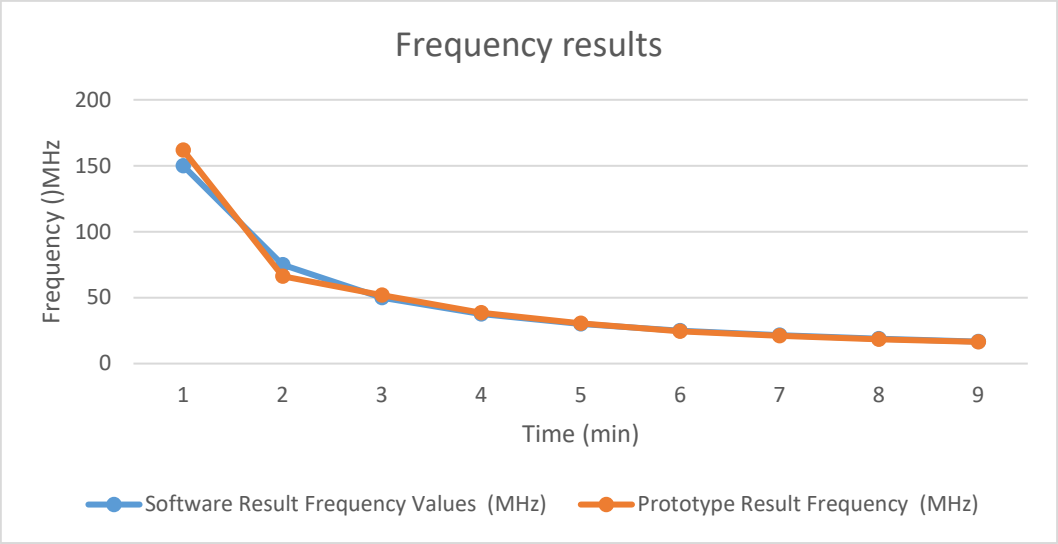

Figure 8.1: Comparison between the software and the prototype results in terms of the frequency

Figure 8.2 shows the reading distance from the software and the prototype simulation. It also shows the comparison between the simulations obtained from the output of the sensing circuit on the Multisim and the prototype distance from sensor while the curve was obtained from the prototype. The result both from the prototype and the software are almost the same.

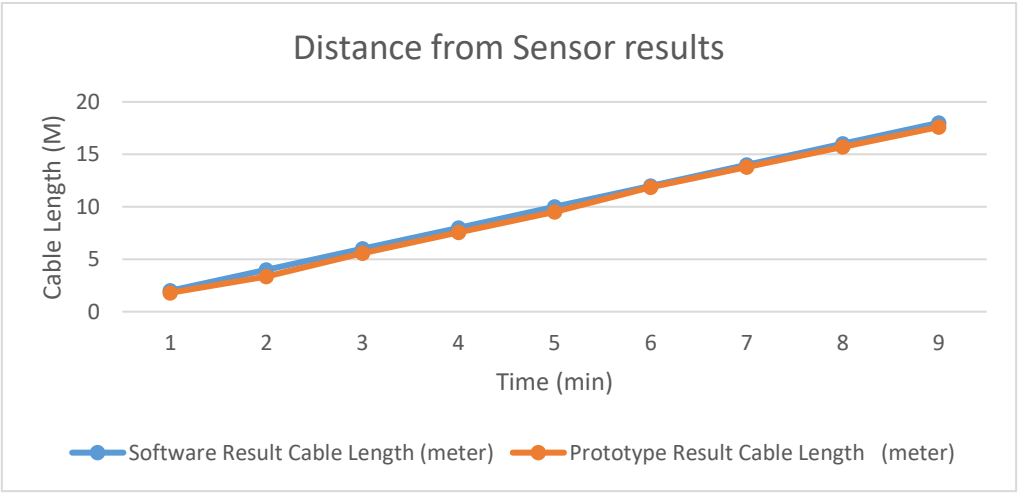

Figure 8.2: Comparison between the software and the prototype results in terms of the distance from sensor

Capacitance value obtained from the software simulations and prototype are plotted, the results are shown in the Figure 8.3.

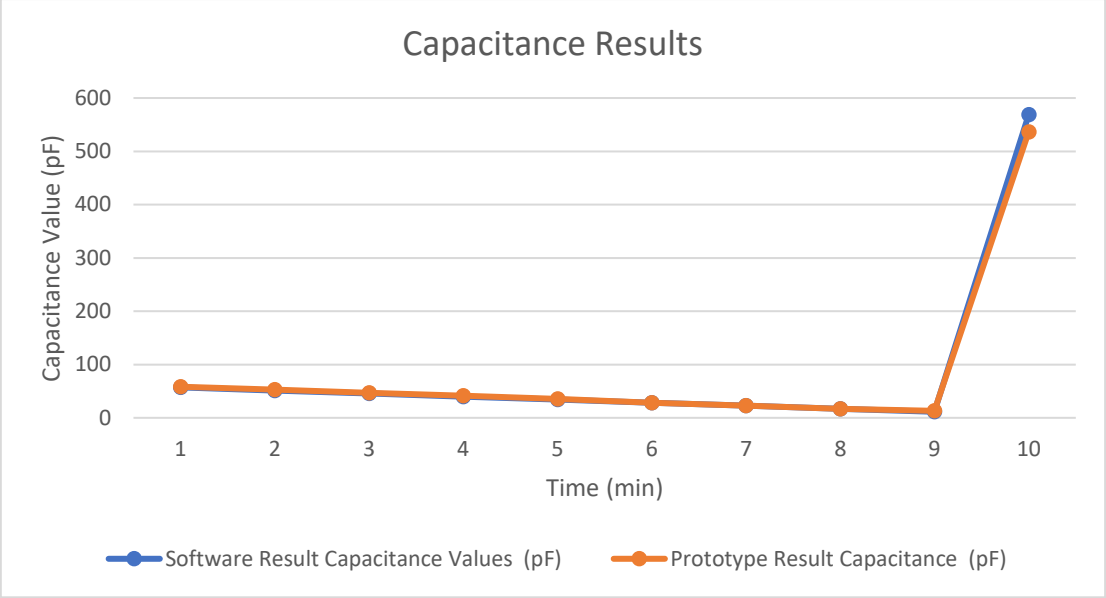

Figure 8.3: Comparison between the software and the prototype results in terms of the capacitance

Figure 8.3 shows the capacitance value from the software tests and the prototype simulation. It also shows the comparison between the simulation capacitances, the marron curve which was calculated from the capacitance value obtained from the output of the sensing circuit on the Multisim and the practical capacitance blue curve, obtained from the FPGA board during tests. These two curves show the patterns from the software simulations and the prototype. Figure 8.3 also shows that the results from the software and the prototype are very close.

In order to have an accurate reading and small error, the cable tampered monitoring system need to be done by measuring the wires type which is used in the test. Error got from the prototype, varies between 1% and 15% results are shown in Table 7.4.

8.2 Chapter Conclusion

In this chapter, the test results obtained from the software and the prototype simulation were analysed. The results obtained between the prototype test and the software test are very close. The analysis of the simulations test results was done and verification made on the prototype performance, the prototype work as per design

CHAPTER NINE: CONCLUSION, FURTHER DISCUSSION AND WORK

9.1 Introduction

This chapter summarizes the dissertation and gives explanation about what was achieved, what was not achieved and the reasons. A summary of the prototype and its performance illustrated, with respect to a telecommunication and utility cable tampering monitoring system was proposed, designed, simulated and analysed. It properly addresses the problem domain and it gives the opportunities of a future work expansion of the research project.

9.2 Implication of the research

The aim of the project was to design and implement a telecommunication and utility cable tamper monitoring system which is able to pinpoint the location of cable tampering. This was achieved and the project showed that when a cable is tampered with the capacitance value from that cable changes and this particular capacitance value is input to the sensing circuit and is converted into a frequency. This frequency is then input to the FPGA which converts it to a distance from sensor. This distance is displayed on the LCD as well as the location where the anomaly took place. Simulation were carried out and it was observed that the following data was read: Capacitance value, period, frequency value, distance from sensor and GPS coordinates.

Since the prototype test indicates the distance from the sensor each time that a cable is tampered with, it can be concluded that the objectives were achieved. The obtained results from the research can be used to detect and reduce cable tampering. The aim of study was to design a cable tampering monitoring system which is able to pinpoint the location of cable tampering, and to investigate cable tampering monitoring system using FPGA technology and a modified reflectometer (sensing circuit); thus, the overall performance of the system.

9.3 Application of the research

The telecommunication and utility cable tamper monitoring system can be use by multiple companies around South Africa where the research was carried out, companies such as:

(i) Electrical Services (ESKOM)
(ii) Train Services (TRANSET, Metro Rail, PRASA)
(iii) Wireless Telecommunications Provider (TELKOM, Vodacom, Cell C, 8ta)
(iv) Local Government and Central Government.

9.4 Limitation of the research

The limitation of this research is that if there is any metallic component, discrete components or paired wire near the capacitance and inductance, the additional items mentioned above will produce an error in the detection of the distance from the sensor. This could be addressed in a future work when redesigning because of time limitation this could not be incorporated in the design.

9.5 Future Work

The work conducted in this research has focused on designing and implementing a cable tamper monitoring system which is able to pinpoint the location where the cable has been tampered with and the distance from the sensor tampered, hardware and software analysis and experimental tests were done as part of the research. The prototype was designed and implemented and testes however, suggestion for future work could be:

(i) The sensing unit should be further expanded by installing more sensors to monitor factors such voltage, current.

(ii) Development of a protective casing for the system to avoid any environmental hazard such (any metallic component, discrete components or paired wire).

9.6 Chapter Conclusion

The main purpose of this research project was to design and implement a cable tamper monitoring system which is able to pinpoint the location of cable tampering. The units of the system comprise a sensing circuit which was implemented combined with the FPGA board, GSM module and GPRS module. Experiments were designed to test the overall performance of the system.

This system was implemented in a way that if there is cable tampering, the prototype detects the anomaly, and automatically inform the user. Based on the results of the research project, the main objective of the thesis has been successfully achieved. The dissertation covers the design and implementation of telecommunication and utility cable tamper monitoring system. To test the feasibility of the telecommunication and utility monitoring system, the simulation results were used to check if the objectives were achieved. This is necessary to determine whether the proposed solution resulted in detection of cable tampering since the aim of the research project was to design and implement a cable tamper monitoring system which is able to pinpoint the location where the tampering took place as well as the distance from sensor cable tampered with, which was achieved.

REFERENCES

AGNIHOTRI, N. 2010 Engineering Garage Inspiration Creation. GSM/GPRS Module. [Online] Available at: <https://www.engineersgarage.com> Accessed 12 April 2016.

AMIN, S.M., WOLLENBERG, B.F. 2005 'Toward a Smart Grid: Power Delivery for the 21st century,' IEEE Power and Energy Mag. 5(3):34-41.

ANDRE, O. 2012. ACDC Dynamics Online. [Online] Available at: http://www.acdc.co.za. Accessed: 16 April 2016.

ARANGUREN, G., NOZAL, L. BLAZQUEZ, A. and ARIAS, J. 2002. "Remote control of sensors and actuators by GSM", IEEE 2002 28th *Annual Conference of the Industrial Electronics Society* IECON 5-8 Nov. 2002, 2(3):2306 - 2310.

BAHRIN, Z.A. & MUHAMMAD H.B.Z.A. 2016. compact copper cable anti-theft system solution. Asian *Research Publishing Network* (ARPN), 11(5):1819-6608, Malaysia, Selangor, [Online]. Available at :< www.arpnjournals.com> Accessed: 10 April 2016.

BERINATO, S. 2007. Red Gold Rush: The Copper Theft Epidemic. [Online] Available at: <http://www.csoonline.com> Accessed 12 June 2016.

BROUN, T.S. 2004. Electricity Theft: a Comparative Analysis. *Journal of Energy Policy Department of Social and Behavioral Sciences*, 32(2):2067-2076. Dubai, United Arab Emirates [Online]. Available at :< http://www.sciencedirect.com/> Accessed: 16 March 2016.

CAO, G., XU, T., LIU, T., YE, Y. & XU, G. 2011. A GSM-Based Wireless Remote Controller. *IEEE International Conference on Electronics*, Communications and Control, 2413-2416, May 2013. [Online]. Available at: < http://ieeexplore.ieee.org > Accessed: 21 March 2017.

COMINS, L. & RIZWANA, S.U. 2010. Stop the cable thieves. *SA Media*. 07-Jun-2010 University of The Free State.

CHENEBERT, A., BRECKON, T.P. & GASZCZAK, A. 2011. "A Non-temporal Texture Driven Approach to Real-time Fire Detection". *IEEE Proc. International Conference on Image Processing*. 1781–1784.

CHO, J.P.S., HAN, Y. and CHUNG, T. 2007. "CAISMS: A context-aware integrated security management system for smart home", 9th *International Conference* on Advanced Communication Technology, ICACT. 531-536.

CHUNG, Y.C., AMARNATH, N.N. & FURSE, C.M. 2009. Capacitance and Inductance Sensor Circuits for Detecting the Lengths of Open- and Short-Circuited Wires. *IEEE*

Transactions on Instrumentation and Measurement, 58(8):2495-2502. [Online]. Available at: < www.sciencedirect.com> Accessed: 10 October 2016.

DEBBARMA, S. 2014. *FPGA Implementation OF Flood Monitoring System in VLSI Design & Embedded System*. Master of Technology in VLSI Design & Embedded System. India: National Institute of Technology Rourkela, Odisha.

DEEPAK, K.P., SHUDHANSHU, T. & ANKIT, T. 2013. Anti-Theft and Monitoring System of Street Lamp Power Cables, *International Journal of Engineering Research & Technology* (IJERT) Allahabad, India. 06 June 2013. [Online]. 6(2): 2278-0181. Available at :< www.ijert.org> Accessed: 1st May 2016.

EDANG, E. 2001. Inexpensive Reflectometer Locates an Open Circuit Along A Cable. *Electronic Design*, 49:(2)115-116. [Online]. Available at: < https://www.electronicdesign.com > Accessed: 21 March 2016.

El-MEDANY, W.M. & El-SABRY, M. R. 2008. GSM-Based Remote Sensing and Control System Using FPGA. *IEEE International Conference on Computer and Communication Engineering*. 1093-1097. [Online]. Available at: < www.sciencedirect.com> Accessed: 10 October 2016.

El-MEDANY, W.M. 2008. FPGA Implementation for Humidity and Temperature Remote Sensing System. *IEEE International Conference on Mixed-Signals*, Sensors and System Test Workshop. 1-4. Available at: < www.sciencedirect.com> Accessed: 10 September 2016.

FUJIYAMA HIROYUKI, 2006. "System-on-a-chip with security modules for network home electric appliances" Fujitsu Scientific and Technical Journal, System-on-a-Chip, 42(2): 227-233.

FURSE, C., CHUNG, Y., DANGOL, R., NIELSEN, M., MABEY, G. & WOODWARD, R. 2003. "Frequency Domain Reflectometry for On Board Testing of Aging Aircraft Wiring," *IEEE Trans. Electromagnetic Compatibility* 306-315, May 2013. [Online]. Available at: < http://ieeexplore.ieee.org > Accessed: 21 April 2016.

GALLI, S. & LE CLARE, J. 2014. Narrowband Power Line Standard in Berger, Power Line Communication: Narrow and Broadband Standards, EMC. Advanced Processing Device, Circuit and Systems. [Online]. 370-300. Available at: <www.sciencedirect.com> Accessed: 10 August 2017.

GANDLA, S., WALEED, K., AL-ASADI, SEDIGH, S., RAGHU, A. and RAO, R. 2008. Design and FPGA Prototyping of a Flood Prediction System, Department of Electrical and Computer Engineering, Missouri University of Science and Technology.

HAN, D.M. and LIM, J.H. 2010.''Smart home energy management system using IEEE 802.15.4 and Zigbee,'' *IEEE Transactions on consumer Electronics*, 3(56): 1403-1410.

HENLE, R.A., KUVSHINOFF, B.W. & KUVSHINOFF, C.M. 1992. Desktop computers: in perspective. *Oxford University Press*. *Server is a fairly recent computer networking term derived from queuing theory*. 417-418.

HESS, T. 2012. Tec Central: Telkom again falls prey to cable thieves [Online]. Available at: < http://www.techcentral.co.za/ > Accessed: 03 August 2016.

INYIAMA H. C., OBOTA M. E., 2013. Designing Flood Control Systems Using Wireless Sensor Networks, *International Journal of Engineering Research and Applications (IJERA)*, 1(3):1374-1382, January -February 2013.

JANI, A. 2003. *Location of Small Frays using TDR*, MS Thesis. Utah State University, Logan, Utah.

KUECK, J.D., KIRBY, B.J., OVERHOLT, P.N. and MARKEL, L.C. 2004. "Measurement Practices for Reliability and Power Quality," Oak Ridge National Laboratory, Oak Ridge, Tennessee, managed by UTBATTELLE, LLC for the U.S. Department of Energy, Jun. 2004[Online].Available:http://www.ornl.gov/sci/btc/apps/Restructuring/ORNLTM2004 91FINAL.pdf

LI, F., QIAO, W., SUN, H., WAN, H. and ZHANG, P. 2010. ''Smart Transmission Grid Vision and Framework,'' *IEEE Tran Smart Grid*,2(1):168-177.

LI, L., XIAOGUANG, H., JIAN, H. AND KETAI, H. 2011. ''Design of new architecture of AMR system in Smart Grid,'' *Proceedings of the 6th IEEE Conference on Industrial Electronics and Applications (ICIEA),* June 2011. 2025-2029.

MACKAY, S., WRIGHT, E., REYNDERS, D. & PARK, J. 2004, Practical Industrial Data Networks: *Design, Installation, and Troubleshooting*, *Newnes.*41-42.

MALMSTADT, ENKE AND CROUCH, 1981 Electronics and Instrumentation for Scientists*, The Benjamin/Cummings Publishing Company*, Inc.

MEIER, J. & JHANGIANI, J. 2007. Evaluate Test System Impedance Matching and Switch Quality. *The effect of impedance matching and switch quality can play major roles in achieving accurate and repeatable measurements with RF/microwaves test system*. [Online]. Available at: < https://www.mwrf.com > Accessed: 03 February 2016.

MENDOZA, J.J., VARGAS, O.G., CASTA, M.R. & VENTURA, R.E. 2005. *FPGA-based real-time remote monitoring system*. Computers and Electronics in Agriculture, Biotronics Laboratory, Faculty of Engineering, Universidad Autonoma De Queretaro,

Mexico. 12 January 2005272-285. [Online]. Available at: < www.sciencedirect.com> Accessed: 10 October 2016.

MOHD CHACHULI, S.A., MOHD NAZRI, S.N., YUSOP, N. & MOHAMAD, N.R. 2016. Cable Theft Monitoring System (CTMS) Using GSM Modem. *Journal of Advanced Research in Applied Sciences and Engineering Technology ISSN*, Melaka, Malaysia. 20162(1): 12462-1943. [Online]. Available at :< http://akademiabaru.com/> Accessed: 20 April 2016.

NETL Modern Grid Strategy. 2008. 'Advanced Metering Infrastructure'. U.S. Department of Energy, National Energy Technology Laboratory, Mag, (1):2-3. March 2008, [Online]. Available http://www.netl.doe.gov.

NIEUWENHOUT, F., DOGGER, J. and KAMPHUIS, R. 2005. ''Electricity storage for distributed generation in the built environment,'' *IEEE Conference Publications*. 5-8

NSTC, 2000 "Review of federal programs for wire system safety," in White House Rep., Nov. 2000.

PARK, J.J., YANG, L.T., LEE, C. 2011. 'Future information Technology' 6th *International Conference, Future Tech 2011, Processing part*-2, 215-222.

PATRICK, D.R., FARDO, S.W. 2009.'Electrical Distribution Systems,' 2nd Edition 2009. 1-12.

RAHIMI, F. and IPAKCHI, A. 2010. ''Demand Response as a Market Resource Under the Smart Grid Paradigm,'' *IEEE Trans. Smart Grid*, 1(1):82-88.

RAYMOND, J. & WOODWARD, 2000. *Using frequency domain reflectometry for water level measurement.* MS Thesis, Utah State University, Logan, Utah.

SCHMITT, OTTO, H.C. 1941. Push-Pull Resistance Coupled Amplifiers. *Review of Scientific Instruments.* 8 (1): 20–21.

SCHWAGER, A. & BERGER, L.T. 2014. PLC Electromagnetic Compatibility Regulations. Power Line Communications: Narrow and Broadband Standards, EMC. *Advanced Processing Device, Circuit and Systems*. [Online]. 169-186. Available at: < www.sciencedirect.com> Accessed: 10 August 2017.

SCOTT, B.J., WRAITH, J.M. & DANI 2002. Time domain reflectometry measurement principles and Applications, USA: *Institute of Electrical and Electronics Engineering (IEEE)*, [Online]. 126-145. Available at: < http://ieeexplore.ieee.org > Accessed: 21 March 2016.

SMAIL, M.K., HACIB, T., PICHON, L.& LOETE, F. 2011, Detection and Location of Defects in Wiring Networks Using Time-Domain Reflectometry and Networks*, IEEE*

Transactions on magnetics, 47(5):1502-1505, [Online]. 126-145. Available at: < http://ieeexplore.ieee.org > Accessed: 21 March 2016.

SMITH, T.B. 2004. Electricity Theft: A Comparative Analysis. *Elsevier Journal of Energy Policy*, 32(2)1:2067-2076. Dubai, United Arab Emirates [Online]. Available at :< http://www.sciencedirect.com/> Accessed: 26 April 2016.

STAFF, W. 2012. *Cable Theft brings down more Telkom services* [Online]. Available at: < http://mybroadband.co.za/ > accessed: 16 April 2016.

SULAIMAN, A., BURHANUDIN, M., ABIDIN, K.B.Z. & AZLAN, M.H.B.Z. 2016. Compact copper cable anti-theft system solution. *Journal of Engineering and Applied Sciences*. [Online]. 11(5):3133-3136. Available at :< www.arpnjournals.com > Accessed: 03/16/2016.

TICHELMAN, B. 2007. ‘‘Using Smart Grid TO Address our Aging Infrastructure’’ (12):3-4, 26 Oct, 2007. [Online]. Available: http://www.elp.com Accessed: 03/16/2018.

WADDOUPS, B. 2001. *Analysis of reflectometry for detection of chafed aircraft wiring insulation.* MS Thesis. Utah State University. Logan, Utah.

WEN-TSAI, S. & YAO-CHI, H. 2011. *Designing an industrial real-time measurement and monitoring system based on embedded system and ZigBee*, Department of Electrical Engineering, National Chin-Yi University of Technology, Taiping, Taichung, Taiwan. [Online]. 4522–4529 Available at :< www.sciencedirect.com> Accessed: 05/10/2016.

WILLIS, H.L., SCHRIEBER, R.R. 2012. ‘Aging Power Delivery Infrastructures,’ CRC Press, 2012. [Online]. Available: http://www.quanta-technology.com.

XIANGJUN, Z., WENTAO, Y., ZHANGLEI, L. 2008 Novel Technique of Capacitive Current Resonance Measurement with Signal Injected for Distribution Networks. *Automation of electric power systems*, 4(32):77-80.

XIAORUI., H.U., YANLONG, Q., WEI, C. & FAN, Y. 2014. Anti-theft and location method based on pulse transmission attribute for power cable, *International Symposium of Fundamentals of Electrical Engineering University Polytechnics of Bucharest*, Romania, 28-29 November 2014, [Online]. Available at: < http://ieeexplore.ieee.org > Accessed: 16 Mae-erch 2016.

YORK, T. A. EVANS, I. G. P*OKUSEVSKI, Z. & SOURCE,* T. 2001. Particle detection using an integrated capacitance sensor. *Sensors and Actuators*, A: Physical, 92(3):74-79.

YUANYUAN, WANG, JINBAO, J., XIANGJUN, Z. & SIDONG, L. 2011. “Anti-theft monitoring and location system for cable of street lamp.” *In Electric Utility Deregulation and Restructuring and Power Technologies* (DRPT), 4th *International Conference* on.

11(2): 315-319 Weihai, Shandong [Online]. Available at :< http://ieeexplore.ieee.org > Accessed: 03/16/2016.

ZANG, D.T. 2008. The Anti-theft alarm system of power cable based on the power line carrier and GSM communications. *journal of Northeast Dianli University Natural Science Edition.* 1(2):84-88. [Online]. Available at :< http://ieeexplore.ieee.org > Accessed: 03/16/2016.

ZHAI, Y. & CHENG, X. 2011. Design of smart home remote monitoring system based on embedded system, Innovative Training Project Fund of Inner, 11(6):978-980.

ZENG, X.J., YI, W.T. & LIU, Z.L. 2008. 'A novel technique of capacitive current resonance measurement with signal injected for distribution networks', Automation of Electric Power Systems, 32(4):77–80.

ZHEN, Y. 2009. Study on a new cable guard alarm system based on fuzzy state estimation. *4th International Conference on Computer Science & Education*. Xiamen University Xiamen, China 3521-4244.

ZHENGYA, X. 2003. Digital Protection for Power Transformer and Medial-Low Voltage Electric Power Net[M), Beijing: China water and power public,2003

ZHENYU, T. & JINLING, Z. 2004. Research of network distributed remote control system based on GPRS, Micro-Computer Information (Control Automation), 20(12):31-32.