RESEARCH ARTICLE OPEN ACCESS

Pipeline Vandalisation Detection Alert with Sms

G.N Ezeh[1], N. Chukwuchekwa[2], J .C. Ojiaku[3] and E. Ekeanyawu[4].
Department Of Electrical And Electronic Engineering Federal University Of Technology Owerri. Imo State, Nigeria.

ABSTRACT
Automated crack and vandalism detection alert for pipeline with remote monitoring and location specification is implemented in this study. The design circuit consists of transceiver (GSM module), microcontroller, power supply and alarm nits. Simulation of the various units was done individually using visual modeling application Proteus. Most of the components used in the research were available on the software and alternatives with similar specifications were used for components that were not available on the Proteus for simulation purposes only. A continuous electrical path was provided by resistant sensor and any break in the signal path causes cessation of signal and provides detectable change in the state of the system. The system was tested on performance of the task of detecting breakage on pipelines and the exact location of such problems.
***KEY WORDS*:** Impact Sensor, Microcontroller, Pipeline Monitoring, SMS Alert, Security, Transceiver.

I. INTRODUCTION

Pipeline system as a medium of transportation is usually attributed to very sensitive products such as crude oil, natural gas and industrial chemicals, in which unattended problems in their operation results in unimaginable catastrophe. These problems include terrorism attacks, vandalism and theft of the pipeline content. The need for implementing adequate security systems for pipeline management has been addressed from time immemorial. While some of these attempts have recorded some level of success, others have contributed insignificantly to this outstanding challenge that is currently giving mankind sleepless nights.

Vandalism refers to illegal or unauthorized activities that results in the destruction of petroleum, gas and chemical pipelines. It is a negative activity aimed at getting products for personal use or for sale in the black market especially in developing countries of the world where they are rampant. About 40% of the world's oil flow through pipelines which run thousands of kilometers across some of the most volatile areas of the world[1].

This makes pipelines potential targets for terrorists. A simple explosion could puncture a pipeline making it non-operational. Due to their length, they are very difficult to protect. The horror scene, of pipeline disaster in the suburb of Lagos city on 26th December, 2006 was a national disaster. Nigerian militants have repeatedly attacked pipelines and related facilities, including the simultaneous bombing of three oil pipelines in May, 2007. In the year 2011, the cost of vandalism and oil theft in Nigeria was put at over $12 billion (N1.8 trillion) [4]. The level of oil theft in Nigeria is becoming alarming and will continue to increase if left unattended. Thus many security measures involving sophisticated technologies have been implemented to mitigate the damages, leakages and failures obtainable in pipelines.

Most of these technologies are very expensive and require a great deal of knowledge to install and operate. The design presented in this study is able to remotely monitor and notify an operator of any form of impact on the pipeline leading to damage and localized fault with the help of the infrastructure of the existing mobile network. This will go a long way in stopping the theft of pipeline products, environmental degradation and also accidental deaths which often result from the explosion of those flammable substances when leakage occurs.

II. THEORY OF THE SYSTEM

Pipeline networks are important parts of the national energy transportation infrastructure vital to the national economy. It is an indispensable means for conveying water, gas, oil and all kinds of products. Undoubtedly, the pipeline project is one of the most important infrastructures in Nigeria as it stretches several thousands of kilometers and passes through cities, villages and rural communities across the country. These pipelines are operated at high pressure and any failure or damage poses a great danger to human health and properties, environmental and ecological disaster and interruption of gas or oil supplies. The pipelines are prone to losing their functionality by any internal or external corrosion, cracking, third party intrusion and manufacturing flaws, thereby leading to damage, leakage and failure with serious economic and ecological consequences.

Third party mechanical damage has proven to be the most serious problem encountered by pipeline industries on their facilities located onshore. The third party damage includes terrorist attacks, vandalism, impact of heavy duty equipment used in construction and agricultural works. These damages to pipelines, if undetected can be catastrophic. They often result in environmental pollution, financial losses and loss of life. Between 1998 and 2009, Nigeria lost over two thousand people to pipeline explosions across the country, pipeline vandalism and attempts by local residents to scoop fuel from vandalized pipelines as shown in figure 1.0. These have accounted for one of the major causes of high mortality rate in Nigeria[1].

Also, over 5,000-kilometers of pipelines are routinely broken down and about 250,000 barrels of crude is stolen daily for sale on the local and international black markets, reportedly costing the country about $6bn to $12bn annually. From 2002 to 2011, records show that about 18,667 incidences of vandalism occurred [2]. Figure 1.1 also shows Vandalized pipeline.

Figure 1.0 Vandalized pipeline and people scooping fuel.

Figure 1.1 Vandalized pipeline

Furthermore, according to the Nigeria National Petroleum Corporation (NNPC), Nigeria lost about N163billion in three years to pipeline vandalism [3]. Pipeline vandalism has crippled fuel supply and incurred over N174billion in product losses and pipeline repairs [4].
The recent jetty explosion in Lagos was as a result of pipeline vandalism [5].

III. MATERIALS AND METHODS

3.1 COMPONENT DESIGN-MICROCONTROLLER

Present-day applications of microcontroller had their beginning in the development of technology of integrated circuits. This development has made it possible to store hundreds of thousands of transistors into one chip. That was a pre-requisite for production of microprocessors, and the first computers were made by adding external peripherals such as memory, input-output lines and timers. Further increase in the volume of the package resulted in creation of integrated circuits[6]. These integrated circuits contained both processor and peripherals. The microcontroller used in this work is PIC16F628A. The functions of microcontroller include powering the system automatically, initializing the GSM module, interpreting the received signals and sending the required signal to the GSM module or the transceiver.

The GSM module used in this design is an already made module and was interfaced with the microcontroller through the serial interface unit. The SIM900 GSM module used has the following general features.

- Quad-band 850/900/1800/ 1900MHz
- Supply voltage range 3.4V to 4.5V
- Low power consumption

Also, any mobile phone can be used as a transceiver. In the case of GSM module, MAX232 is needed to be incorporated in the circuit design to do the necessary voltage conversion.

3.2 COMPONENT DESIGN-POWER SUPPLY

For any electronic device to work, it must require a source of power.
Most of the semiconductor components do not require high voltage supply for them to work and most of them are destroyed permanently if they are supplied with a high voltage.
Figure 2 shows the Circuit diagram of power supply unit.

The diodes used for rectification have a maximum voltage rating of 50V, thus a transformer is needed for stepping it down. A step-down transformer with a transformation ratio of 20:1 was used to convert the input voltage to ±12V. The diodes D_1, D_2, D_3 and D_4 are arranged and used to rectify the

low voltage A.C to a D.C output with ripples. The capacitor **C** is used to filter out the A.C ripples and allows only the D.C part to flow to the regulator. The regulator produces the 5V used to power the rest of the circuit. In most designs, assumptions are always made to ensure certain conditions are accomplished.
The assumed values hence help in calculating the variables.
The following assumptions were made:
Input frequency = 50Hz
Secondary voltage of the power transformer, T_1 = 12V
Ripple voltage, Vr < 5mV
Using

$$V_{max} = V_{rms} * \sqrt{2} = 12 * \sqrt{2}$$
$$= 16.97V \approx 17V$$

This value helps in calculating the peak inverse voltage of the rectifying diodes.
Peak inverse voltage of diodes

$$(D_1 - D_4) > \frac{3}{2} V_{max}$$
$$PIV > \frac{3}{2} \times 17$$
$$\approx 26V$$

A silicon diode with data number IN 4001 has a peak inverse voltage of 50V, and a maximum safe current of 1A. Applying the laws of semiconductor component use, the rated values must always be higher than the operational values. IN4001 is very suitable since its operational value of 26V PIV is less than the rated value of 50V.
Therefore, $D_1 - D_4 = IN\ 4001$
Capacitor C_1 and C_2 can be calculated using the formula

$$C \geq \frac{1}{4\sqrt{3} * f_o * V_r * RL}$$

Where, f_o = Output frequency
V_r = Assumed ripple voltage (5mV)
RL = Expected load resistance taken here to be 300Ω
F_i= Input frequency of 50Hz

$$f_o = 2 * f_i = 2 * 50 = 100Hz$$

Therefore,

$$C \geq \frac{1}{4\sqrt{3} * 100 * 0.005 * 200}$$
$$= 450\mu f$$

Standard value = 470µf

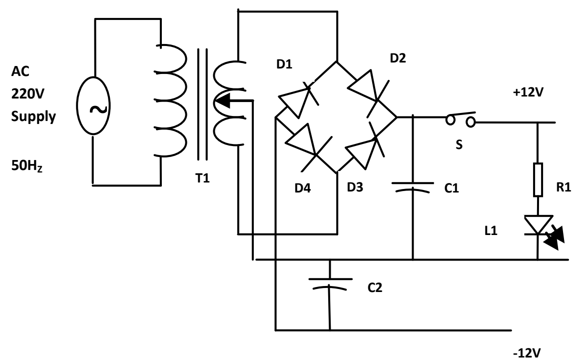

Figure 2: Circuit diagram of power supply unit.

3.3 SYSTEM BLOCK DIAGRAM DESCRIPTION

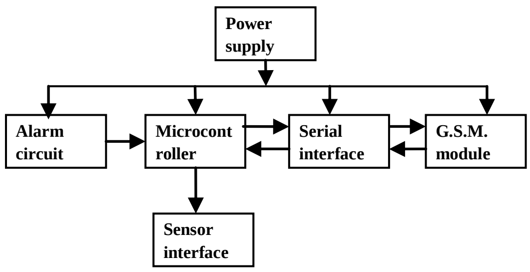

Figure 3: System block diagram.

Figure 3 shows the various building blocks or major sections of the work.

With the help of the basic block diagrams, the entire circuit can be divided into smaller units and designed separately so as to make the work less complicated. It comprises of

- The power supply unit
- Alarm unit
- The control unit
- Serial interface unit
- The G.S.M module
- Sensor interface unit

3.4 SYSTEM FLOW CHART

Figure 4 describes the algorithm for the software design of the program in a flowchart model.
Assembly language programming has been the popular method for writing the programs needed by most microcontroller of this grade but the coding of the microcontroller used for this work was done using a high level language known as C language. This language has an edge over the assembly language in the sense that it is coded in a clear English language format unlike the latter, where

mnemonics and operands are used. The program was written with Dev C++ and compiled. The PIC Kit2, an already made programmer was used to load the program into the microcontroller using MPLAB software.

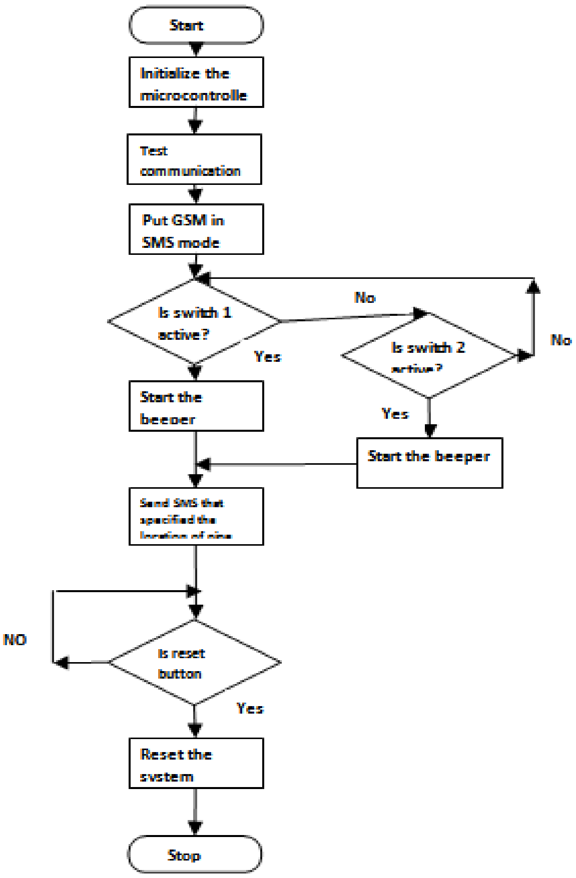

Figure 4: System flowchart

Figure 5 shows the main circuit diagram of the system

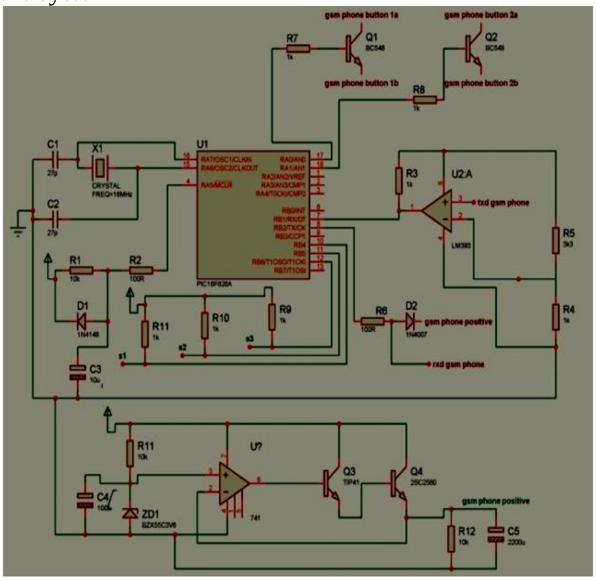

Figure 5: System circuit diagram.

IV. TESTING AND RESULTS

It is now common in our present age to model and simulate a work before implementing or producing a physical prototype of the work. This has been made possible by the advances in technology in the areas of computer software engineering. Thus, the conceptual design of the work can be simulated on a computer system to analyze the behavior of each unit of the system and the entire system as a whole after integration, hence ensuring that the system is working before resources can be dedicated to the hardware implementation. This helps in saving time and money. The simulation of the system was done using Proteus Virtual System Modelling software, an electronic simulation software running on a personal computer. Most of the components used were available on the software. Alternatives with similar property were used for the components that were not available on the Proteus for simulation purposes only. The microcontroller program was written in C language, converted into hex codes and loaded into the microcontroller in the software for the simulation process. Some of the results obtained while running simulation test using proteus are shown in figures6,7 and 8 indicating the exact location of breakage when the pipeline is tampered with.

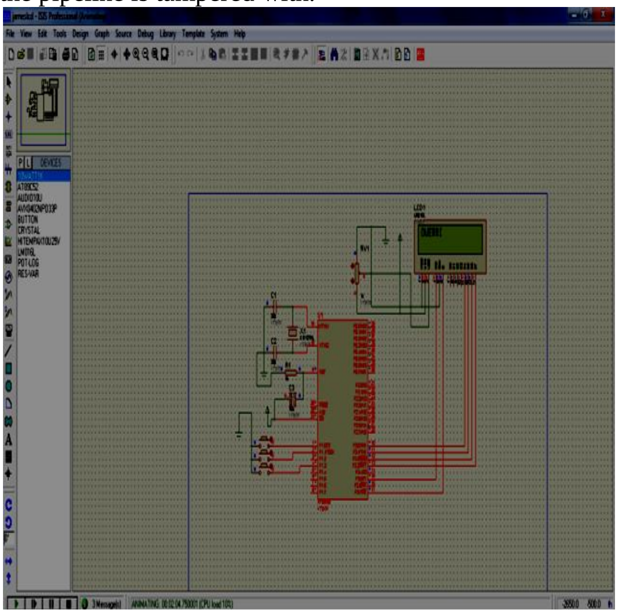

Figure 6: Breakage at Owerri

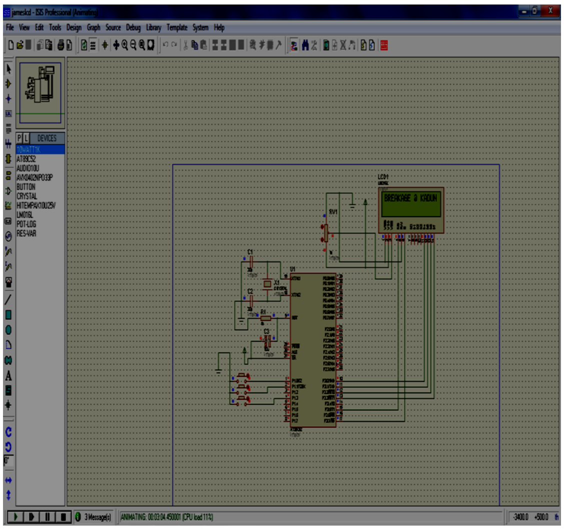

Figure 7: Breakage at Kaduna

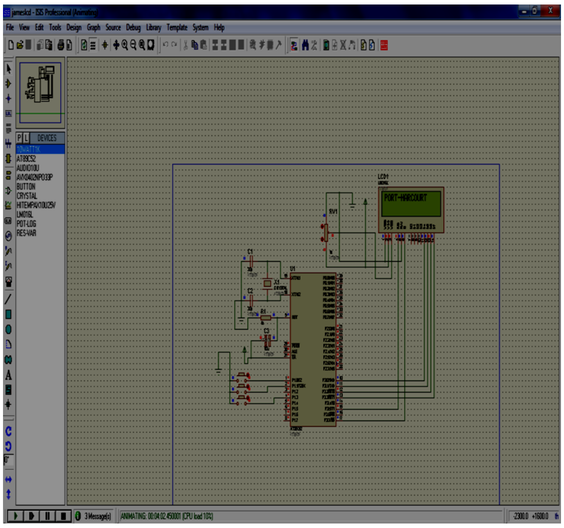

Figure 8: Breakage at Port-Harcourt

The system produced results that met the system specifications and the entire system objectives. When the sensor used in the design was broken, the system detects the breakage and the control unit sends out signal to the alarm unit to activate the buzzer alarm.

Also, the LED indicator indicates the transmission of signal. The indicator and the alarm continue to indicate a breakage at the sensor until the SMS is sent to the operator. The SMS will be received by the operator three times consecutively indicating the actual location of vandalism. The system automatically switches off after transmitting the alert signals.

V. CONCLUSION

A method for providing automated crack detection for pipeline with remote monitoring and location specification was developed in this study. A continuous electrical path was provided by resistant sensor and a break in the signal path will cause cessation of the signal and provide detectable change in the state of the system. This results to triggering of an alarm and notification via SMS to an operator's mobile phone. The benefits of this study include early detection of pipeline damage, reduction in financial losses and alleviation of environmental degradation.
The sensor design in this work can be modified into a sheet having a signal path for either electric signal or optical signal and wrapped around the pipeline over a predetermined length. The sensor can also be incorporated early into the design of the pipeline system either by wrapping it on the outer surface or covered with a resin so as to improve its reliability.

REFERENCES

[1] A nation in search of pipeline safety www.saharareproters.com/nigeria

[2] Shifts in pipeline vandalism in Nigeria www.aggbrokomeyer.word.com/2013

[3] NNPC lost about N163billion in the space of three years to pipeline vandalism www.thisdaylive.com (visited 19th August; 2013).

[4] How pipeline vandals cripple fuel supply.www.nnpcgroup.com/public relation (Visited 19th August; 2013).

[5] Lagos Jetty explosion caused by pipeline vandalization. www.informationng.com (visited 19th August; 2013).

[6] www.wikipedia.org/PIC_microcontroller

[7] PIC16F628A datasheet

[8] Ihueze C.C(2011) "Communication systems for pipeline protection in Nigeria Niger Delta" Global research publishing, (pp. 213-222).

[9] Olugboji, O. A. (2011) "Development of An Impact Monitoring System for Petroleum Pipelines," United Kingdom.

[10] Mehta V. K. and Mehta, R. (2010) "Principles of Electronics," Ram Nagar, New Delhi, S. Chand and Company LTD.