International Journal of Informatics and Communication Technology (IJ-ICT)
Vol.10, No.1, April 2021, pp. 65~74
ISSN: 2252-8776, DOI: 10.11591/ijict.v10i1.pp65-74

Design and implementation of an integrated pipeline security system with optmized scheduling

U. K. Okpeki, A. O. Oyubu
Department of Electrical and Electronics Engineering, Delta State University, Abraka, Delta State, Nigeria

Article Info

Article history:

Received Nov 4, 2020
Revised Jan 22, 2021
Accepted Feb 8, 2021

Keywords:

Coverage
Design
Microcontroller
Offshore
Processor
Security
Surveillance

ABSTRACT

Offshore equipment and facilities are some of the most capital intensive and strategically located assets that require millions to billions of dollars to setup. Thus, it is important to put in place a stout security and surveillance system to ultimately protect these assets from vandalisation and theft. Monitoring of intruders/ unfamiliar objects within and outside the offshore platform requires a round-the-clock observation through provided security personnel who are stationed so as to quickly respond to any threat within a safe distance in the event of any physical intrusion but this measure is fraught with some challenges. Some of these challenges include fatigue, error in human judgement, and the limited vision of humans to mention but a few. To remedy these weaknesses and ensure a robust protection, the design and implementation/ setting up of a surveillance system to detect and track real time security concerns with a much wider and effective coverage area to enable the control unit make a well informed decision appropriately is an imperative. The system presented in this paper is designed to operate in harsh (sea waves, and fog) and unprotected (extreme heat, cold precipitation) environment.

Corresponding Author:

U. K. Okpeki
Department of Electrical and Electronics Engineering
Delta State University
P.M.B. 1, Abraka Delta State, Nigeria
Email: akposweet@yahoo.com

1. INTRODUCTION

Since offshore equipment and facilities are about the most capital intensive and strategically located assets that require a colossal amount of capital ranging from millions to billions of dollars to setup, it is absolutely necessary to put in place a robust security and surveillance system to ultimately protect these capital intensive investment. This is not only due to their vital economic importance to our country, Nigeria, but also due to their high rate of vulnerability to both internal and external threat which could result to a potential nightmare to lives and property on board the various offshore platforms. Over the years, many technologies have evolved in the area of security and surveillance. Video surveillance, closed-circuit TV, IP Camera system, Digital or Network Video recorder (DVR/NVR) among other systems have become so ubiquitous and have become almost absolutely necessary to business organisations, homes, and industries' security and safety [1]. As of date, Video Surveillance System, (VSS) has become indispensable to virtually every sphere of human endeavour in this century.

Monitoring of unfamiliar objects within and outside the platform requires a round-the-clock observation by the provided security agents, who in the event of any physical intrusion, quickly respond within a safe distance; however, this measure is fraught with some challenges. Some of these challenges

include fatigue, error in human judgement, and the limited vision of humans to mention but a few. To remedy these weaknesses and ensure a robust protection, the design and implementation/ setting up of a surveillance system to detect and track real time security concerns with a much wider and effective coverage area to enable the control unit make a well informed decision appropriately is an imperative [2, 3]. The designed system which addresses the issues of security and safety as presented in this paper, can be implemented on industrial facility, oil and gas platform, as well as residential building and environs.

A security system based on the internet-of-things in which an IOT device, Raspberry Pi was used is presented in [4].The surveillance system incorporates a camera that serves as the sensor of the system. The camera detects motion and automatically captures a video of the region where the motion is detected. The proposed design only focuses on detecting motion and relies on the interpretation of the captured video for appropriate action(s) to be taken. An error in human judgement might lead to false alarm among other shortfalls and defeat the aim of setting up the system. The authors in [5] developed a home security system using internet –of –things with online data server based on FAVORIOT platform. Their design incorporates among other things, a microcontroller equipped with internet module, both Passive infrared (PIR), and infrared sensors which detect the intruders/unauthorized entry. The data received are sent to the microcontroller for transmission to the end user. The sensors used in this work can be tricked by a smart criminal and the data sent compromised.

A proposed design which is an improvement on the traditional home security system, CCTV was implemented in [6] using Raspberry Pi 3, Arduino, webcam, and a PIR sensor. In this proposed system, the PIR detects movements and activates the webcam to capture; and upon successful capturing, triggers an alarm to warn the end user. Issues of safety from possible gas attack and imminent fire outbreak were not contemplated. The authors in [7] built their system around a microcontroller, the Arduini uno, to interconnect the various components, a magnetic Reed sensor to monitor the status, a buzzer for blaring the alarm, and a WiFi module, ESP8266, to interface and communicate utilizing the Internet. Again, the vulnerability of the internet to hackers and the possibility to tamper with the data being sent are of major concern in this system. A modern home security system that is capable of noticing an intruder, whether the intruder's face is slightly or totally concealed with materials of fabric, leather, fibre or plastic is proposed in [8]. The proposed system is also able to detect invaders/burglars utilizing CCTV camera not having night vision features. The issue of error in human judgement in interpreting the captured video, and the possible delay before appropriate action(s) is taken is a concern here.

The works, [4-8], rely only on the detection of movement and eventual video capture to secure the home and facilities where such security system is deployed. Factors that may jeopardize human life and property were not contemplated. Our work in addition to the detection of movement/intrusion either by humans or animals through its motion sensor is also able to sense gas leakages which may be coming from a cracked or damaged pipe or from a possible gas attack through the incorporated gas sensor, and detects high temperature which may lead to fire outbreak on oil platforms using the temperature sensor and alerts personnel in real time; thus guaranteeing safety. Since many of the existing systems rely on camera to detect intrusion and identify the intruders, real time alert to personnel to take immediate action(s) against intruders and possible attackers will not be possible. The intruders may only be identified after the theft or attack had been committed.

The power supply used in this work is designed to obtain a stabilized +12v and +5v dc power to the main circuit. The ICs used are low power ICs, each of which can take a dc voltage ranging from 3v to 6v (for the ICs requiring 5v) and 3v to 15v (for the ICs requiring 12v) for proper operation. 220/240Vac, 2000mA with a turn's ratio of 16: 1 was used for its complexity of the circuit which would require substantial amount of power to operate properly. A 50V, 3300μF in the design was used to maximize dc voltage obtain from rectified output which should be at least twice less than the voltage needed by the filtering capacitor. In order to obtain the regulated +12v and +5v, voltage regulators of 7812 and 7805 were used in the design. However, 7815 was used to turn on the relay. At the heart of the smart pipeline security system, is a controller unit acting as a Processor. The controller unit is designed to power actuators like LEDs, LCD-display, Buzzer, and LCD screen. The design consists of the following sensors: Motion, Gas and Temperature sensors.

2. LITERATURE REVIEW

Security which is generally the state of being free from danger or threat can in another sense be said to be the safety of a State, Organization or Industry against criminal activities such as terrorism, theft, piracy, espionage, or vandalization of pipe lines both in offshore and onshore. A major measure that has over the years been adopted to ensure proper security of offshore equipment and facilities is surveillance. Surveillance is simply the monitoring of behaviour, activities, or other changing information for the purpose of influencing, managing, directing, or protecting people. This can include observation from a distance by

means of electronic equipment such as closed-circuit television (CCTV) cameras or interception of electronically transmitted information such as Passive Infrared detector or phone calls. Over the years, many security systems have been developed and deployed to ensure adequate security of equipment and facilities both in residences and industries, but a number of concerns have cropped up regarding the effectiveness, stability and the security of these security systems.

A number of worries regarding Video Surveillance System are connected to privacy concerns for palpable reasons. The consequences of the privacy of VSS are crucial considering the disclosures circulating around universal surveillance programme [9], and the unethical behaviours emanating from video surveillance especially [10]. Outside these worries, a Video Surveillance System that is vulnerable or tampered with could give rise to a plethora of other concerns that are not associated with privacy. For instance, a breach of the VSS was sported to have put the security of a correctional facility in jeopardy [11], exposed organisations that deal in currency like banks, and clubs [12] to the danger of robbery, or interrupt the operations of Cops and law-enforcement [13]. In [14], the passkey used in the work is different for each individual at home, which improves the odds for hacking the keypad. Moreover, these passkeys are chosen by users who are vulnerable to social engineering and other hacks.

In a number of the proposed systems assumptions of possible sophisticated attackers were not made; thereby making such systems to be no match for sophisticated attackers. The systems also do not consider any other entry points into the home apart from the front door, thus, a home secured with such systems is still very vulnerable to unauthorised entrants who can gain entry through other openings other than the front door. The LED and IR sensors used by [15] to identify intrusions could easily be spoofed by a sophisticated attacker. In [16], the authors pointed out the increase in security of the home because of remote access. The user can be made aware of an intrusion as soon as it happens, so that he can view the home through various cameras installed at different parts of the home. The paper completely ignores the plethora of security vulnerabilities that exist in the devices used to connect and automate a home. Moreover, the chance of an attacker exploiting these vulnerabilities is increased significantly when the home is connected to the Internet. In addition, the cameras used in this work have security issues, which are discussed as follows:

The works of [17-19] implement cameras at home. Streaming live video feeds over the Internet is never a good idea, especially when it is from inside the home. If these implemented cameras are compromised, then the attacker will have an eye inside the home. A BBC report by [20] highlighted the vulnerabilities in wireless cameras. Moreover, people do not like to be watched; it affects their normal behaviour and makes them uncomfortable. The infrared sensor-based intrusion detection system specified by [18] can be spoofed by a skilled intruder, so its ability to identify intruders can be queried. In [19], the authors provided users access to the home using a web browser. This opens the home to a different set of browsing-related security issues like session hijacking, cookie stealing, and cross-site scripting.
The work done by [17] can only provide limited security, as they only used cameras and no other security mechanisms in their system.

3. MATERIALS AND METHOD

This section describes the selection of the different components, the approximate calculations and design specifications of the work. The Integrated Pipeline security system with optimised scheduling is an integration of automation system and security. The design analysis begins with a detail engineering design of the power pack, transceiver, amplifier units and the various sensors that make up the system. The block diagram of the design is as shown in Figure 1.

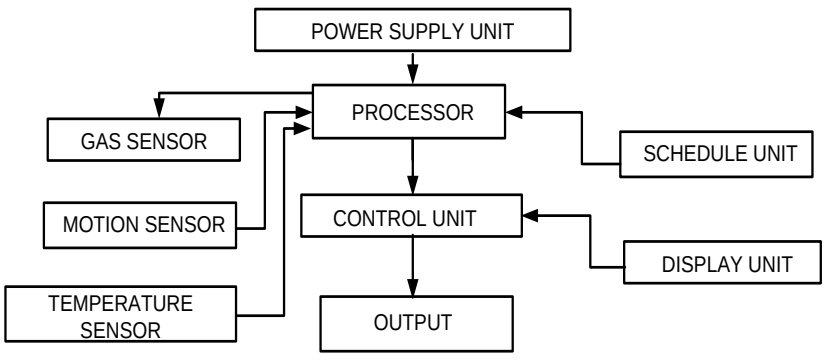

Figure 1. Block diagram of the designed system

3.1. Power supply unit

The aim of this unit is to obtain a stabilized +12v and +5v dc power supply to the main circuit. The ICs used are low power ICs, each of which can take a dc voltage ranging from 3v to 6v (for the ICs requiring 5v) and 3v to 15v (for the ICs requiring 12v) for proper operation.

3.1.1. The transformer

The ratings of the transformer used in this work is as follows.

Input voltage - 220/240Vac
Output voltage - 15Vac
Current rating - 2000mA

In the market transformers are rated based on current bearing capacity as follows: 300mA, 500mA, 1000mA, 1500mA or 2000mA (2A).

220/240Vac, 2000mA with a turns' ratio of 16: 1 was chosen owing to the complexity of the circuit which would require substantial amount of power to operate properly.
Hence, the maximum power required computed from the transformer rating

P = IV where I = Current and V = Voltage
= 2 x 15
= 30 watts

The calculation below shows how a perfectly regulated voltage of +12v and +5v dc were obtained. The transformer, T1 is a step-down transformer of 220/240Vac to 15Vac. This a.c voltage is rectified to d.c by the bridge rectifier D1-D4, while capacitors C1 and C2 serve as filter capacitors as shown in Figure 2.

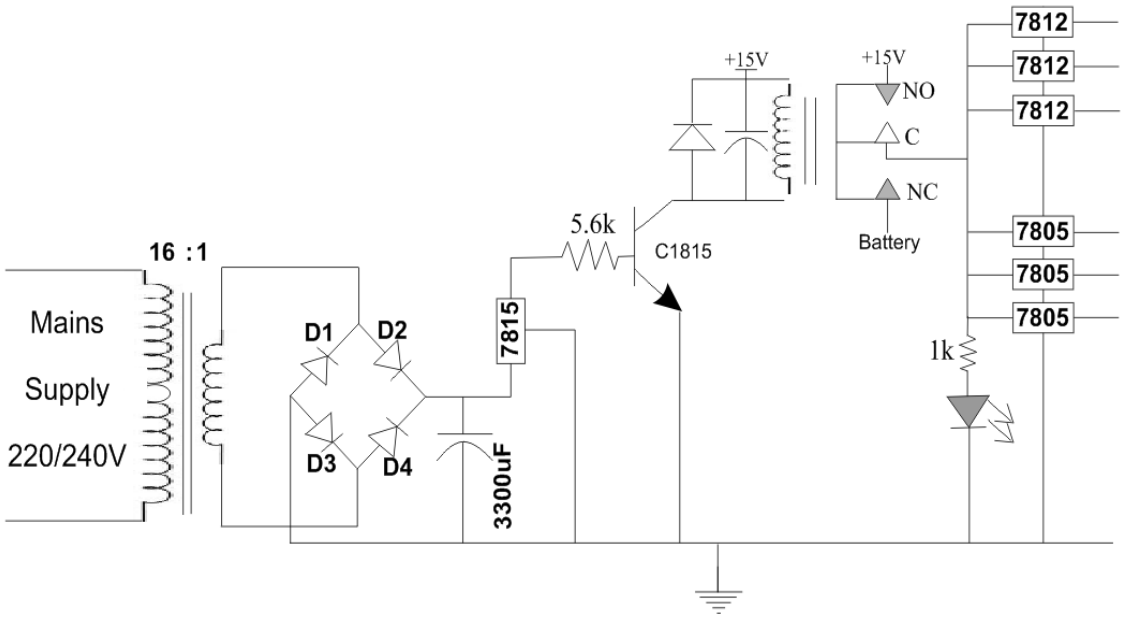

Figure 2. The power circuit of the designed system

3.1.2. Rectifying diode

The rectifying diode IN4001 used in the design has the following specifications.

Peak Reverse Voltage 50 V
Maximum Blocking voltage 50 V
Rectified Current at 75ºC 1A
Overload surge 8.3ms 50A
Junction capacitance 30pF
Operating Temperature -65 to +175

3.1.3. Capacitor specification

C_1 = 3300 x 10^{-6} f, 50V, C_2 = 0.1uf +5%, A 50V, 3300µF was used in the design, owing to the fact that maximum dc voltage obtain from rectified output should be at least twice less than the voltage needed by the filtering capacitor. C_2 is an optional capacitor but put in place to remove any residual a.c ripples from the supply and the chosen value is, 0.1 µF.

3.1.4. Voltage regulator

To obtain the regulated +12V and +5V, positive voltage regulators 7812 and 7805 were used in the design. However, 7815 was used to turn on the relay as shown in Figure 2.

3.1.5. Transistor/relay switching and operation

Whenever the designed system is powered on, voltage flows from the mains supply into it. The rectified voltage in the secondary winding is regulated to 15Vac by the 15V fixed voltage regulator. This regulated voltage is fed through the base of the transistor to turn 'ON' the relay. The relay is introduced into the power pack basically to interface between battery and mains supply such that if mains supply fails, the battery powers the system until power is restored.

3.2. Microcontroller unit

The PIC18F2520 is an Enhanced Flash microcontroller with 10-bit A/D and nanowatt technology. The PIC18F2520 family introduces design enhancement that make these microcontrollers a logical choice for many high-performance and power sensitive applications. The PIC18F2520 device includes an internal oscillator block which generates two different clock signals; either can be used as the microcontroller's clock source. The PIC18F2520 is the microcontroller used in this work. Its pin configuration is shown in Figure 3

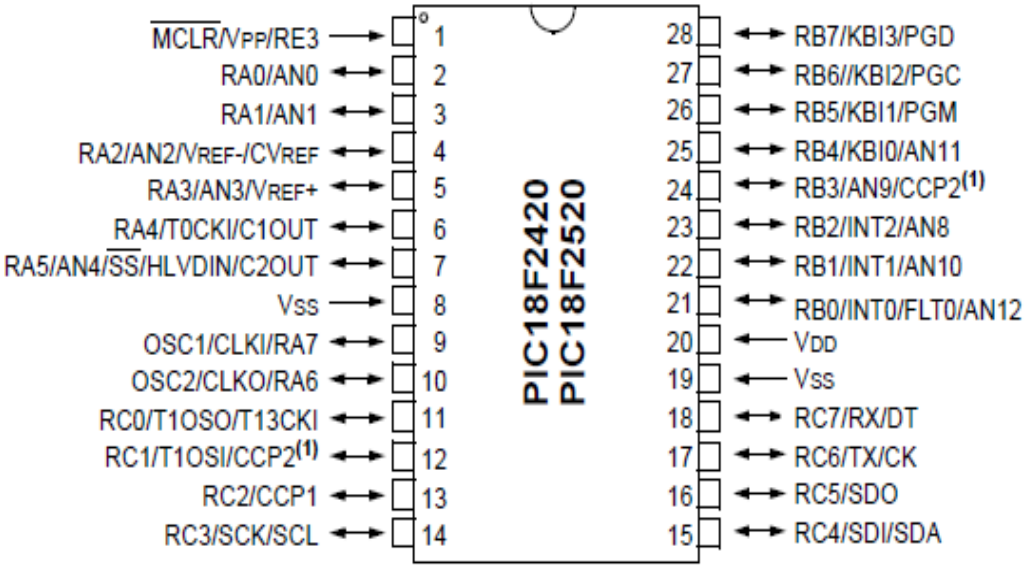

Figure 3. Pin configuration of PIC18F2520

The PIC18F2520 Port B (Pins 21 to 26) is connected to LCD, used basically for the display of the various activities occurring at intervals to give visual information of the observed process, while pin 27 is used as a digital input to the microcontroller to track motion of the intruder. The information received through this digital input is sent via the motion sensor. Pin 28 of Port B, is used as a digital output pin. At this pin an actuator, LED, is connected to indicate the presence of smoke when detected. Pins 2, 3 and 4 of Port A, are analogue inputs through which the Smoke sensor, Temperature sensor and Gas sensor communicate to the microcontroller. Pins 9 and10 of Port A, are used for external crystal oscillator respectively

Port C was also used in this project. Port C, pin 11, 12, 13, 14, 15 and 17 were used respectively. Pins 11 and 12 are used as input pins for buttons. These buttons are used to set the system time for proper time recording during pipeline monitoring. Pin 13 is used as an output pin wherein an actuator, LED, is attached to give a visual indication of the presence of intruder when detected. Pin 14 is used as an output pin

and a transistor is directly coupled to it, which is meant to switch a buzzer alarm, thereby creating an audio alert notification of the presence of abnormal situation. Pin 15 is used as an output pin as well, coupled to it is an actuator of type LED. The LED is called system state monitor. This LED blinks every 10 seconds indicating that the smart pipe monitoring system is active. Pin 17 is also used as an output pin. An active HIGH LED is attached to it. The LED is ON when the gas level is normal but goes off as soon smoke is detected. It is through those pins that data enters the microcontroller. In order to allow for internal program execution without resetting itself frequently, MCLR pin is connected to Vcc (+5v) through a pull up resistor of value 10kn. If the device is to be allowed to fetch code from external program memory locations starting at 0000H up to FFFFH, the power pins of the controller must be connected to VCC (pin 20) and ground GND(pin 8 and 19) respectively.

Pin 10 (CLK2) is an output from the inverting oscillator amplifier which is connected through a 22pf capacitor to ground as recommended. Pin 9 (CLK1) is an input to the inverting oscillator amplifier which is connected through a 22pf capacitor to ground as recommend.

The connection of pin 9 and 10 helps to determine the frequency of operation of the microcontrollers.

Port 1 (Pin 9) is used as reset switching

To determine reset time

One machine cycle is the time taken to execute an instruction

Machine cycle = 12 pulses of crystal oscillator.

Hence, $time\ taken = \frac{Oscillator\ Frequency}{12}$ (1)

For one machine cycle

$= \frac{16\text{MHZ}}{12}$

=1.333μs

Recall that it takes two machine cycles to reset. Hence, time to execute reset instruction.

= 2 x time of one machine cycle

= 2 x 1.333μs = 2.666μs

Reset time = 2.666μs

3.3. Software design/Implementation

The software consists of the program or set of instructions upon which microcontroller runs; thus the software program determines the operation of the system in general. The first step in the development of the program code was generating of the program algorithm. Thereafter an effective source code was developed and transferred to the microcontroller to enable it receive analogue input from the sensor, process the received input signal and send output to the actuators which display the system's status on the LEDs and 'Turn' Buzzers accordingly. Embedded "C++" programming language was used in this work. The written codes enable communication between the microcontroller, sensors, LEDs and Buzzers.

3.4. System flow chart

Figure 4 is the program flowchart used for this work.

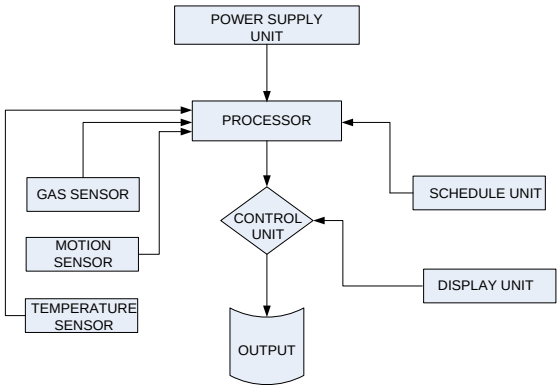

Figure 4. The flow chart of the pipeline security system

From the diagram above, the security and surveillance system, the various units and their functions are explained thus:

- Proximity Sensor: A proximity sensor is a sensor that is able to detect the presence of nearby objects without any physical contact. A proximity sensor often emits an electromagnetic field or a beam of electromagnetic radiation (infrared, for instance), and looks for changes in the field or return signal. The object being sensed is often referred to as the proximity sensor's target
- Gas Sensor: The gas sensor senses gas or smoke, typically as an indicator of pipeline leakage or fire.
- Temperature Sensor: The temperature sensor detects and measures hotness and coldness and converts it into an electrical signal.
- Processor: The processor receives multiple queries from the various sensors, processes these data and sends them to the control unit for further action.
- Control Unit: Based on the processed data the control unit makes the final decision which becomes evident in the output line.
- Schedule Unit: The schedule unit is responsible for scheduling of processes in such a way that each sensor's value gets read and the read data get sent and displayed accordingly. As such all three sensors work together without conflict, while the processor processes all the al the data from all sensor as though it is processing data from a single sensor.
- Output: The output unit receives instructions from the control unit to drive the output devices -the actuators like buzzer, LCDs and LEDs intended to be driven.
- Display Unit: This unit is responsible for displaying relevant actions and keeping track of records.

3.5. Principle of operation

Figure 5 is showing when the integrated pipeline security system is powered on, an initialization process is established. This process makes a welcome remark and designation and displays same on the LCD screen. After this, it immediately creates a secure connection with the sensors attached to the processor. If the communication/connection is successful, there is a handshake between the processor and all the peripheral devices connected; this handshake is also broadcast through the buzzer and LCD screen. Due to the fact that each of the attached sensor has a transient starting time, which present itself as start-up noise, the processor unit create a 60 seconds stabilizing window for all the sensors. During this stabilization window, the control unit is oblivious of any signal received. After the stabilization window, the system enters into an active state, at which point the integrated pipeline security responds to any increase in temperature beyond the preset threshold of 40^{o}C, intruder alert, and presence of gas/smoke above the reference value. There is a white blinker LED that blinks every ten seconds indicating that the system and together with the components as designed is perfect and in normal working condition. A green light indicates acceptable gas level in the environment the system monitors, while red LED indicates the presence of gas/smoke above the preset threshold value.

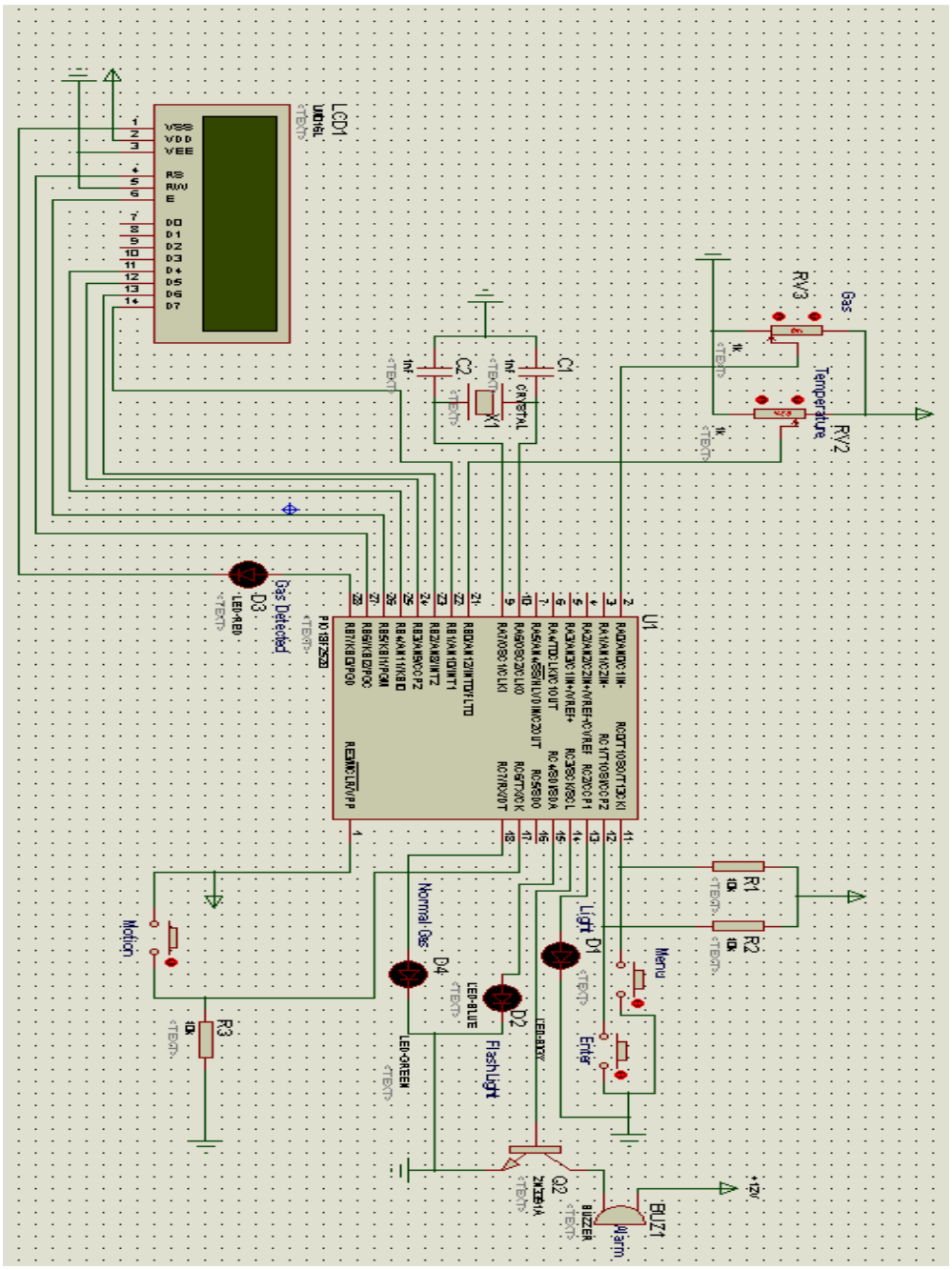

Figure 5. The complete circuit diagram of the system

4. TEST AND RESULT

The system consists of a software portion and a hardware portion. The software portion was first realized using mikroC PRO for PIC™ to develop the code for the project in embedded "C++" programming language. The circuit was then designed in Proteus 8 Professional™ and the software was loaded into the circuit, then extensive simulation and testing were carried out to ensure the system performs without errors and at maximum efficiency. After simulating the system and modifying it as necessary, construction of the hardware portion commenced. The overall circuit was broken into units and each unit was first tested on a breadboard before they were transferred to a Vero board and electrically linked by soldering after this, several tests were carried out on the device to confirm the level of its performance and efficiency. Thereafter, it was confirmed that the system was functioning well and in line with overall design aim and objectives as shown in Figure 6 and Figure 7.

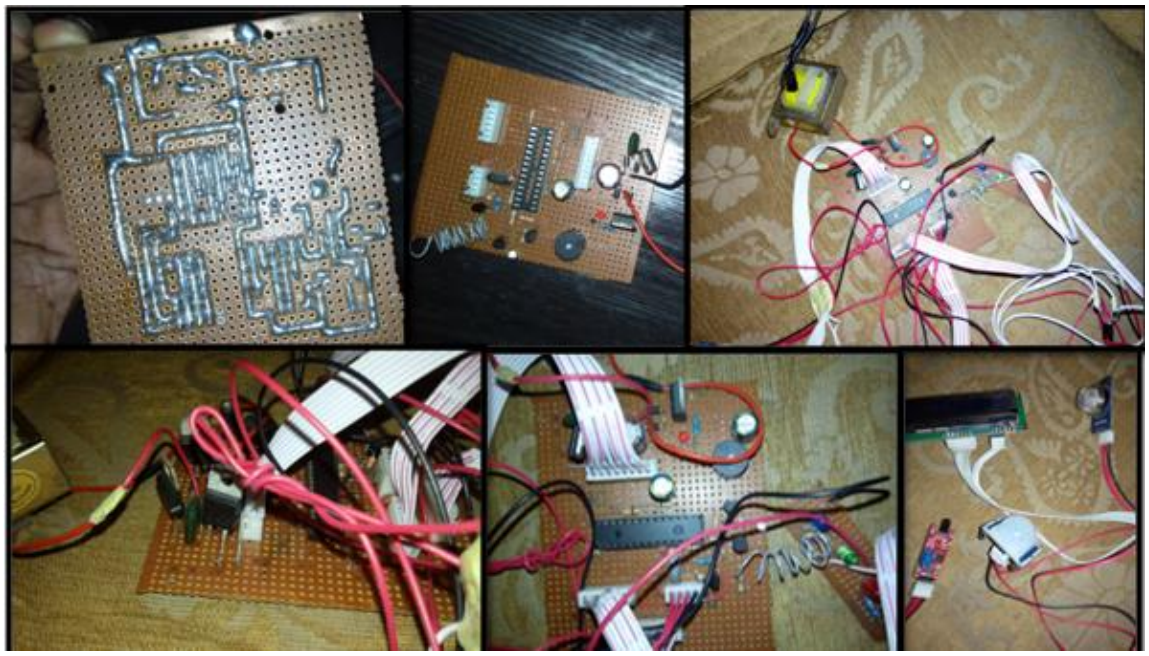

Figure 6. The various components/units soldered on vero board after extensive testing and electrically linked

Figure 7. Pictorial view of the various display units

5. CONCLUSION

The design and implementation of an integrated pipeline security system with optimized scheduling, a security and surveillance system in oil production platform to be deployed to secure and survey oil platform, has been actualized. It can also be deployed to secure homes, business places, and schools. Unlike other designs which are restricted only to the detection of intruders, our design in addition to detecting intrusion also addresses the safety of the people and property within the facility where it is deployed. It ensures safety from incidences of inferno resulting from excessive temperature, gas leaks or outright gas attack by notifying personnel appropriately utilizing the temperature sensor, and the gas sensor respectively. The various sensors- Motion, Gas and Temperature sensors work together to make the device an effective one. The sensors are active LOW sensors, meaning that when not triggered, they output a HIGH signal on their signal line but when triggered i.e when variables of interest within the environment of operation are detected, they send a LOW signal and the control unit reacts appropriately. The device is automated, thus can function without human intervention.

REFERENCES

[1] Security Focus, "ABUSTVIP1550/21550 Multiplevulnerabilitie," [Online]. Available: http://www.securityfocus.com/archive/1/520045, 2011.

[2] Okpeki, U. K, "Design and Construction of A Smart Security System," *Journal of Sustainable Technology*, vol. 9, no. 1, pp. 25-36, 2018.

[3] Okpeki, U. K, and O. O, Afieroho, "A Comparative Analysis of Electronics Security System," *International Journal of Engineering*, vol. 7, no. 1, pp17-21, 2013.

[4] Norharyati binti Harum, Mohanad Faeq Ali, Nurul Azma Zakaria, Syahrulnaziah Anawa, "Smart Surveillance System using Background Subtraction Technique in IoT Application," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 12, pp.122-128, 2018.

[5] Mohd Azlan Abu, Siti Fatimah Nordin, Mohd Zubir Suboh, Mohd Syazwan Md Yid, Aizat Faiz Ramli, "Design and Development of Home Security Systems based on Internet of Things Via Favoriot Platform," *International Journal of Applied Engineering Research*, vol 13, no. 2 pp. 1253-1260, 2018.

[6] S. Nico, and R.W Wingky, "Design of Smart Home Security System using Object Recognition and PIR Sensor," *Procedia Computer Science*, vol. 135, pp. 465-472, 2018

[7] A, Anitha, "Home security system using internet of things," *IOP Conf. Series: Materials Science and Engineering*, no. 263, pp.1-11, 2017.

[8] Sharnil Pandya, Hemant Ghayvat, Ketan Kotecha, Mohammed Awais, Saeed Akbarzadeh, Prosanta Gope, Subhas Chandra Mukhopadhyay, Wei Chen, "Smart Home Anti-Theft System: A Novel Approach for Near Real-Time Monitoring and Smart Home Security for Wellness Protocol," *Applied System Innovation*, vol. 1, no. 42, pp. 1-22, 2018

[9] Bugged Planet – Surveillance Industry and Country's Actings, [Online]. Available: http://buggedplanet.info/.

[10] Oakland Domain Awareness Center (DAC), [Online]. Available: http://oaklandwiki.org/Domain_Awareness_Center.

[11] A. Kidman, "How A Prison Had Its CCTV Hacked," [Online]. Available: http://goo.gl/sKombD, September 2012.

[12] J. Aron, "Want to rob a bank? Hack your way in," *New Scientist*, vol. 220, no. 2937, pp. 1-22, 2013.

[13] Digital Munition, "Owning a Police Car and its DVR," [Online]. Available: http://www.digitalmunition.com/OwningCopCar.pdf.

[14] U. Saeed, S. Syed, S. Z. Qazi, N. Khan, A. Khan and M. Babar, "Multi-advantage and Security Based Home Automation System," *2010 Fourth UKSim European Symposium on Computer Modeling and Simulation*, Pisa, pp. 7-11, 2010.

[15] A. Alheraish, "Design and implementation of home automation system," in *IEEE Transactions on Consumer Electronics*, vol. 50, no. 4, pp. 1087-1092, Nov 2004.

[16] A. R Delgado, Rich Picking, Vic Grout, "Remote-Controlled home automation systems with Different Network Technologies," *Glyndwr University Research Online*, 2006.

[17] M. Danaher, D. Nguyen, "Mobile Home Security with GPRS," In *Proceedings of International Symposium on Information*, pp.377-380, 2002.

[18] W. Bing-Fei, Hsin-Yuan Peng, Chao-Jung Chen, "A Practical Home Security System via Mobile Phones," *Proceedings of the 5th WSEAS International conference on Telecommunications and informatics*, Spain, pp. 299-304, 2006.

[19] S. R. Das, S. Chita, N. Peterson, B. A. Shirazi and M. Bhadkamkar, "Home automation and security for mobile devices," *2011 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, Seattle, WA, pp. 141-146, 2011.

[20] Joseph Steinberg, "Massive Internet Security Vulnerability- Here's What You Need To Do," *BBC News*, 2014