Development Of a Smart Surveillance System for Vandals' Detection and Tracking on Petroleum Pipelines

AGOHA STEPHEN CHUKWUMA[1], F. K. OPARA[2], O. C. NOSIRI[3], A. O. AKANDE[4], G. INNY-MFON JOSHUA[5], C.K. OGUZIE[6]
[1,2,5]Department of Electronic Engineering, School of Electrical System Engineering and Technology, Federal University of Technology Owerri (FUTO) Owerri, Nigeria
[3,4]Department of Communications Engineering, School of Electrical System Engineering and Technology, Federal University of Technology Owerri (FUTO) Owerri, Nigeria
[6]Department of Polymer Engineering, School of Engineering and Engineering and Technology, Federal University of Technology Owerri (FUTO) Owerri, Nigeria

Abstract- Crude oil production is extremely important in the global economy. Effective management and control of that product is extremely important. The indecent acts of vandalism are increasing, notable the southern part of Nigeria, with thousands of barrels of crude oil lost due to these vandals when transporting its products. This paper presents an intelligent surveillance pipeline with the ability to recognize real-time intrusions to monitor and attract attention for emergency responses. The Method used consists of a motion detection system, ultrasonic and vibration sensors, warning systems, and a web application control panel. The development was simulated using Proteus software and programmed with MPLAB-IDE. The design consists of an Arduino UNO Atmega Microcontroller as the main controller, a PIR sensor camera for image detection and snap snapping, and a PIR sensor camera, an RFID reader/card for authentication, and also integrated with an IoT system which also is connected to the internet allowing it send and record images with the Network Video Recorder (NVR), a buzzer as an alarm and a web application control panel that could be accessed over the Wi-Fi to manage the system. The system test worked as expected using a variety of scenarios, including user authentication, intruders, or false authentication. The surveillance camera also operates at night and automatically switches to the infrared sensor. Focused on the body near the sensory device, blurring the background to recognize facial features. This enhances the overall security by providing a comprehensive view of the perimeter and enabling rapid detection of intrusions.

Index Terms- RFID, NVR, MPLAB IDE, ESP32, PIR, CCTV, IoT, HDI

I. INTRODUCTION

Pipelines are an essential part of any nation's infrastructure and are important for the transportation and distribution of liquid energy resources, such as petrol, natural gas, and other combustible products (Nicola, 2022). Pipeline is a long underground pipe, basically for transporting oil, gas, etc. over a long distance (Oxford Dictionary, 2020).

Just as operating system problems can usually lead to unimaginable disasters, pipeline systems, which are usually the main medium for transporting various liquids, especially crude oil, are the main medium for crude oil. Such operational system problems may include terrorist attacks, vandalism, and theft on the pipeline. (Obodoeze, et. al. 2014).

Meanwhile, Vandalization is a predominant problem across Nigeria, including the Niger Delta. Vandalization refers to illegal or unauthorized activities that destroy oil, and gas pipelines. Negative activity aimed at maintaining products for personal use or sale in the black market, especially in developing countries (Obodoeze et al., 2014).

The length and location across remote areas through which pipelines cross make it a potential target; therefore, need for security from vandalization caused either by natural hazards, accidents, or unwanted interference from vandals. These incidents can have various impacts on public safety, the economy, and the environment.

There are multiple reasons a person would commit an act of vandalism toward a petroleum pipeline, such as; it can be an act of revenge, poverty, unemployment, sabotage, or an act of theft that absorbs oil for personal benefit. This vandalism toward the petroleum pipeline has led to a significant loss, thereby disturbing the operation of providing oil and gas to the consumer (Obodoeze, et. al. 2014).

Vandalism will increase and remain if the government or the International Oil Companies (IOCs) take no thorough measure in the country. Many security and technical measures have been used to stop vandalism in oil pipelines and to identify leaks and breakdowns in oil pipelines, but none of these techniques or measures has met the desired outcome due to obvious factors such as corruption and incompetency. (Obodoeze, et. al. 2014).

The need to implement surveillance for pipeline was addressed in previous related works. Some of these methods have documented success relating to the objectives, while others have made insignificant contributions to this challenge of the country. (Obodoeze, et. al. 2014).

Therefore, a monitoring and tracking system is needed to prevent acts of vandalism against the petroleum pipeline, as the traditional method of surveillance is not effective and has high operational costs.

According to Obodoeze, et al (2014), pipeline infrastructure must be continuously monitored to ensure the safety and integrity of crude product being transported. Therefore, it uses underground and surface technologies such as downholes, distributed temperature systems, and permanent systems for pressure and temperature sensor monitoring.

Video surveillance systems in various fields of our society are expedient, from homes, institutions, and industries, providing safety in many ways. Looking at the different surveillance systems over time, there's always improvements, efficient, convenient, and safe ways for people to secure their space and properties. Smart surveillance systems have proven to be a valuable tool for pipeline risk assessment as it has the potential to enhance real-time monitoring providing emergency response.

The purpose of monitoring the pipeline is to monitor the use of road rights and to recognize interventions that can affect the interests and safety of nearby people using intelligent devices. By using intelligent devices, this system offers significant improvements to existing surveillance systems.

The system can interpret any input of the surveillance image and can free operators from the need to stare at monitor screens while on surveillance duty, thus freeing the operator therefore only being alerted when abnormal behavior is interpreted.

Pipeline Surveillance is a design that quickly detects penetration with the system before the vandalism occurs, alerting the pipeline operator, and allows the vandalism scene photo/video film material to be captured if the vandal destroys the pipeline. This helps reduce pipeline products theft, environmental degradation and death. This is because it is often caused by the explosion of these withdrawal materials when they occur.

II. LITERATURE REVIEW

Pipeline Vandalization and The Challenges in Nigeria

Crude is Nigeria's most important natural resources thereby making transporting of oil and gas via pipeline and an important part of the energy transportation infrastructure for the economy. This is an essential tool for communicating all kinds of liquid products, extending over thousands of kilometres and passing through towns, villages, across the country. (Punch Newspaper, 2021).

These pipelines operate at high pressures and fault along the system is a major danger to environmental, ecological disasters, human health, properties, and disruptions in gas or oil supply. Pipelines are affected by corrosion, cracks, penetration of third-party providers, and loss of functionality due to manufacturing errors. Mechanical damage to third-party providers becomes most serious problem that the pipeline industry has had at facilities (Ezeh et al., 2014). The huge oil installations built in the Niger Delta region explain their susceptibility to vandalism. At the moment, the installations in Niger Delta region, has over 600 oil fields, of which 360 fields are on land, with over 3,000 kilometres of pipelines away from the coast connecting region and various export connections and 275 river station links. It is pertinent to note that oil spills resulting from pipeline vandalism have continued to be a challenge, with most incidents along these major pipelines (Bakpo & Agu 2009).

Shell Oil Developers, one of the most important oil operators in Nigeria recorded a total of 2944 oil spill incidents. The data show a noticeable increase from that 235 cases in 1995 have increased significantly to 330 in 2000. The least number of 224 oil spill incidents was observed in 2005.

Table 2.1 shows the volume of spilled incident from 1995 to 2005. (Essien, 2018)

Year	Number Of Spills	Volume In Barrels(bbl)
1995	235	31,000
1996	326	39,000
1997	240	80,000
1998	248	50,000
1999	320	20,000
2000	330	30,100
2001	302	76,960
2002	262	19,980
2003	221	9,916
2004	236	8,317
2005	224	11,921

Also, it was reported that about 250,000 barrels of crude oil are 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. (Yo-Essien, 2018).

Table 2.2: Shows the volume of Crude oil lost due to illegal bunkering.

2014		
Month	Security Deferment (bbls)	Loss Due to Oil Theft (bbls)
Jan.	4,679,301	2,172,341
Feb.	4,153,114	1,679,874
Mar.	9,534,642	1,253,825
TOTAL	18,367,057	5,106,040

The table shows that over 5 million barrels of crude oil total has been lost due to illegal bunkering from pipeline vandalism. The latest STEM explosion in Lagos was the result of pipeline vandalism. The recent jetty explosion in Lagos was a result of pipeline vandalism (Yo-Essien, 2014). The Nigeria National Petroleum Corporation (NNPC) said the incident occurred after the truck crashed into a stacked gas bottle in a gas processing system near the Corporate System 2B pipeline before it fought.

Preliminary findings showed the immense impact of the explosion, leading to the collapse of nearby homes and damaged several NNPC pipelines. Additionally, Nigeria National Petroleum Corporation (NNPC) found that Nigeria lost approximately N163 billion to vandalism in three years. (Ezeh et al., 2014; This Day, 2014; NNPC, 2014).

Pipeline vandalism crippled fuel supply and created product losses and repairs of over N174 billion in pipeline. (NNPC, 2014). Many lives were lost to explosions and fires that result from destroyed pipelines with crude oil and refined products when destroyed. The environment has also deteriorated, and many of the arable land has been completely destroyed.

III. MATERIALS AND METHODOLOGY

3.1 Materials

The materials used are listed and discussed for the enablement of full understanding of the materials, their types and complexities.

The following are the devices deployed:

Hardware Component

i. Power Supply Unit (which consist of Voltage Regulator 78L05, IN4007 diodes, BC547 transistor and 12v transformer, capacitors and resistors)
ii. Battery
iii. RFID Reader
iv. Arduino Uno R3
v. An ESP32
vi. PIR sensor Camera
vii. Ultrasonic sensors V2.0B
viii. Vibration Sensor SW-420
ix. A Network Video Recorder
x. SIM900D green
xi. Sounder
xii. 4G Modem (Internet Connectivity)

Software Package

i. MPLAB IDE.
ii. Proteus Design Suite

3.2 METHOD

Following the research design which is the experimental design on how each material works together to make the smart surveillance work effectively, quantitative analysis was adopted to achieve the aim of the work.

The design details the structured process of conceptualizing, planning, and specifying the architecture, components, and functionalities required to create an effective security solution for protecting designated perimeters of the pipeline.

This phase bridges the gap between system requirements and actual implementation, focusing on designing a robust and scalable system that meets operational needs while ensuring accuracy and responsiveness in detecting and mitigating security threats.

Figure 3.1 describes how the whole experimental design interconnects.

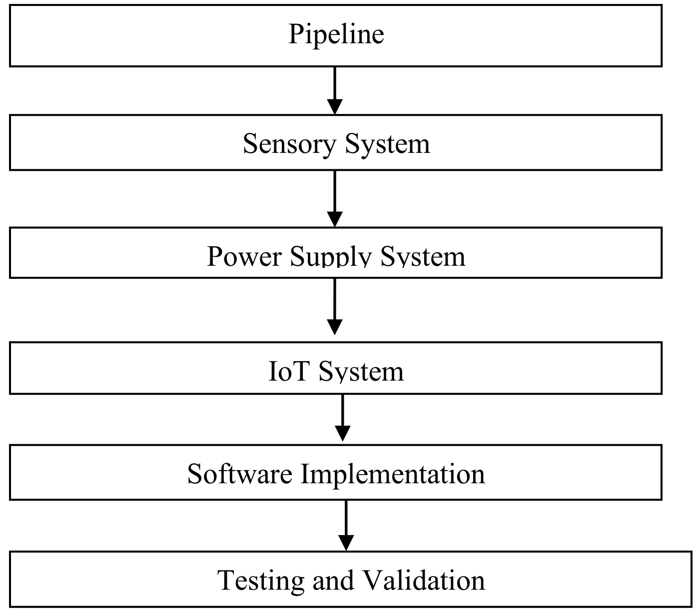


Figure 3.1 Block diagram for the structured process design

3.2.1 Development of a Smart Surveillance System

The design is considered to sense the presence of intruder and abnormalities within and around the pipeline for vandalization.

The system consists of hardware and software design.

Hardware: This consist of the hardware design carried out to understand the bodily test-bed for the system.

Software: This consist of the software program used to program the sensor initializations communication, and transfers information from the deployed test bed to an online server, to the exact email addresses and mobile numbers of the authorities at the control room so the operator can view videos/photos footage captured from a vandalization scene.

The diagram in both Figure 3.2 and Plate 3.1 shows the interconnections between different components that constitute the circuit.

This focuses on developing a smart surveillance system that detects and tracks motion within the system as well as responds to it immediately by capturing and identifying the image and administering the outcome to the device administrator through email. The system can be monitored from anyplace by the authorized user.

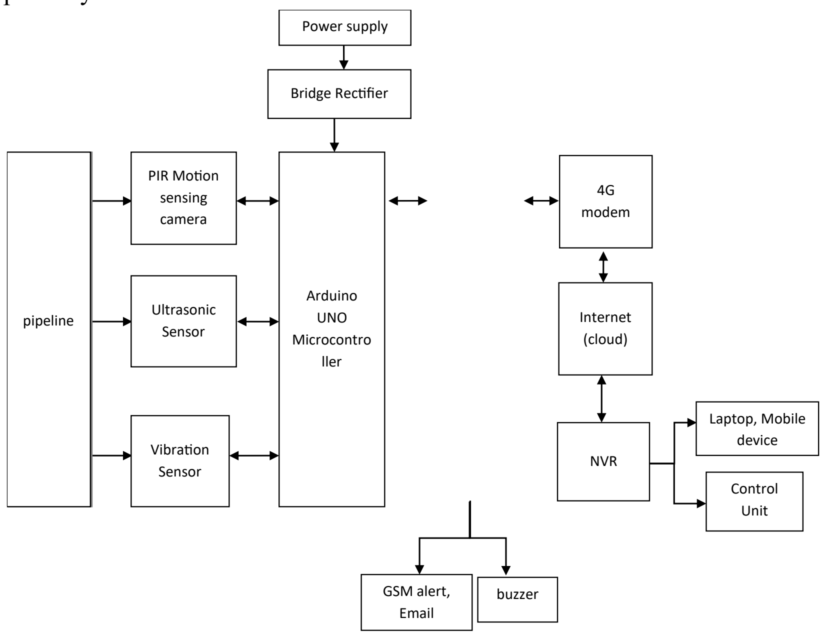


Figure. 3.2 A block diagram of the Hardware Design System.

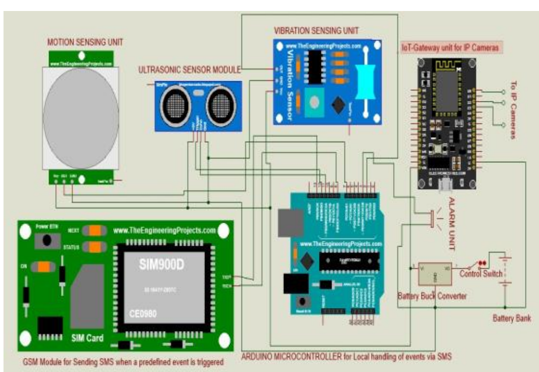


Plate: 3.1: 2D Circuit Diagram of Smart Surveillance Security System for pipeline

Power Supply Unit System

This unit is built using components which includes: rectifiers, filters, voltage regulators, renewable energy, etc. The system requires a reliable power source to operate. This can include backup power options like batteries, renewable energy, or generators, as the case may be.

Voltage regulators

In other to ensure efficiency in power supply, voltage regulators ensure the voltage flowing through a unit doesn't exceed between two ranges of voltage regulators – 5V and 12V.

Load Analysis

Before any electrical/electronic project is carried out following the standard method, the system's load analysis must be considered. Each component has specific quantity of power required to drive it.

Should it get less of it, the component will act abnormally. The components used in this project were carefully chosen based on their voltage and current requirements. Below is the table showing the load analysis.

Table 3.1 Shows the Components, Current, and Voltage they Require to Operate Effectively.

Component	Voltage	Current	Quantity	Total Power
Arduino Nano	5v	20mA	1	0.1W
GSM Module	5v	500mA	1	2.5W
RFID Reader	5v	26mA	1	0.13W
Ultrasonic Sensor	5v	15mA	2	0.15W
Vibration Sensor	5V	10mA	4	0.2W
Buzzer	3.3v	10mA	1	0.033 W
Red LED	2.2v	5mA	1	0.011 W
ESP 32	5v	20mA	1	0.2W
Relay	5v	50mA	1	0.25W
TOTAL POWER				5.724 W

```
Algorithm 1
// Initialize the variable
Variable X = Vibration sensor.
Variable Y = Ultrasonic sensor.
Variable Z = Camara sensor (PIR).

Alarm
{
// Declare the input and output
X = true positive
}
Dis-alarm {
X = true negative
}
{
//Create interrupts
X = False positive
}
Dis-alarm {
X = False negative
}
Interrupt – Alarm {
//Call Alarm module
Is X true positive or true negative
}
Trigger system {set pin = High
}

Interrupt disarm {
Is X False positive or False negative
Call disalarm module
}

Set the threshold voltage
//Get sensor proportional to distance of nearest intruder, such that
If value >=21
ALARM-SYSTEM
If value <=20
DISALARM-SYSTEM

Read sensor {
Compare Source 1 input (Variable Y) to the threshold voltage
If source 1 is greater than the threshold voltage
Send alarm 'source 1 is active'
Else, go to source 2

Read source 2 input (Variable Y)
Compare source 2 input (Variable Y) to the threshold voltage
If source 2 is greater than the threshold voltage
Send alarm 'source 2 is active'
Else, go to source 3

Read source 3 input Variable Z
If source 3 is greater than the threshold voltage
Send alarm 'source 3 is active'

Else, repeat the loop.
```

The algorithm flowchart design followed a series of processes to accomplish its holistic design and functionality.

Algorithm 2

1. Start
2. Initialize System
3. Data Acquisition
4. Preprocess Video Data
5. Intruder Detection
6. Activity Recognition

7. Anomaly Detection
8. Tracking
9. Alert System
10. Logging & Analysis
11. System Feedback
12. System Maintenance and calibration
13. End

Figure 3.2 shows the flow process interconnections between different subsystems that constitute the entire functionality of the surveillance system.

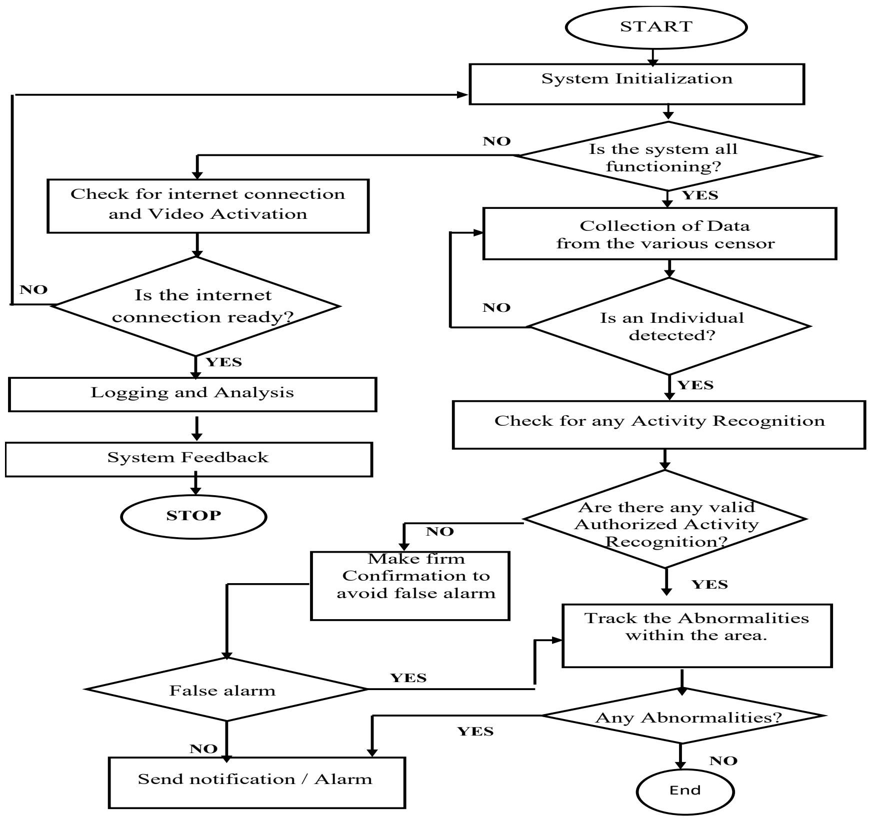


Figure 3.2: Control Flowchart for The Entire Surveillance system

3.2.4 Software Implementation Program Design

This is achieved by the use of an MPLAB-written software program script to accomplish a real-time surveillance system as designed in this research.

Program Code: A program was written in C++ language to control the microcontroller; it was written using the MPLAB IDE. The MPLAB IDE is a Windows IDE (Integrated Development Environment), it has an editor window for writing code, tools to aid debugging, a programmer interface, etc. After the codes are written, they are compiled to generate a hex file which is then programmed (burned) into the microcontroller using a PICKIT2 programmer.

PROGRAMMING

The code used in programming the Arduino microcontroller to send out a warning email in proximity to the exposed cameras when the different sensor sends a signal of logic 1 to the circuit is given below.

```
#include <SoftwareSerial.h>

const int vibrationPin = A0;  // Analog input pin for vibration sensor
const int ultrasonicPin = A1;  // Analog input pin for ultrasonic sensor
const int vibrationsirenPin = A3;       // Digital output pin for vibration siren/alarm
const int ultrasonicsirenPin = A4;       // Digital output pin for ultrasonic siren/alarm
```

```
void setup() {
  pinMode(vibrationPin, INPUT);
  pinMode(ultasonicPin, INPUT);
  pinMode(vibrationsirenPin, OUTPUT);
  pinMode(ultrasonicsirenPin, OUTPUT);
  Serial.begin(9600);
}

void loop() {
  int vibrationValue = analogRead(vibrationPin);
  int ultrasonicValue = analogRead(ultrasonicPin);
  if (vibrationValue > threshold || ultasonicValue ==
HIGH) {

 // Trigger siren/alarm
    digitalWrite(sirenPin, HIGH); //send an SMS
    // Send alert via IoT module
    Serial.println("Vandal detected!");
    Serial.println("AT+CMGF=1"); // Set SMS mode
    delay(100);
    Serial.println("AT+CMGS=\"+1234567890\"");
// Replace with phone number
   delay(100);
    Serial.println("Vandal detected");
    delay(100);
}
  delay(1000); // Wait for a second before next read
}

#include <WiFi.h>
#include "esp_camera.h"

// Wi-Fi Credentials
const char* ssid = "YOUR_SSID";
const char* password = "YOUR_PASSWORD";

// PIR Sensor
#define PIR_PIN 23 // Adjust as needed

// Camera Configuration (Adjust according to your
setup)
#define CAMERA_MODEL_AI_THINKER
#include "camera_pins.h"  // Include the camera pin
definitions

  void setup() {
  Serial.begin(115200);
  // Initialize PIR sensor
  pinMode(PIR_PIN, INPUT);

   // Initialize Wi-Fi
  WiFi.begin(ssid, password);
  Serial.print("Connecting to WiFi");

  while (WiFi.status() != WL_CONNECTED) {
    delay(100);
    Serial.print(".");
  }

  Serial.println("Connected to WiFi");
    // Initialize camera
  camera_config_t config;
  config.ledc_channel = LEDC_CHANNEL;
  config.ledc_timer = LEDC_TIMER;
  config.pin_ssr = SS_PIN;
  config.pin_pwdn = PWDN_PIN;
  config.pin_reset = RESET_PIN;
  config.pin_xclk = XCLK_PIN;
  config.pin_sccb_sda = SIOD_PIN;
  config.pin_sccb_scl = SIOC_PIN;
  config.pin_d7 = D7_PIN;
  config.pin_d6 = D6_PIN;
  config.pin_d5 = D5_PIN;
  config.pin_d4 = D4_PIN;
  config.pin_d3 = D3_PIN;
  config.pin_d2 = D2_PIN;
  config.pin_d1 = D1_PIN;
  config.pin_d = D_PIN;
  config.pin_vsync = VSYNC_PIN;
  config.pin_href = HREF_PIN;
  config.pin_pclk = PCLK_PIN;
  config.xclk_freq_hz = 20000000;
  config.pixel_format = PIXFORMAT_JPEG;
  config.frame_size = FRAMESIZE_VGA;
  config.jpeg_quality = 12;
  config.fb_count = 2;

  // Initialize the camera
  if (esp_camera_init(&config) != ESP_OK) {
    Serial.println("Camera init failed");
    return;
  }
}

void loop() {
  if (digitalRead(PIR_PIN) == HIGH) {
    Serial.println("Motion detected!");

    // Capture image
```

```
  camera_fb_t *fb = esp_camera_fb_get();
  if (!fb) {
   Serial.println("Camera capture failed");
   return;
  }
// Send image to server
  WiFiClient client;
  if (client.connect("YOUR_SERVER_IP", 80)) {
   client.println("POST /upload_image HTTP/1.1");
   client.println("Host: YOUR_SERVER_IP");
   client.println("Content-Type: image/jpeg");
   client.print("Content-Length: ");
   client.println(fb->len);
   client.println();
   client.write(fb->buf, fb->len);
   Serial.println("Image sent to server");
  } else {
   Serial.println("Failed to connect to server");
  }

  // Return the frame buffer back to the driver
  esp_camera_fb_return(fb);
  // Delay for 10 seconds to avoid multiple triggers
  delay(10000);
 }
 delay(500);  // Short delay for loop
}
    // Trigger camera (optional)
  digitalWrite(cameraPin, HIGH);
  delay(1000);
  digitalWrite(cameraPin, LOW);
 }
else {
  digitalWrite(sirenPin, LOW);
 }
 delay(100);
}

#include <ESP32 MailClient.h>
#include <WiFi.h>
#include <Ultrasonic.h>

#define TRIGGER_PIN_1_14
#define ECHO_PIN_1_15
#define TRIGGER_PIN_2_16
#define ECHO_PIN_2_17
#define TRIGGER_PIN_3_18
#define ECHO_PIN_3_19

Ultrasonic ultrasonic1(TRIGGER_PIN_1, ECHO_PIN_1);
Ultrasonic ultrasonic2(TRIGGER_PIN_2, ECHO_PIN_2);
Ultrasonic ultrasonic3 (TRIGGER_PIN_3, ECHO_PIN_3);

const char* ssid = "your-ssid";
const char* password = "your-password";
const char* to = "recipient@example.com";
const char* from = "sender@example.com";
const char* smtpServer = "smtp.example.com";
const char* smtpUser = "username";
const char* smtpPassword "password":

void setup() {
Serial.begin(115200);
WiFi.begin(ssid, password);
while (WiFi.status() != WL_CONNECTED) {
delay(1000);
Serial.println("Connecting to WIFI..");
}
Serial.println("Connected to the WiFi network );
}

void loop() {
// Measure the distance from each ultrasonic sensor
long distance1 = ultrasonic1.distanceCentimeters();
long distance2 = ultrasonic2.distanceCentimeters();
long distance3 = ultrasonic3.distanceCentimeters();

// Check if any of the distances are less than a certain threshold
if (distance1 < 10 || distance2 < 10 || distance3 < 10) {
Serial.println("Proximity to camera detected!");
// Send an email
MailClient.send(to, from, "Proximity to camera detected",
```

IV. RESULTS, CONCLUSION AND RECOMMENDATION

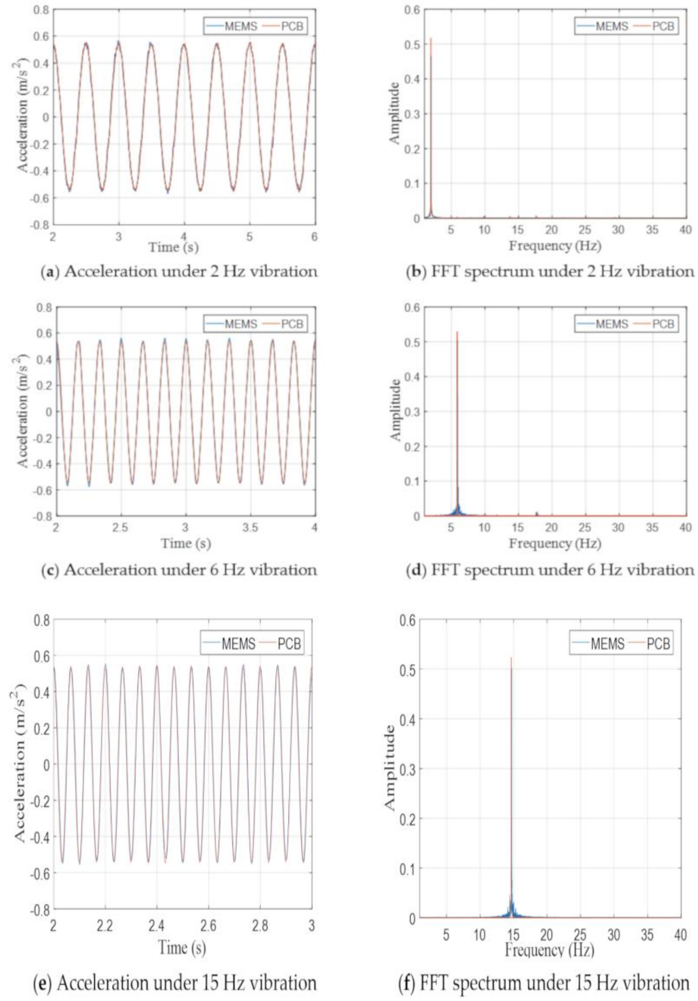
RESULTS

Tests for intrusion detection and video surveillance were conducted by connecting all the subsystems and providing a single power source to all of them and results were obtained. An obstacle was brought close to the pipeline, the camera tilted and focused its lens on it, grabbed the image of the object, and kept a real-time view of the object. When the obstacle continued and hit the pipeline with enough force to cause vibration, the alarm buzzed and the GSM module sent out a message indicating a breach in the pipeline system.

4.1.1 Camera (PIR sensor) and NVR Unit Test Result
The cameras reacted when motion was detected during odd hours. The cameras are able to function during both daytime and nighttime, giving optimal imagery in both conditions. When there aren't natural or other light sources the IR sensor comes on which enables clear imagery. The camera is able to detect motion and send a push notification which alerts the user or administrator on their device.

Table 4.1.1 A Table of Camera and NVR unit test.

S/N	Condition	Result
1	Natural light	Coloured imagery output
2	Night time (dark)	Black and white imagery output
3	Power supply	Cameras and NVR performs normally
4	No power supply	No system function
5	Internet connectivity	Push notifications available, live streaming, and local storage
6	No Internet connectivity	Only local video storage
7	Proximity to the camera in natural light	Images in the background are visible
8	Proximity to the camera in the dark	Images in the background are blurred out
9	Movement in priority areas	A push notification is sent



(a) Acceleration under 2 Hz vibration (b) FFT spectrum under 2 Hz vibration
(c) Acceleration under 6 Hz vibration (d) FFT spectrum under 6 Hz vibration
(e) Acceleration under 15 Hz vibration (f) FFT spectrum under 15 Hz vibration

Plate 4.1 Vibration Sensitivity

The table below shows the vibration sensor test result from the vibration sensitivity

Table 3.3 Vibration Sensor Test Result

4.1.3 Ultrasonic to the Arduino Test Result
The ultrasonic sensors reacted according to the obstacles detected. It was noticed that two sensors can't share the same trigger and echo pins connecting to the Arduino microcontroller. If the pins are shared the microcontroller only works with signals from the sensor and ignores the input from the second sensor, and as such the ESP32 is required.

Table 4.1.2. A Table of Ultrasonic to the Arduino

Vibration Tuning (°)	Amplitude (m)	Frequency (Hz)
0	0.0	00
90	0.51	2
180	0.53	6
270	0.52	15

unit test

S/N	Condition	Result
1	Close range to the sensor	The ultrasonic sensor can detect a sound wave
2	Far range to the sensor	The maximum sensing range for the ultrasonic sensor is 24 inches around the pipeline.
3	Internet connectivity present in the circuit	The Arduino microcontroller sends notification email to the admin
4	No internet connectivity present in the circuit	The sensor doesn't need the internet to send a signal to the Microcontroller.

4.1.4 Microcontroller Test Result

An Arduino and ESP32 microcontroller, which is a low-power microcontroller, was deployed to process proximity sensing within the system, and works according to the signals coming from the different subunits of the system. It was deployed over other models of microcontrollers because it is network-enabled, which helps it send alerts and Emails over the internet. The cameras enable live streaming with a stable internet source and local storage in the Network Video Recorder (NVR).

CONCLUSION

This work, design of smart surveillance system for vandals' detection and tracking on petroleum pipelines, a continuous field application of this technology prevents or minimize theft and crime rate in Niger Delta region and country at large by utilizing a smart phone to ease the tracking and monitoring process whereby the authorized user get access to the IP address and an internet service provider (ISP) for secure internet connectivity.

RECOMMENDATIONS

Security breaches can happen in any facility even with the most developed technology-enabled surveillance systems and for this reason, there’s lot of room for improvement. Furthermore, the progress of the design is successfully implemented using a prototype.

Recommendations made in this study are aimed to ensure easy access to already existing knowledge on how to design and install a smart surveillance system that runs effectively and perform optimally. The next step forward is to expand the design at scale across the general laboratory/field and to present this to other companies to adopt this surveillance approach in their departments.

Some more recommendations include: microcontrollers such as Raspberry Pi for a more robust operation of the surveillance cameras; alternative power sources such as Solar panel, inverters can be made provision for the surveillance systems to work independently.

Recommendation is also made to oil-producing companies such as the NNPC, SHELL, and other pipeline product transportation companies to adopt this approach as a precursive measure for securing assets, lives, and properties.

REFERENCE

[1] Adejimi, Sodiya, Ojesanmi, Falana, & Tinubu. (2023). A dynamic intrusion detection system for critical information infrastructure. Scientific African, Vol. 21.

[2] Akila, R., Merin, J. B., Radhika, A., & Behera, N. K. (2023). Human Activity Recognition Using Ensemble Neural Networks and The Analysis of Multi-Environment Sensor Data Within Smart Environments. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 14(3).

[3] Anjali Patil Ms, (2014). "AI-based Home Automation System using Raspberry Pi, Master

of Engineering student", Department of Computer Science and Technology, V.V.P.I.E.T. Solapur.

[4] Attar T., Chavan P., Patel V., Gupta M., and Mukhopadhyay D (2018). An Attempt to Develop an IoT-based Vehicle Security System; International Symposium on Smart Electronic Systems, IEEE, 2018.

[5] Bello, S. A. (2020), How to stop pipeline vandalism https://www.vanguardngr.com/2020/07/how-to-stop-pipeline-vandalism-fmr-nscdc/

[6] Benezeth Y., Jodoin P.M., Saligrama V., and Rosenberger C. (2009). Abnormal events detection based on spatio-temporal co-occurrences. In IEEE Conference on Computer Vision and Pattern Recognition, pages 2458–2465, 2009.

[7] Celeste Tholen, (2021). How Does a Motion Detector Work, ‖ Internet: https://www.safewise.com/home-security-faq/how-motion-detectors-work/June 10, 2021.

[8] Cermeño E., Pérez A., and Sigüenza J. A., (2018). "Intelligent video surveillance beyond robust background modeling," Expert Syst. Appl., vol. 91, pp. 138-149, 2018.

[9] Chandra S. P., Roopalakshmi R., Kaveri B. Kari, Pavan R., Kirthyand P., Spoorthi P. N., (2019). “IoT Based Framework for Automobile Theft Detection and Driver Identification,” Springer Nature Singapore Pte Ltd., 2019.

[10] Danny Jost. (2019) What is the ultrasonic sensor? [Online] [Accessed on the 16th of December 2022]

[11] Doe J., (2014). "A Perimeter Intrusion Detection System (PIDS) based on sensor networks," Applied Mechanics and Materials, vol. 568-570, pp. 468-472, June 2014,

[12] Ezeh G. N, Chukwuchekwa N., Ojiaku J. C. and Ekeanyawu E. (2014) "Pipeline Vandalisation Detection Alert with Sms", Int. Journal of Engineering Research and Applications Vol. 4, Issue 4 (Version 9), April 2014, pp.21

[13] Gaona-Garcia P, Montenegro-Marin CE, Prieto JD, Nieto YV. (2017). Analysis of security mechanisms based on clusters IoT environments. Int J Interact Multimed Artif Intell. 2017;4(3):55–60.

[14] Gatsis, K. and Pappas, G.J. (2017) Wireless Control for the IoT: Power Spectrum and Security Challenges. 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI), Pittsburgh, 18-21 April 2017, 341-342.

[15] Godwin O. O., and Kazeem I. R., (2021). Remotely – monitored anti-pipeline vandalization Detection Expert System. Department of Computer and Information Sciences, Tai Solarin University of Education Ijagun, Ogun State, Nigeria

[16] Ibrahim S. W., (2016). "A comprehensive review on intelligent surveillance systems", Commun. Sci. Technol., vol. 1, no. 1, pp. 7-14, May 2016.

[17] Ida Hübschmann (2020). ESP32 for IoT: A Complete Guide.

[18] Jeevanand D., Mohamed Rilwan, Murugan P. and Keerthivasan K. (2014). Real-Time Embedded Network Video Capture and SMS Altering System, International Journal of Communication and Computer Technologies, Issue:05, Volume 02-NO.11, ISSN NUMBER: 2278- 9723, June 2014.

[19] Jennifer Pattison Tuohy (2021). Types Of Security Cameras, Internet: April 1, 2021.

[20] John T. (2012). “TUC backs NUPENG on alleged JTF’s connivance with bunkers”, Daily Sun, Thursday, 16, August, 2012, pp.10.

[21] Kim S. H. and Lim S. C., (2018). "Intelligent intrusion detection system featuring a virtual fence, active intruder detection, classification, tracking, and action recognition," Ann. Nucl. Energy, vol. 112, pp. 845-855, 2018.

[22] Kramp T., Van Kranenburg R., Lange S., (2013) “Introduction to the Internet of Things”. In: Bassi A. et al. (eds) Enabling Things to Talk. Springer, Berlin, Heidelberg.

[23] Kumar M., Murthi Sarma N., Sridevi Ch., Pravin A., (2012). "ARM9 Based Real-Time Embedded Network Video Capture and SMS Altering System", International Journal of Research in Computer and Communication Technology, Vol.1, Issue 7, pp.489-493, December 2012.

[24] Lee H.K., and Chuah C. W (2018). Smart Indoor Home Surveillance Monitoring System Using Raspberry, International Journal on Informatics Visualization, 2(4), 299-308.

[25] Liang K. M., Hon H. W., Khairunnisa M. J., Choong T. L., and Khairil H. Z. (2012). "Real-time intrusion detection system for outdoor environment," in Proceedings of the ISCAIE, Kota Kinabalu, Malaysia, 3-4 December 2012, pp. 147-152.

[26] National Oil Spill Detection and Response Agency (NOSDRA) 2016. National Oil Spill Detection and Response Agency (NOSDRA) Nigerian oil spill monitor.

[27] Nicola Curtis (2022). Ineffective maintenance can lead to serious consequences. Nicola Curtis is a technical copywriter at Rotork. Issue March 2022

[28] NNPC (2014). "How pipeline vandals cripple fuel" supply", Accessed online at http://www.nnpcgroup.com/public relation on June 24, 2014.

[29] Nosiri O.C., Akwiwu-Uzoma C.C., Nmaju U.A., Elumeziem C.H. (2018). Motion Detector Security System for Indoor Geolocation. International Journal of Engineering and Applied Sciences (IJEAS), 5(11), 24-30.

[30] Obodoeze F. C., Asogwa S. C. and Ozioko F. E. (2014). Oil Pipeline Vandalism Detection and Surveillance System for Niger Delta Region. International Journal of Engineering Research & Technology (IJERT) IJERTIJERT ISSN: 2278-0181. www.ijert.org. Vol. 3 Issue 7, July – 2014

[31] Odalonu, Boris (2015). The Upsurge of Oil Theft and Illegal Bunkering in the Niger Delta Region of Nigeria: Is There Any Way Out? Mediterranean Journal of Social Sciences 6 (3), pp. 363–573.

[32] Ojediran B., and Ndibe J. (2005). "Oil Spill Management: SPDC and the Environment, 2005." Unpublished.

[33] Okoli, Al Chukwuma (2016). Petroleum Pipeline Vandalism and National Security in Nigeria, 2001–2012. PhD thesis submitted to the School of Post-graduate Studies, Nigerian Defence Academy, Kaduna, p. 1.

[34] Paing S. N., Oo M. Z., Othman M., and Funabiki N., (2019). "A Personal Use Vehicle Anti-Theft Tracking System Using IoT Platform", IJCSE, an open-access journal, Volume 4.143, 2019.

[35] Pajouh H. H., Javidan R., Khayami R., Dehghantanha A. and Choo K. R., (2019) "A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IoT backbone networks", IEEE Trans. Emerg. Topics Comput., vol. 7, no. 2, pp. 314-323, Apr. 2019.

[36] Premium (2017). Times Vandals cut Nigeria's oil production by 800,000 barrels per day. 2017. http://www.premiumtimesng.com/news/top-news/203515-vandals-cut-nigerias-oilproduction-800000-barrels-per-day-kachikwu.html Internet

[37] Punch Newspaper, (2021). Unending menace of pipeline vandalism. 14th January 2022

[38] Sahara Reporters (2014). A nation in search of pipeline safety http://www.saharareproters.com/nigeria

[39] Sfar A. R, Chtourou Z, Challal Y (2017). A systemic and cognitive vision for IoT security: A case study of military live simulation and security challenges. International Conference 2017 - ieeexplore.ieee.org

[40] Shell Petroleum Development Company; (2018). Oil Spill Data. http://www.shell.com.ng/environment-society/environment-tpkg/oil-spills.html

[41] Sheshai. S. S (2016), Raspberry PI Based Security System, University Of Nairobi, Kenya.

[42] This day, (2014) "NNPC lost about N163billion in the space of three years to pipeline vandalism", accessed online at http://www.thisdaylive.com on June 13, 2014.

[43] Ying-Wen Bai, Li-SihShen and Zong-Han Li, (2010). "Design and Implementation of an Embedded Home Surveillance System by use of Multiple Ultrasonic Sensors" Consumer Electronics, IEEE Transactions on Volume:56, Issue:1, ISSN:0098-3063 February 2010.

[44] Yo-Essien L. P. E. (2018), "Oil Spill Management in Nigeria: Challenges of Pipeline Vandalism In The Niger Delta Region Of Nigeria", pg.16.