THE PROTECTION OF CRITICAL INFRASTRUCTURES USING PERIMETER FENCING SECURITY

[1]Engr. Fidelis C. Obodoeze

[2]Oliver Ifeoma Catherine

[3]Engr. Levi N. Osuji

[1,3]Department of Computer Engineering, Akanu Ibiam Federal Polytechnic, Unwana. [1]fcobodoeze@gmail.com , [3]engrlevi.osuji@gmail.com

[2]Department of Computer Science, Akanu Ibiam Federal Polytechnic, Unwana. Prestigiousbaby1130@gmail.com

Phone/WhatsApp: +2348062926794

Abstract:

The protection of critical and sensitive infrastructures such as public buildings, power plants, nuclear plants, oil and gas pipelines and wells, offshore oil facilities, medical facilities, etc cannot be overemphasized especially in an area where there is high rate of vandalism and terrorism. There is a growing concern in Nigeria concerning the rampant vandalization of petrolatum and gas pipelines that deliver critical petroleum products across the length and breadth of the country for the survival of the national economy. Power infrastructures such as transformers, electricity cables and other critical power equipment are also targets to vandals and thieves. In the North East region of Nigeria, Telecommunication Base stations have been target of attacks by Boko Haram and ISWAP terrorists operating in that area. Nation's airports, military facilities are also targets to terrorist targets. Perimeter security fencing or security is vital for successful monitoring and detection of unwanted movement or intrusion into any of these critical assets be it above-the-ground, underwater or buried underground assets. Perimeter security can be installed to monitor, track, and classify intrusions into any critical assets whether remote or nearby. This paper explored all the intricacies and operational methodologies of using wireless and wired fibre optic perimeter security in monitoring, tracking and detecting unwanted intrusion into any critical assets for the overall protection of these assets against any form of vandalism and terrorism.

Keywords: *Critical asset, SCADA, fibre optic, perimeter fencing, perimeter security, wireless sensor, vandalism, terrorism, false alarms*

1.0 INTRODUCTION

Critical assets or infrastructures are high-value and sensitive targets that can be attacked or intruded via either vandalism or terrorism. There is therefore a crucial need to protect these high-value assets from intrusion and attacks.

Critical infrastructures or assets such as power plants, telecommunication equipment, public water supply, sensitive public buildings, medical and laboratory equipment, aircraft, oil and gas pipelines, nuclear plants, storage tanks, oil wells etc need to be protected by installing perimeter fence security such as fibre optics intrusion systems or wireless sensors both inside and outside the perimeter fence. These critical infrastructures need to be protected using end-to-end perimeter protection which requires both physical security measures, such as fencing, and perimeter fence detection systems.

If the perimeter security is weak, critical infrastructure could be left vulnerable to physical attack, resulting in irreparable damage. For instance, if there is no perimeter fence security at right of way of oil and gas pipelines, vandals could break in undetected and steal the petroleum product and may even damage the pipelines infrastructures. Public water supply or source can be poisoned by terrorists.

Wireless sensors are miniaturized and battery-powered and can be quickly and easily deployed for autonomous surveillance, even without existing infrastructures. Also wireless sensors perimeter fence security systems are nearly invisible which ensures undetectability by intruders Wired perimeter fence security systems such fibre optics perimeter fence intrusion detection system can be deployed to monitor and track any form of intrusion or attack on any critical asset. Fibre optics though is more costly and difficult to procure and install but have been proven to be far easier and more reliable during maintenance; this is because fibre optics sensing eliminated the problems of false alarms that are common with other perimeter fence security systems.

1.1 Components of Perimeter security Systems

The perimeter security system consists of a transmitter and a receiver mounted in line with each other on the outer boundary of the premises or assets that is being monitored. The transmitter continuously transmits the infrared beam and the receiver at the same time detects it.

1.2 What is a perimeter fence?

Perimeter fencing is carried out to barb and enclose a given area and preclude vandalism and unauthorized access. Perimeter fences indicate a boundary that separates a property, asset or an infrastructure from the rest and is usually employed for visual appeal, privacy, and security. Rigging a perimeter fence on a property is an ideal way of preventing theft, vandalism and terrorism etc. Perimeter fencing acts as the first point of defense against any attack by an intruder. The most common type of perimeter fence is available as a series of vertical metal bars such as mesh fencing, school fencing, prison fencing, etc. These fences are preferred for high-security properties or critical assets and are sometimes connected at the top and the lower part using a horizontal bar, which fortifies them. Also critical assets can be protected using extreme perimeter security solutions should go for a security electric fences. This perimeter fencing is efficient at stopping intruders from entering any property by giving

them a shock. Certain perimeter fences are great for security reasons and may be used around utility stations and swimming pools. Fig.1 shows a typical barb-wired fence to protect a power plant from being vandalized or looted using a fibre optic security system mounted on it.

Fig. 1: A fibre optic perimeter security mounted in a barb-wired fence to protect power station

2.1 METHODS OF INSTALLING PERIMETER SECURITY FENCE SECURITY TO PROTECT A CRITICAL ASSET

The following methods can be adopted to protect any critical asset using perimeter fencing:

a. *Above-the-ground or surface systems using wireless systems and fibre optics intrusion detection systems*
b. *Buried optical fibre perimeter fence intrusion system*
c. *Underwater or marine intrusion detection security fence*

Fig.1 shows also a type of above-the-ground intrusion detection security fence being used to protect a power plant from being vandalized. This type of perimeter fencing intrusion detection systems can be implemented using either wireless or fibre optics system or both combined together. As shown in Fig.2, this type of underwater security system is a rigid steel grating supporting an interlaced fibre-optic sensor cable which is fully encased in solid resin. This combination of a tough physical barrier with intrusion detection provides an extremely effective alarm generation system.

*Fig. 2: An underwater perimeter fence intrusion system (*Remsdaq, 2022)

2.2 State of the Art in Perimeter Security

Critical infrastructure locations are frequently vulnerable to theft, vandalism, and attack. Intruders can be deterred and detected at the perimeter using devices like intelligent lighting, fence sensors, and video analytics before they hurt themselves or cause property damage.

Systems for perimeter security may safeguard vital infrastructure for facilities of various sizes, whether they are used alone or in combination with other multi-layered solutions.

Detect/Identify Intruders Before They Enter:

A first line of defense against invasions or intrusions is the installation of perimeter intrusion detection systems.

While there are many different kinds of perimeter sensor systems, some of them are better suited for protecting critical infrastructure than others.

The following factors can be considered when comparing and selecting various intrusion detection systems:

Factors to consider before selecting perimeter security system:

The factors or considerations include the following:-

1. **Coverage**

Does the system cover the full perimeter or boundary (i.e., are there any blind spots)?

2. Probability of detection (Pd)

Can attempts to breach the perimeter be detected by the system promptly and correctly each time?

3. **Nuisance alarm rate (NAR)**

Does the system generate false alarms or real alarms when there is an actual or real intrusion into the perimeter of an asset ? If there is a simulated intrusion, does the security system detects that?
Security may begin to suffer if the system sets off alarms in calm or windy weather because responders may get complacent.

4. **Ease of installation and configuration**

Is the perimeter fence security easy to install and setup? Can it be easily configured and maintained from a remote location by a maintenance staff using an equipment without the need to travel to the site location?

5. **Integration with Security and Video Management Systems (SMS/VMS)**

Can the system's information be presented in a way that enhances situational awareness? Can the SMS/VMS provide the exact location of intrusion attempts on a map, for instance?

- Is it possible to automate camera control using the VMS and alarm integration?
- Is there complete activity tracking so that incident reports can be produced?

6 Cybersecurity concerns

Can the system be hardened to keep physical security systems safe against computer-based attacks?

Fence-Mounted Sensors:
Existing fences become smart fences because of the installed sensors on the fence which can locate and identify efforts to climb, cut, or raise the fence's fabric. They operate consistently in all weather circumstances and are robust, affordable, field-tested, difficult to defeat, and cost-effective. Other on-site security resources, such as PTZ cameras, as well as deterrence tools like sirens, loudspeakers, and/or security lights, can be activated when an intruder is identified using the generated alarm (which contains the intrusion zone or precise position). Security professionals can control the system from a central monitoring station, like SCADA, where they can assess the situation remotely and take the right action. Fig.3 shows a typical

PZT solar powered security camera that can be deployed to ensure all-round security of any physical critical asset or property.

Fig. 3: PZT solar-powered outdoor 4G self-mounted camera

For important infrastructure locations, especially those with longer perimeters like oil and gas pipelines, fiber optic-based fence sensors are a preferred option. These sensors are resistant to lightning and electro magnetic induction (EMI), non-conducting, and intrinsically safe in explosive environments. A single unit placed indoors or outdoors in a secure area may frequently provide support for longer coverage distances, allowing it to safeguard the whole perimeter of a building or a remote facility like an oil and gas pipeline. The devices provide high-value security features like precise range, environmental adjustment algorithms, and cut immunity by utilizing cutting-edge sensing techniques like Coherent Optical Time-Domain Reflectometry (C-OTDR).

The installation of a fence-mounted fibre-optic (above—the-ground) locator system is shown in Fig.4.

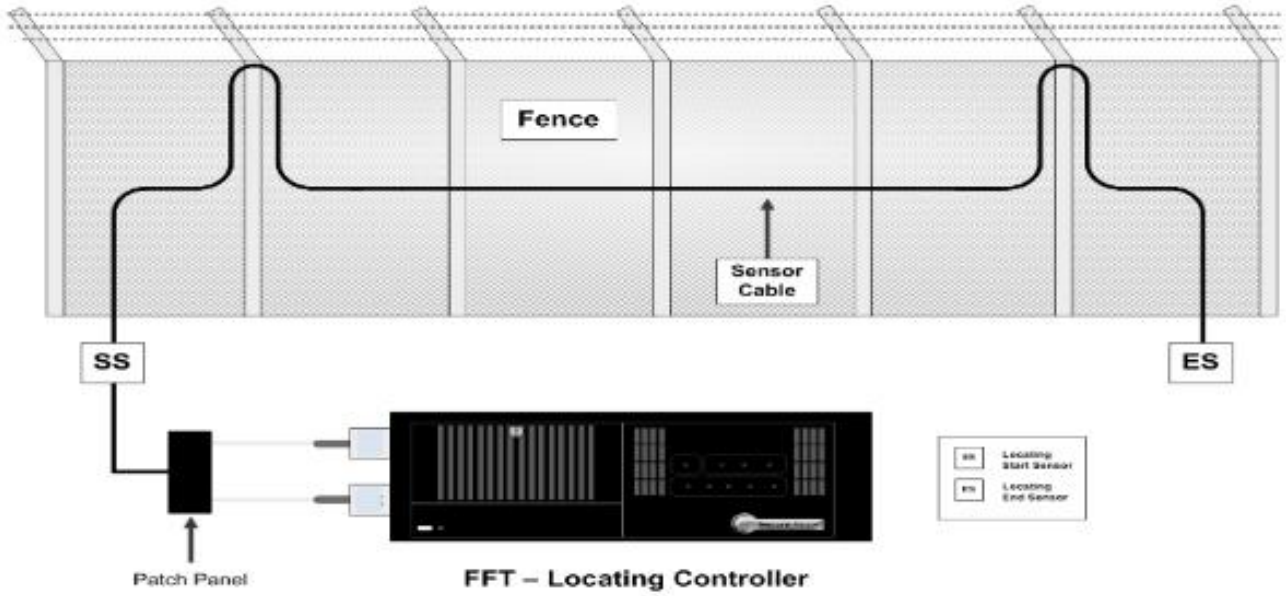

***Fig.4:** A fence-mounted fibre-optic FFT Microstrain Locator system. (SS=start sensor and ES= end sensor)*(Mahmoud et al, **2012**)

In buried systems such as oil and gas pipelines or transformer's armoured cables, the sensing cable is typically buried next to the pipeline to detect third party interference (TPI)activities as shown in Fig. 5 Inevitably it will also be sensitive to other non-intrusion events such as those from nearby traffic and railway crossings.

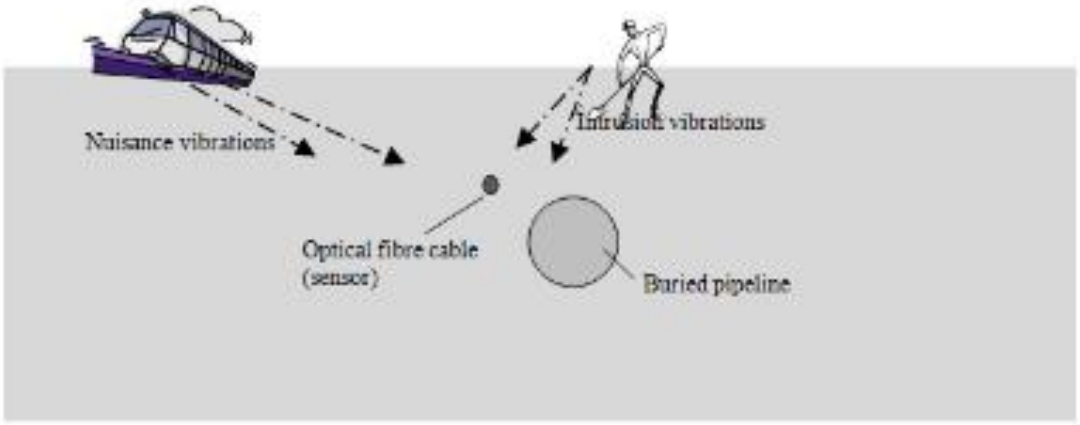

Fig.5. A Cross section of a buried fibre-optic intrusion detection system for detecting third party interference (Mahmoud et al, **2012**)

Precision range, a significant technological advance over older "block" sensors, offers a number of advantages. Information about the location of intrusions can be utilized to guide surveillance cameras and also allow sensitivity levels to be changed for particular fence sections (for example, to accommodate for changes in fence construction). The ability to detect between actual intrusion attempts and site- or area-wide disturbances brought on by

strong winds can help range capabilities reduce nuisance alarms. Finally, range lowers operational expenses by making it easier for maintenance employees to find and fix problems.

What would happen if a cable were to cut is a recurring concerns or worry with sensors that are positioned on fences. When this occurs, whether on purpose or unintentionally in an effort to trick the sensor, the system promptly notifies the incident and its precise position. Furthermore, time-domain reflectometry-based systems continue to be able to locate and identify intrusions up until the cut. The sensor becomes cut-immune when put in a redundant-loop design, continuing to give detection on the entire perimeter even after a cable cut.

Perimeter sensors can be added to perimeter fence gates, which are already normally outfitted with electronic access control and closely monitored by video cameras. By directing the cable onto each moving panel, swing gates can utilize the same fence sensor securing the perimeter (the cable is trenched from one side to the other). Other technologies work well for sliding gates. Virtual detection zones may be watched over by outdoor people and vehicle tracking video analytics if the area can be seen clearly from above.

An embedded accelerometer can also be used, in wireless gate sensors, to analyze gate movement in three-dimensions, enabling the sensor to distinguish between gate activity, intrusion attempts, and environmental conditions. The sensor communicates with a nearby processor over an encrypted and monitored wireless link. If there is a suspicious event or an intrusion attempt, communication link failure, or an attempt to remove the sensor from the gate – an alarm is immediately generated.

Intelligent Lighting:

A recent development in perimeter security is intelligent, low-voltage lighting. LED-based luminaires installed on fences outside of designated hazardous areas offer uniform, focused wide-spectrum illumination along the fence line. A high Color Rendering Index (CRI) number implies colors are accurately portrayed, substantially benefiting security personnel with identification. This improves the quality of video feeds by minimizing hot spots. Additionally, LED-based lighting has an average lifespan of over 10 years, which virtually eliminates maintenance.

Although these advantages are valuable, how do they apply to perimeter sensors? This is where the term "intelligent" is relevant.

The fence vibrations brought on by a vandal or intruder trying to cut, climb, or lift the fence fabric are picked up by sensors included within the luminaires themselves. Additionally to alerting the SMS/VMS, the nearby luminaires might immediately go into full power or strobe. Potential intruders may change their behavior if they are aware they are being monitored.

Video Analytics:

With the advent of HD cameras with outstanding low-light, infrared, and thermal capabilities, as well as higher performance/lower cost computing resources, the usefulness of video analytics has significantly increased in recent years. Complex video analytic software has been created as a result of developments in computer vision research and is now optimized for people tracking both indoors and outdoors, left/removed item detection, PTZ auto-

tracking, face and license plate recognition, crowd detection, and other functions. These software modules could be integrated on certain cameras or a part of a VMS.
Video analytics provide a new set of technologies that significantly improve perimeter security at a relatively cheap cost, rather from serving as a replacement for conventional fence-mounted sensors. Video analytics, for instance, can make use of a facility's current camera system to follow and detect people close to perimeter fences, giving early notice of possible security events before they happen.
Video footage from a surveillance camera shows a location that is guarded by both an intelligent lighting system and an outside people monitoring video analysis.

Cybersecurity of Physical Security Devices:

Whenever physical security devices are deployed, they themselves have the potential to become cybersecurity targets, often with the intention to be used as a springboard for targeting other critical systems. This is what have been experienced in Niger Delta Oil region of Nigeria where wireless sensors that are used to monitor oil wells are destroyed by vandals trying to steal crude oil or petroleum products (Aroh et al, 2010).

Site owners and integrators should ensure the following in order to prevent physical security devices from introducing new vulnerabilities:

- Security devices are physically protected against tampering and are configured to sound alarms if tampering does occur;
- Inter-device communications are segregated from external network connectivity;
- Software applications use encrypted communications;
- Software vendors conduct Penetration Testing (PEN Testing) by trustworthy third parties.

Increased Security, Increased Public Safety:

The objective of consistently detecting efforts to evade perimeter fencing and gates can be achieved with the aid of perimeter intrusion detection technology, which includes sensors mounted on fences, intelligent illumination, and integrated video analytics. The most important factors to consider when assessing these systems for use at critical infrastructure facilities are to make sure they accurately identify intrusion attempts while avoiding false alarms, blind spots, and other security gaps, are cost-effective for sites with long perimeters, and can be properly integrated to improve overall security response capabilities without subjecting the organization to additional cybersecurity risks. Environmental and public safety concerns can be reduced with the help of security procedures and the use of the suitable physical technology.

3.0 PROPOSED METHODOLOGY FOR PROTECTION OF CRITICAL INFRASTRACTURES IN NIGERIA

For early detection, classification and identification of any illegal intrusion in a designated area, a remote wireless system can be used. This is better than conventional CCTV wireless cameras. Fig.6 shows the architecture of an integrated wireless perimeter fence security system combining both traditional wireless systems such as infrared sensors, seismic /acoustic sensors as well as thermal and CCTV cameras and GPS receivers. It is also possible to combine this wireless integrated perimeter fence security with a wired perimeter fence security such as fibre optics sensing system.

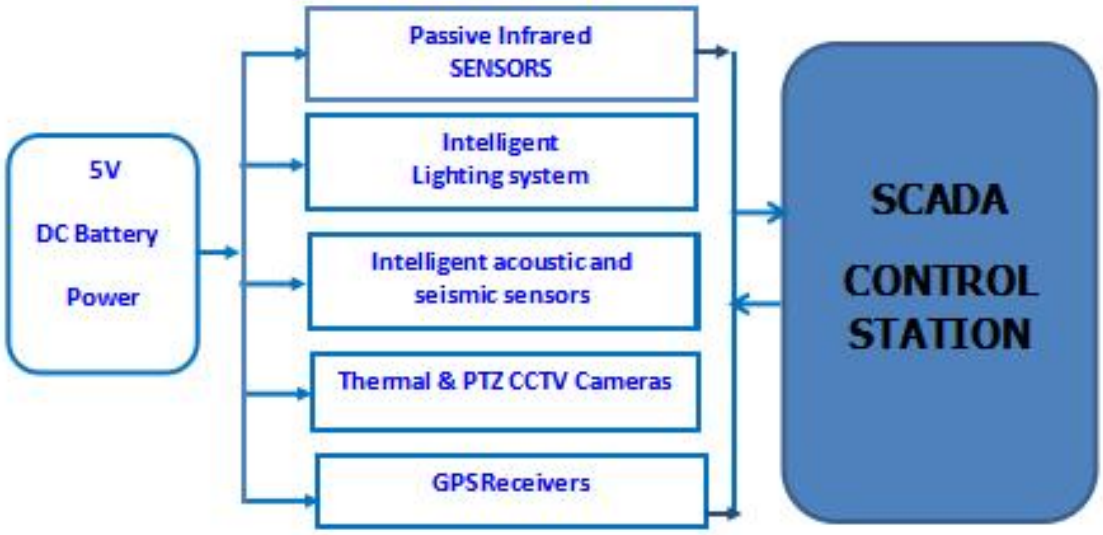

Fig. 5: The components of a wireless perimeter fence intrusion detection system

Passive infrared sensor is an electronic sensor that measures infrared light radiating from objects in its field of view. They are most often used in PIR based motion detectors, PIR sensors are commonly used in security alarms and automatic lightning applications. They are used to detect motions or movements by humans or animals in any particular location. They emit signal when the infrared sensors in them detect radiation from humans or animals.

Acoustic sensors are used to detect sound or for eavesdropping, they detect mechanical vibrations in a solid. They are a class of wave sensors that applies micromechanical systems which rely on the modulation of surface acoustic waves to sense a physical phenomenon (Wikipedia, 2022).

A seismic sensor is an instrument to measure the ground motion when it is shaken by a perturbation. This motion is dynamic and the seismic sensor or seismometer also has to give a dynamic physical variable related to this motion.

Thermal cameras are originally developed for surveillance and military operations but they are now being deployed for building inspections (moisture, insulation, roofing, etc.), firefighting, autonomous vehicles and automatic braking, skin temperature screening, industrial inspections, scientific research, etc.

Global Positioning System (GPS) *unit or receiver is used to detect the geographic position or coordinates of an object in a particular location.*

Fibre optics perimeter fencing system can also be used on its own or combined with other technologies to detect intrusion into any critical asset or infrastructure. Although, fibre optics is expensive to procure and install but it has the advantages of increased reliability because it eliminate false alarms associated with other perimeter fence sensing technologies.

An example of an integrated perimeter fence security using RaySense Optical sensor technology is shown in Fig.6.

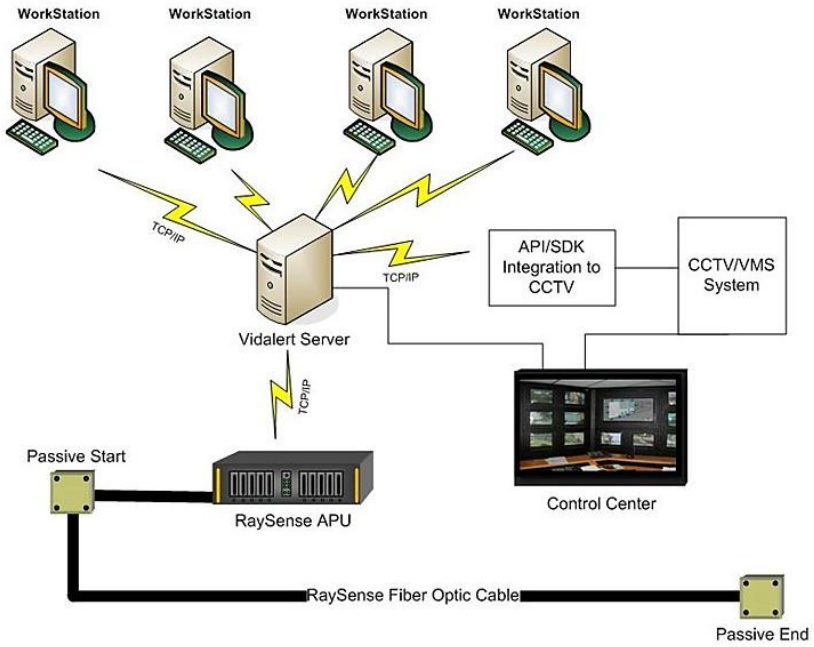

Fig. 6: System layout of RaySense integrated fibre optic perimeter fence security (RBTEC, 2022).

According to RBTEC (2022), the RaySense System uses a typical single-mode fiber optic cable as a powerful vibration sensor. RBtec uses different technologies such as Distributed Acoustic Sensing (DAS) Technology and Distributed Vibration Sensing (DVS) Technology for different applications as a measurement of monitoring a fiber optic. The fiber optic cable becomes extremely sensitive to pressure, acoustics and motion, capable of detecting minute vibrations transmitted through the fence, soil or the surface. The RaySense System can monitor the vibration signals along the length of the fiber optic cable and have the ability to locate an intrusion event and classify the specific signatures based on the detection algorithm. utilizing fiber-optic cable, the system is the most economically competitive technology currently available for long distances. Requiring only a single alarm processing unit (APU) to cover up to 100km/62 miles if the cable starts and ends at the same point (loop) or 50 km/31 Miles in a straight line combined with a rugged fiber-optic sensing cable, results in the most cost-effective fence detection solution for large perimeters.

4.0 SUMMARY AND CONCLUSION

The protection of critical and sensitive infrastructures such as public buildings, public water supply, power plants, airports, railway stations, nuclear plants, oil and gas pipelines and wells, offshore oil facilities, medical facilities, etc cannot be overemphasized especially in an area where there is high rate of vandalism and terrorism such as obtainable in Nigeria. There were reported cases of vandalism and theft of public infrastructures in Nigeria such as oil and gas pipelines, telecommunication base stations, power stations, electricity transformer and armoured cables. All these criminal acts hurt the Nigerian economy. This paper x-rayed the importance of perimeter fencing security systems in protecting and defending critical public infrastructure from all sort of attacks and vandalism. This paper has x-rayed different state-of-the-art technologies that can be employed in setting up and installing perimeter fence security in protecting critical assets in the country.

Perimeter fence security systems should be installed to monitor and track any act of vandalism or terrorism from a central SCADA control center to any critical national asset or infrastructure.

4.1 RECOMMENDATIONS

The following recommendations are suggested for implementation in Nigeria so as to protect critical public assets and facilities:

1. It is recommended for any critical assets or infrastructure to be protected using fibre optics perimeter fence intrusion security to eliminate false alarms and to ensure reliability and security.

2. It is recommended that SCADA be centrally installed so as to monitor 24/7 what is going on at the remote site of the critical assets such as oil and gas pipelines, crude oil wells, airports, train stations, Power plants/stations, together with an integrated perimeter fence intrusion detection system.

3. It is recommended that railway tracks in Nigeria be protected from terrorist attacks and vandalism by installing CCTV cameras and other wireless intrusion detection systems

4. It is also recommended that integrated security systems such as fibre optics system and Wireless systems using PIR, PTZ CCTV Camera using video analytics, and lightening system to track illegal intrusion into any critical assets or infrastructure

References:

K.N. Aroh, I.U. Ubong, C.I. Ezeh, I.M. Harry, J.C. Umo-Otong, A.E. Gobo (2010).”Oil Spill ‘incidents and pipeline vandalization incidents in Nigeria: Impacts on Public Health and Negation to the attainment of the Millennium Development goals”, Disaster Prevention and Management Journal , Vol. 19 Issue 1, pp.70-87, ISSN 0965-3562.

RBTEC (2022). “RaySense Principle of Detection”. Accessed online at https://www.rbtec.com/perimeter-sensors-and-underground-protection/fence-intrusion-detection-products/raysensefencefiberoptic

Remsdaq(2022).”Aquemesh underwater intrusion detection system”. Retrieved online at https://www.remsdaq.com/solutions/integrated-security-systems/perimeter-intrusion-detection-systems-pids/aquamesh-perimeter-intrusion-detection-system/

Seedahmed S. Mahmoud, Yuvaraja Visagathilagar, and Jim Katsifolis (2012).”Nuisance alarm suppression techniques for fibre-optic intrusion detection systems”. Proceedings of SPIE - The International Society for Optical Engineering 8351:121-January 2012. DOI: 10.1117/12.915950

Wikipedia (2022).” Surface acoustic wave sensor”. Retrieved online at https://en.wikipedia.org/wiki/Surface_acoustic_wave_sensor