A Fault Tolerant Design For Critical Infrastructure Protection In Nigeria: A Case Of Oil Pipelines In The Niger Delta Region.

Ofoegbu Osita Edward

(Lecturer II) Deparment of Physics Electronics, Oduduwu University Ipetumodu Osun-State, Ile-Ife, Nigeria.
Email: edoxnt@yahoo.com

ABSTRACT: Since Oil was discovered at oloibiri in 1956, Nigeria as a nation has experienced significant growth in the oil and gas sector as it now accounts for more than 85% of the country's GDP. The growth of this sector with its commercial gains and importance has culminated in the rise of illegal activities by people who attempt to sabotage operations as in the care of militants, terrorists or bunkerers who intercept pipelines transporting the oil with the aim of siphoning for personal gain. This growing malaise has resulted in enormous financial losses to the government and environment concerns resulting from the attendant oil spillage. Effort made by the government has not yielded much success in curbing this ever-expanding malaise. This paper attempts to proffer a solution framework using emerging technological solutions by adopting a fault tolerant approach to remote monitoring of the pipeline network .A wired/wireless sensor network approach in proposed with suitable restructuring of the pipeline topology to support its implementation. The fault tolerant approach would also encompass human effort to ensure optimal delivering of service so as to aid security agents/monitoring groups to track, trace, apprehend and prosecute the culprits who perpetuate these acts.

Keywords: CIP, Fault tolerance, Pipelines, SCADA.

1 INTRODUCTION

Critical Infrastructure protection (CIP) is a concept that relates to preparedness and response to serious incidents that involve the critical infrastructure of a region or nation [1].Critical infrastructure in itself has been widely adopted and defined to distinguish those infrastructure elements that if damaged or destroyed would cause serious disruptions in the system itself or of dependent systems [1] .Examples of such system are water supply networks, telecommunication utilities ,power utilizes ,oil and gas pipeline networks ,airports, bridges, dams, mass transit, railway services etc. The term critical infrastructure protection was coined after a presidential directive by the then president of the united states Bill Clinton in May 1998 to develop a national program to ensure the security and reliability of vulnerable and interconnected infrastructures in the United States. Pipelines provide a means through which goods are transported i.e. mainly liquids and gases. Nigeria as a country is blessed richly with huge hydrocarbon deposits specifically in the Niger Delta basin therefore pipelines are used as a mode of transport for crude and refined petroleum products. The pipeline transverses the entire landscape of Nigeria's Niger Delta region and it utilizes vast traits of land. Since the Nigerian economy is dominated by the oil and gas sector the pipeline network thus constitutes a major critical Infrastructure. Available data from the oil and gas sector estimates the pipeline network at over 3000km [2] which covers transportation of petroleum products from oil refineries and import-receiving jetties to storage depots in Nigeria. To effectively manage and monitor this network of pipelines a pipeline monitoring system(PMS) [1] which is technically a SCADA is applied to act as a leak detection system and there exists several implementations all over the globe such as the ORLEN lietuva system applied in the gas pipelines in the Ukraine, etc .Despite the application of monitoring measures to detect the abnormalities in the pipeline network , the challenges still abound as the Niger Delta area which bears Nigeria's crude oil earnings from exports which amount to over 86% of the annually generated revenue is creeping with crude oil thieves, vandals, bunkerers and also the latest threats from terrorists .Numerous economic criminals have setup illegal refineries with the sole purpose of refining illegally bunkered crude oil for sale in neighboring countries and in most cases the criminals collaborate with the security personnel attached to police the infrastructure. According to a report by shell petroleum, one of the major international oil companies(IOC) operating in the Niger Delta region of Nigeria, Nigeria loses about 2 billion US dollars annually as a result of activities of crude oil thieves and pipeline vandals who profit illegally from crude oil theft in the Niger Delta region [2].

2 RELATED WORKS

2.1 Objectives of the Paper

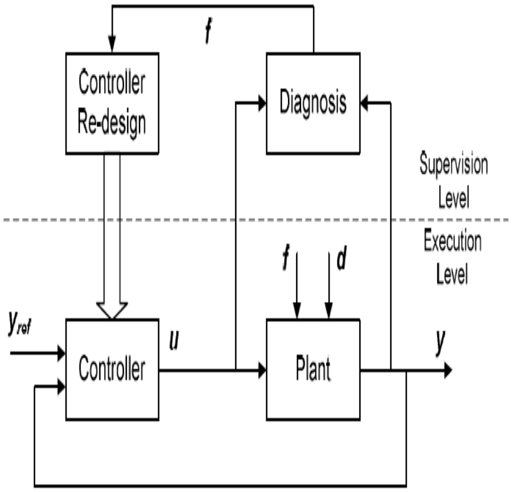
This paper is a holistic survey of the pipeline structure and the monitoring system used and how restructuring the pipeline network with a fault tolerant approach utilizing a wired/wireless sensor network approach, fibre optic and remote control terminals can be used to provide 24-hour complete surveillance and monitoring of the pipeline network while providing reliable information relating to intrusion and leak detection which both suggest third party activities. The real time data collated would be used to trigger alarms with the aim of alerting the security operatives and closing an emergency shut down valve to isolate the region of intrusion. At the end of the paper, a holistic implementation framework on how the overall system operates is proposed and presented such that accurate /concise data collated from the system can help law enforcement and security operatives arrest these identified National security challenges.

2.2 Related Work

There are a lot of research efforts currently ongoing to tackle the militancy/oil bunkering occurring in Niger Delta region of Nigeria. The rise in terrorist activities specifically the BOKO HARAM, AN-SARU, JAMBS, MEND etc , all pose a National security challenge as was highlighted by authors [2,3]. Here they proposed a National security implementation framework to solve the problem of oil bunkering using wireless sensor networks from the survey of the various challenges facing the oil pipeline network in Nigeria, using a wireless sensor network above cannot tackle the issue of longetivity of the implemented system with regards it susceptibility to faults due to the fact that pipeline transverse different terrains. The power problem with regards the use of battery operated wireless sensors which makes maintenance operations an up-hill task especially for pipelines that transversed into hard to reach areas like the swampy regions of the Niger Delta, the unavailability of sufficient sunlight to recharge the batteries of the wireless sensors especially in dense forests and swampy regions. It is clear that wireless sensors alone cannot tackle this security challenge but requires the fusion of a fault tolerant approach to provide much needed redundancy which can give an acceptable degraded performance when the system fails .Thus, extending the longetivity of the pipeline monitoring system.

2.3 Fault Tolerance and Fault Tolerant Control

Modern technological systems rely heavily on sophisticated control systems to meet increased safety and performance requirements and this is a particularly time in safety critical infrastructures where a minor or often benign fault could potentially develop into catastrophic events if left unattended. To prevent fault induced losses or performance drop and minimize potential risks new control techniques and design approaches need to be developed to cope with system component malfunction. The control system that posses such a capability in often known as a fault tolerant control system [7].Therefore fault tolerance is a concept comprising of fault tolerant control (FTC) and Fault Detection and Isolation(FDI) which generally implies that when a fault occurs in a system the main problem is to raise an alarm, ideally diagnose what fault has occurred and then decide how to deal with it such that the problem of detecting a fault, finding the source/location and then taking appropriate action in the basis of fault tolerant control[7].



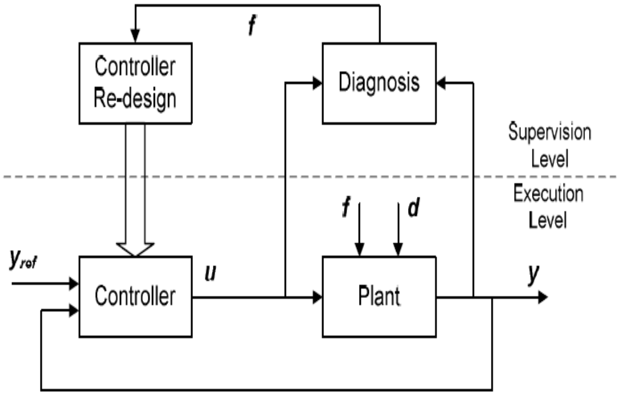


Figure 1: The Architecture of Fault Tolerant Control [7].

2.4 Sensor Network (Wired/Wireless)

A sensor network is a group of specialized transducers with a communication infrastructure intended to monitor and record condition at diverse locations. A sensor network consists of multiple detection stations called sensor nodes, each of which maybe small in size, lightweight and portable. The wired sensor in a network configuration actually communicates with other nodes in the network or to a data collating point through physical wire connections. While in the wireless scheme the communication transmission and reception is done wirelessly over the air. A typical sensor node would comprise of a transducer, microcomputer, battery, transceiver and power source where the transducer generates electrical signals based on sensed physical effects and phenomena, the microcomputer processes and stores the sensor output, the transceiver which as earlier said could be hardwired/wireless/hybrid receives command from a central computer and transmits the data[4]. Wireless sensor networks (WSNs) are IEEE 802.15.4 enabled devices capable of robust and reliable multichip communication [5, 6], a wired/wireless sensor network can be deployed to provide redundancy and fault tolerance with useful application in environmental monitoring applications specifically in the oil and gas sector. In the wired/wireless network scheme wireless sensors are connected together with physical wires and configured such that the wire provides a source of power for the sensor as well as acting as a communication medium. If in the event of a failure such as a cut-wire or damaged connecting cable the battery in the sensor powers the sensor which then transmits it data wirelessly. A combination of a wire to provide power to the sensor together with an optical fiber cable provides a communication medium fused with the wireless transmission capability of a wireless sensor which should provide sufficient fault tolerance in most monitoring application in unmaintainable and hard to reach areas. The figure below depicts a suitable wireless sensor node which is currently installed by a prominent oil and Gas company (IOC) ,shell petroleum development company (SPDC) in over 1000 wells scattered in Nigeria's Niger Delta region[2]. An integration of a rechargeable battery associated circuitry implementing a wired/wireless scheme using physical cables and fibre optic would provide an optimal approach to monitoring pipelines parameters such as pressure, temperature, flow rate etc which would enable detection of third party intrusion.

Figure 2: A model of vMBusX-SP battery-powered Smart Wireless Sensor installed by SPDC in her over 1000 oil wells and other oil facilities in the fields of Niger Delta to fight vandalism and theft [2]

2 Optical Fibre Cable

An optical fibre cable in a cable containing one or more optical fibers where the optical fibre elements are typically individually coated with plastic layers and contained in a protective tube suitable for the environment where the cable would be deployed for use in strenuous environments such as oil pipelines which transverse diverse terrains. A robust cable construction must be implemented such as the loose-tube construction where the fiber is laid helically into semi-rigid tubes allowing the cable to stretch without stretching the fibre itself. This method of construction protects the fibre from tension during laying and also from temperature changes [5].

Figure 3: Optical Fiber Cable.

3 The Proposed Fault Tolerant Design for Oil Pipeline Monitoring in Nigeria

In this section the implementation framework for integrating fault tolerance for pipeline monitoring in Nigeria is shown below.

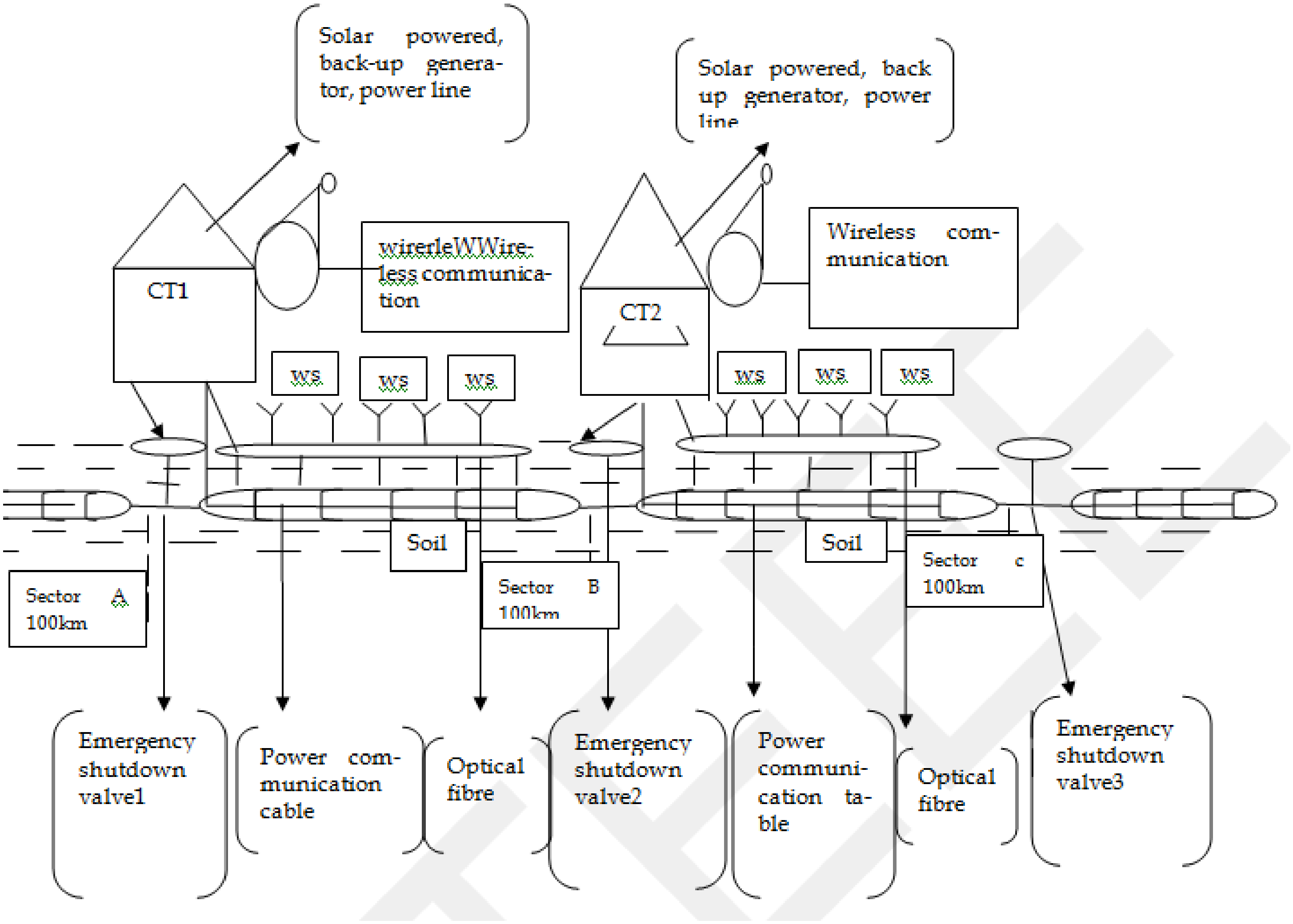

Solar powered, back-up generator, power line
Solar powered, back up generator, power line
wirerleWWireless communication
Wireless communication
CT1
CT2
ws
ws
ws
ws
ws
ws
Soil
Soil
Sector A 100km
Sector B 100km
Sector c 100km
Emergency shutdown valve1
Power communication cable
Optical fibre
Emergency shutdown valve2
Power communication table
Optical fibre
Emergency shutdown valve3

Figure 5: The Proposed Fault tolerant Pipeline Monitoring System.

CT_1, CT_2 = On-site control/monitoring office which would also serve as a manned security base for the army and civil defense forces for Physical security in the various sectors. In Fig5, it is proposed that HDD Technology should be used in Marsh land/swampy areas to ensure that pipelines are buried deeper into the ground. Where the control terminal(CT) include a power source for providing electrical power to the sensors in the network and could be solar powered source, back-up generator or power line supply.

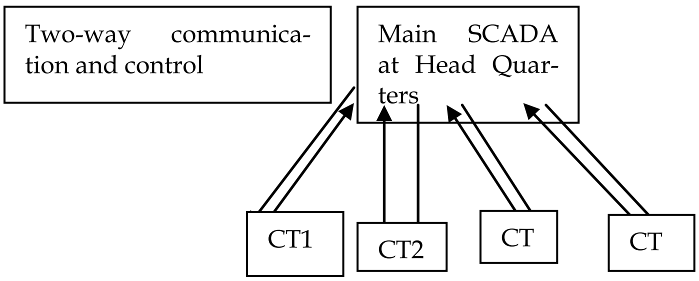

Two-way communication and control
Main SCADA at Head Quarters
CT1
CT2
CT
CT

Figure 6: Overall Framework of Communication in the Proposed Architecture.

The CT would also provide the light source for the fibre optic cable in the network and an automated alarm system unit for the security operatives. The pipelines would be divided in sectors of a fixed manageable length such as 100km or less with a control terminal at each intersection providing monitoring and control function for the section under its control. The system Architecture incorporates an emergency shutdown valve controlled at each control terminal such that in event of observed third party interference that sector can be isolated from the rest of the pipeline network. The wire in the wired/wireless architecture provides the necessary power to the sensors scattered along the entire length of the pipeline, the fibre optic cable provides a mean to detect intrusion or digging as any of the above activities would result in a distortion in the fibre optic cable causing the light transmitted to be reflected or cut-off at the point of intrusion, thus triggering suitable alarm at the CT in charge of that sector. The CT should be manned by system engineers and security personnel comprising of the Army/civil defence to ensure swift response to alarms. Fig 6 depicts a two-way communication and control between the control terminals in the field and the main SCADA at the headquarters of the monitoring agency. There exist redundant control terminals to which each CT in the field reports. The architecture is in such a way that if an unauthorized third party decides to sabotage the system by eliminating a CT in the field, the redundant CT at headquarters automatically assumes control and communicates with the on-field wireless sensor network. It should be noted that sabotaging a field CT could result in loss of power for the fibre optic cable network and the wired/wireless sensors that is solved by incorporating the wireless scheme that is battery powered so it can continue to function independently while an energy/power management scheme such as multi hopping or an agent based scheme can be implemented in the network to conserve battery power thus creating a reliable system that can function according to specification though in degraded performance whenever fault occurs.

4 Conclusion

Nigeria is currently facing great challenges with regards oil bunkering and rising terrorism. Huge losses in revenue abound due to the activities of these hoodlums thus hampering the development of the country. It is imperative that the country finds an optimal solution to monitoring and control of its most important critical infrastructure which is pipelines as it is the most vulnerable to attacks than any other oil installation because it transverse through hard to reach areas. To effectively monitor and control oil pipelines due to their distributed nature and their likelihood to transverse hard to reach areas a fault tolerant monitoring approach was proposed that would improve the longetivity of the system. The proposed system when implemented would go a long way in attempting to solve the malaise of bunkering and vandalism in a way that allows system longevity and easy maintainability by providing data relating to pipelines status irrespective of third party interference method.

6 Future Work

The purposed scheme is robust and flexible as it can be modified or improved further by incorporating Satellite Imaging Technology, video surveillance, GPS etc to the system to address all scenarios that can exist in the field.

7.2 Acknowledgments

The author would like to acknowledge the insight from Proffesor H.C inyiama for his guidiance and fatherly advice during the development of the proposed system especially in the use of a wired/wireless scheme that provided a more realistic way to power the entire system in a fault tolerant manner.

7.3 References

[1]. Wikipedia, What is a Critical Infrastructure Retrieved on August 29, 2013 at http: //en.wikipedia.org/wiki/critical infrastructure.

[2]. C.O.Iwendi and A.R Allen, Wireless Sensor Network Nodes: Security and Deployment in Niger-Delta Oil and Gas Sector, International Journal of Network Security and Its Applications (IJNSA),2011, Vol.3, No.1, pp.68.

[3]. T.Fasasi, D. Maynard and H.Nasr, Sensors remotely monitor wells in Nigeria swamps, Oil and Gas Journal, 2005, pp.2.

[4]. I.F.Akyildiz, W.Su, Y.Sankarasubramaniam and E.Cayirci, A Survey on Wireless Networks, IEEE Communications Magazine, 2002, pp.102-114

[5].] S. Petersen, P.Doyle, S.Vatland, C.S.Aasland, T.C.Andersen and D.Sjong, Requirements, Drivers and Analysis of Wireless Sensor Network Solutions for Oil and Gas Industry, IEEE Communications Magazine, 2007, pp.219.

[6]. [17] G.Sharma, S.Bala, A.K.Verma and T.Singh, Security in Wireless Sensor Networks using Frequency Hopping, International Journal of Computer Applications (0975-8887), 2012, pp.1.

[7]. R. J. Patton, “Fault-tolerant control: The 1997 situation,” in IFAC Fault Detection, Supervision and Safety for Technical Processes, KingstonUpon Hull, U.K., 1997, pp. 1029–1051.

[8]. Adita et al., (2001). ‘Remote Data Acquisition Using Wireless-SCADA’. International Journal of Engineering, 3(1), 224-231.

[9]. Flanker, k (2004) Using Industrial Ethernet in the Oil and Gas Industry, Retrieved on august 21, 2013 at http://www.moxa.com

[10]. I.F.Akyildiz, W.Su, Y.Sankarasubramaniam and E.Cayirci, A Survey on Wireless Networks,IEEE Communications Magazine, 2002, pp.102-114.

[11]. N. Bessani, P. Sousa, M. Correia, N. F. Neves, and P. Verissimo. The CRUTIAL way of critical infrastructure protection. IEEE Security & Privacy, pages 44–51, Nov./Dec. 2008