Wireless Sensor Networks (Wsns) In Industrial Automation: Case Study Of Nigeria Oil And Gas Industry

Fidelis C. Obodoeze[1], Frank E. Ozioko[2], Calista N. Mba[3], Francis A. Okoye[2] And Samuel C. Asogwa[4]
1.Renaissance University Enugu,2.Enugu State University of Science and Technology (ESUT),3.Caritas University Enugu,4.Michael Okpara University of Agriculture Umudike

Abstract

Just recently wireless sensor networks (WSNs) are being widely used in many applications especially in the effort to automate industrial processes and operations. In this paper, we x-rayed different applications of WSNs and actuators in industrial automation efforts, especially in Nigeria oil and gas industry. We also proposed deployment and control architectures for automating monitoring and reporting of oil and gas pipelines vandalisation in Niger Delta region using wireless sensors and intelligent actuators to enhance and improve real-time reporting of incidences of crude oil bunkering and pipeline vandalisation as well as capture the biometric identities of the suspected pipeline vandals in order to lead to their subsequent arrest and prosecution.

1. Introduction

Just recently wireless sensor networks (WSNs) have started receiving great attention in both academia and industry due to their varied useful potential applications in both domestic and industrial applications as a result of their low-cost and miniature size as well as their ease of deployment. In today's competitive industrial market, there are lots of demands on industrial firms to improve on efficiencies, comply with environmental regulations and meet corporate financial objectives [1]. Given the increasing age of many industrial systems and the high cost of acquisition, deployment and maintenance of traditional wired communications in industrial automation systems, low-cost industrial automation systems such as wireless sensors are becoming the today's no.1 choice in order to reduce capital expenditure (CAPEX), operating expenses (OPEX), improve productivity and increase efficiency.

In Nigeria industrialization efforts, the use of wireless sensor networks has started yielding positive and tangible results. This is exemplified by the massive deployment of wireless sensor networks in the last seven (7) years in the Nigeria oil and gas industry by both the International Oil and gas Companies (IOCs) and local oil and gas firms in order to boost crude oil prospecting and production while complying with environmental regulations. Wireless sensors together with other cutting-edge wireless communication technologies have helped in no small measure to automate completely crude oil production and prospecting in the Nigeria Niger Delta region. For instance WSNs help IOCs operating in Niger Delta region such as Shell, Total, Mobil, Chevron, etc in production optimization in the areas of remote monitoring of pipelines, oil wells, oil rigs, flow stations, natural gas leaks, corrosion, H_2S, equipment condition, and real-time reservoir status. Data gathered from wireless sensor nodes enables new insights into plant operation and innovative solutions that improve platform safety, optimize operations, prevent problems, tolerate errors, and reduce operating expenses (OPEX) [2]. According to [3], the applications of wireless sensor networks (WSNs) and other wireless technologies in the automation of oil and gas industries include process monitoring, asset management, plant management, productivity enhancements, Health, Safety and environmental (HSE) monitoring and applications for meeting regulatory requirements. Figure 1 depicts the automation areas or applications in the oil and gas industry using wireless sensor networks. Details of the advantages of these applications in oil and gas automation can be obtained from [4]. Figure 2 depicts the vMBusX-SP model of micro wireless sensor units deployed by one of the major IOCs in Niger Delta region of Nigeria, Shell Petroleum Development Company (SPDC), in January 2005 to help monitor her over 1000 oil wells scattered remotely in Niger Delta region in order to deter vandals from pipeline vandalisation and crude oil theft. Monitoring remote oil and gas locations and devices in Niger Delta oil region is essential for efficiency, safety and security. Figure 3 shows one of over 1000 Shell's oil wells where these vMBusX-SP micro wireless sensor units where installed in the Niger Delta to help monitor status of oil and gas plant and pipelines.

Profit racketeering have led oil pipelines vandals in Niger Delta region to apply desperate measures in order bunker and steal crude oil. These desperate measures of vandals have led to sabotage of the positive efforts of automation of oil and gas pipelines and facility monitoring in the Niger Delta region using wireless sensors. It was reported by [5] that crude oil vandals vandalize both crude oil pipelines and the installed wireless sensors in order to steal crude oil undetected. It was equally observed that despite huge investments by the IOCs to improve on the confidentiality and integrity of the data from the WSN, high cases of vandalisation of wireless sensor nodes by vandals remained unabated [6].This result in the inability of IOCs to receive report of incidences of pipeline vandalisation on time or even not at all while the vandals have the day, since the wireless sensors which are supposed to report the incidences are vandalized first.

.

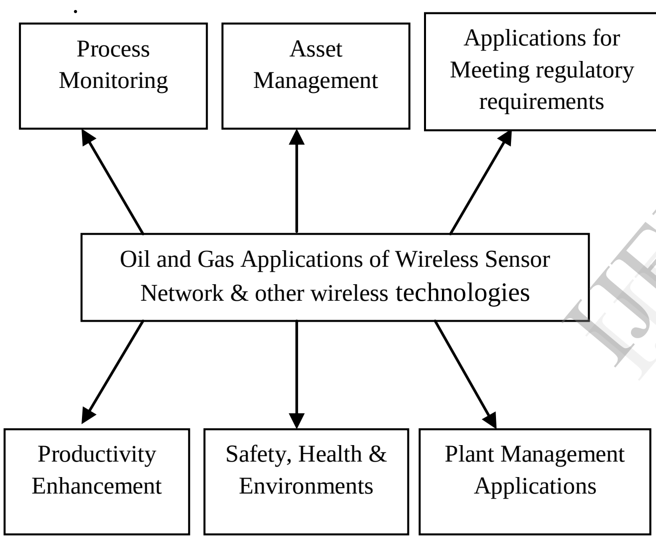

Figure 1. Automation areas of wireless sensor network in oil and gas industry [3]

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 [7]

Figure 3. The vMBusX-SP unit is barely noticeable on this oil well in the Niger Delta, thus providing a feature that helps prevent theft and sabotage [8]

1.1. Contribution of this paper

This paper highlights different automation applications of wireless sensor networks in oil and gas industrial automation and at the end proposes deployment and control architectures using WSNs and intelligent Actuators that can help pre-emptively to prevent pipeline vandalisation by reporting on time to the control room any incidence of pipeline vandalisation as it occurs real-time or by applying intelligent actuator (s) to trigger robotic action(s) to prevent pipeline vandalisation, and proactively to capture and send to control room the biometric recognitions or identities of oil pipelines vandals so that the vandals could be arrested and prosecuted to serve as deterrent to would-be vandals in future.

2. State of the art in Niger Delta oil region

The Nigeria Niger Delta region produces about 2.2 million barrels of crude oil per day apart from liquefied natural gas (LNG) production. Most of the oil fields are scattered in remote swampy areas of Niger Delta and the IOCs operating in the area have spent several billions of dollars in both capital expenditure (CAPEX) and operational expenditure (OPEX) in the provisioning of oil and gas infrastructure to enhance crude oil prospecting and production. Due to the swampy and remote locations of these oil wells it was very difficult in the past for the IOCs to monitor the oil wells and facilities. This led to the personnel of the IOCs to pay regular maintenance and supervisory visits to the oil wells and facilities with armed military escorts because of the high prevalent incidences of kidnapping, pipeline vandalisation and crude oil bunkering in the region. This is because oil and gas production facilities are critical infrastructure and as such can be targets for sabotage and terrorist attacks [9]. Recent advances in wireless sensors and communication systems can be deployed to provide monitoring and surveillance services for these facilities [10] and reduce the number of site visits and onsite personnel required for the operations. Supervisory Control and Data Acquisition (SCADA) solutions provide a base for improved monitoring and management of oil and gas installations such as pipelines, production sites, valve installations, compressor stations and other remote sites [11].

Already these wireless technologies and SCADA have been deployed in the region but incidences of pipelines vandalisation, kidnapping of oil workers and crude oil bunkering continue to be on the increase [6]. This is because the wireless sensor devices that suppose to monitor the oil fields are vandalized first by vandals before targeting the crude oil pipelines in a bid to cover up their criminal acts. Improved versions of SCADA automation, which are digital and smart oil fields, need to be implemented in the Niger Delta oil region to tackle the rampant incidences of oil plant/pipeline vandalisation and crude oil bunkering.

3. Automation System Components

Automation involves the use of processes and sensing systems to provide a complete automatic feedback and control functions for industrial or factory operations or processes. Automation has five basic components and most of the automated systems, plants, operations and machines contain whole or parts of these components or sub-systems. In most generalized form, automation and its components or sub-systems can be identified as the following:

1) *Feedback*
2) *Sensors, Measurements and Recognizing Systems*
3) *Mechanization*
4) *Computer or the controller*
5) *Information and display devices*

Quantitative sensors, transducers, digital oscilloscope and spectrum analyzer can be used to take measurements while qualitative sensors can be used as recognizing systems in industrial automation. Mechanization can be handled using all sorts of mechanical actuators. Computer or the controllers are necessary in order to run the control algorithms for the control of automated operation or process. Information and display devices provide visual interface for the real-time viewing of the reported processes through some sort of Internet Protocol (IP) networks such as Wi-Fi and WiMAX; this is similar to what Supervisory Control and Data Acquisition (SCADA) is doing in oil and gas industry. Qualitative sensors or recognizing systems such as cameras (wireless IP and Closed-Circuit Television (CCTV)) can equally aid in imaging or machine vision to aid actuator-triggered devices such as industrial robots visually to take biometric recognition of objects and send the common operational picture (COP) to the connected wireless IP base stations and finally to the SCADA control room.

Figure 4 shows a typical closed-loop control system with feedback used in most industrial automation efforts.

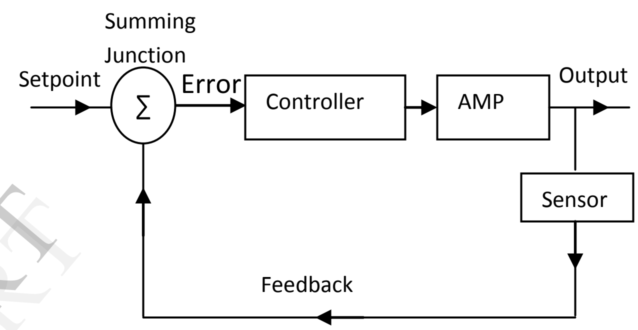

Figure 4. A typical Closed-loop control system with feedback

Figure 5 shows how WSNs can be integrated into other automation devices such as actuators, quantitative sensors, qualitative sensors, controller or the computer, Analog-to-Digital Converters (ADCs), Programmable Logic Arrays (PLA), Remote Terminal Units (RTUs), etc. using Transmission Control Protocol of Internet Protocol (TCP/IP). The TCP/IP makes it possible for the automation devices and the monitored event to be connected real-time to the control room via corporate intranet or internet network as shown in Figure 6.

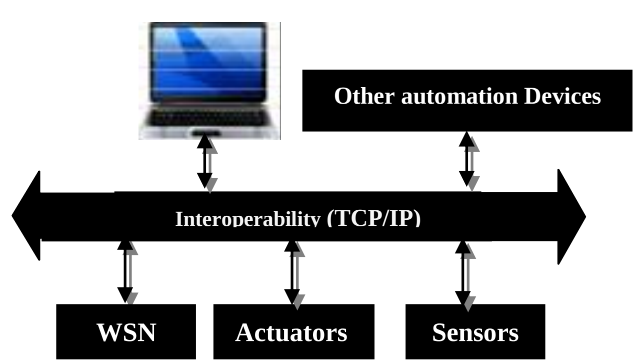

Figure 5. Integration of WSNs into other automation devices

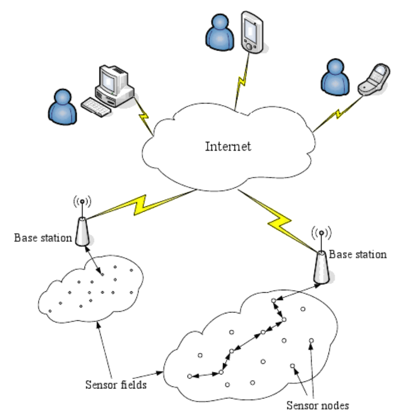

Figure 6. Accessing WSNs-monitored fields through Internet using TCP/IP

4. The roles of sensing and actuation in oil plant/pipeline monitoring and security

According to [12], the effective response to large-scale disasters requires that all participants can rapidly assess all available information. They also need the ability to take action without having to rely on deployed human forces. To achieve these objectives, emergency organizations use different types of sensors to collect information about people, objects, and the environment. Then they can respond automatically to that information with actuators, which are mechanisms that act on devices- for example to turn them on or off, adjust them, or move them. This is a similar situation required in oil and gas industry, especially in Niger Delta region, to monitor oil plants and pipelines using WSNs and take pre-emptive or proactive actions using actuators immediately an incidence of trespass and vandalisation of plant or oil pipelines is detected by the WSNs without human intervention. The pre-emptive response or reaction by the actuators can be to raise an audible alarm or fire a warning gun shot in order to scare away the vandals while the proactive response or reaction may be to capture the biometric identification (facial recognition) of the vandals using low-cost wireless Internet Protocol (IP) cameras or wireless Closed Circuit Television (CCTV) cameras and immediately dispatch the photograph to the SCADA control room enroute a Wi-Fi base station. The photographs or facial recognition of the vandals can be obtained and this will help in their subsequent identification, arrest and prosecution.

Firing a warning shot or raising an audible alarm can also help alert the patrolling vehicles of the Joint Military Task Force (JTF) in the Niger Delta region to apprehend and arrest the culprits. Low-cost wireless IP cameras or wireless CCTV cameras can be deployed in sync with the WSNs to provide these proactive actuator capabilities.

Section 5 describes the deployment architecture for the sensing and actuation functions for oil and gas plant and pipeline safety monitoring in oil and gas industry. Intelligent decision systems can be used to provide the much needed control functions for the effective coordination of the sensor-actuator cooperation. Intelligent system algorithms or Artificial Intelligence (AI) can be fitted into the actuators to make them to act intelligently depending on the inputs from the sensors. Actuators can be turned intelligent robots or intelligent agents. Section 6 describes our proposed intelligent decision system control architecture which can be used to control actuator response to the detection of incidences of vandalisation by the wireless sensors.

5. Our proposed deployment framework for WSN actuators for oil and gas pipeline monitoring

The framework of the proposed WSN-Actuator cooperation to detect oil and gas plant/pipeline vandalisation is depicted clearly in Figure 7. In Block A, the vandalisation of oil and gas pipelines (pressure leakage) are detected by the fitted pressure sensors which passes the data to the wireless sensor network (WSN) which then reports the vandalisation event to the next wireless sensor node using multi-hop shortest route in Block B. In Block C, the vandalisation event is reported to the Actuator (s) by the wireless sensors in Block B. In Block D, the Actuator (s) can then activate the attached wireless IP cameras or wireless CCTV cameras to snap photographs (biometric facial recognition) of the vandals. In finally in Block E, the captured photographs of the vandals from the wireless IP cameras or CCTV are received at the SCADA Control room via the nearest Wi-Fi base station. The facial recognition of the vandals can be used later to apprehend them. Similarly, the Actuator (s) can activate a Robot, using a control algorithm, to fire a warning shot or go physically to capture the criminals as contained in Block D.

Figure 8 also shows the architecture that enables WSN-Actuators and intelligent decision systems such as agents or robots to interact with the monitored environment and feedback data to the control room via mobile Wi-Fi base stations.

According to [13], exploration and production in oil fields is typically a geographically distributed industrial process, monitoring and controlling which is an extremely challenging task. The automation of this task has undergone three major development stages [14]:

computerised (SCADA-based), digital (Internet-based), and smart oil fields.

A traditional SCADA system includes sensors, actuators, remote terminal unit (RTU) or programmable logic controller (PLC), supervisory computer, and communication links. The supervisory computer acquires data from oil production remotely and manipulates the production process through RTU or PLC, which typically have very limited operational capabilities, and as such cannot be considered intelligent systems.

Digital oilfields deploy Internet and web-based SCADA that use the modern Internet technologies to help customers to increase productivity, to improve the flexibility of automation systems, and to minimise the cost of SCADA systems. The core elements of a digital oilfield are web and data servers, wired or wireless communication links that use TCP/IP and Ethernet communication protocols. The scope for applying intelligent data processing techniques is somewhat wider in digital oilfields, but can be done mostly as open-loop control. On-line close-loop control through the use of such technologies as smart sensors, simulation modelling and artificial intelligence can be achieved in the smart oilfields that represent the richest application domain for intelligent condition monitoring and control.

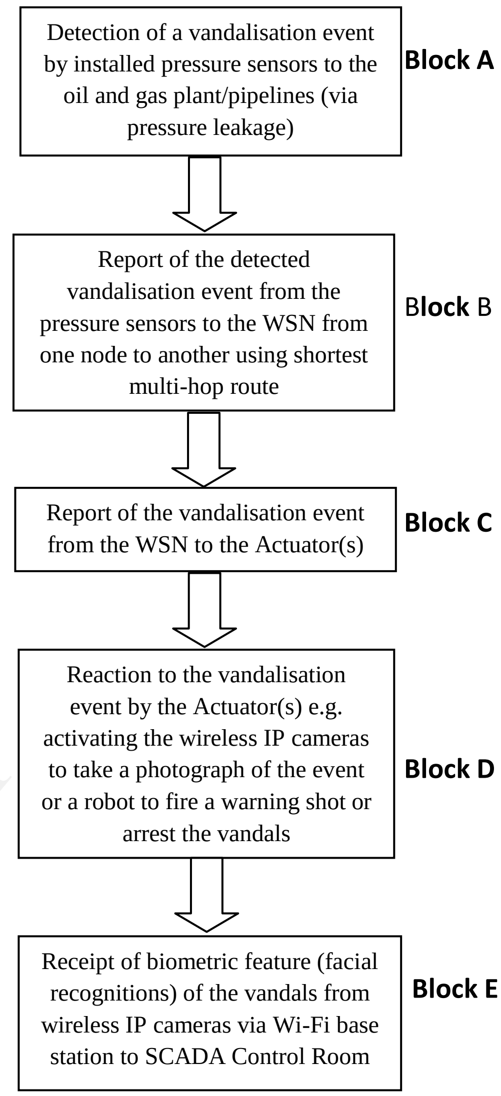

Figure 7. Workflow of the proposed WSN-Actuator cooperation towards apprehending and prosecuting oil and gas plant/pipelines vandals

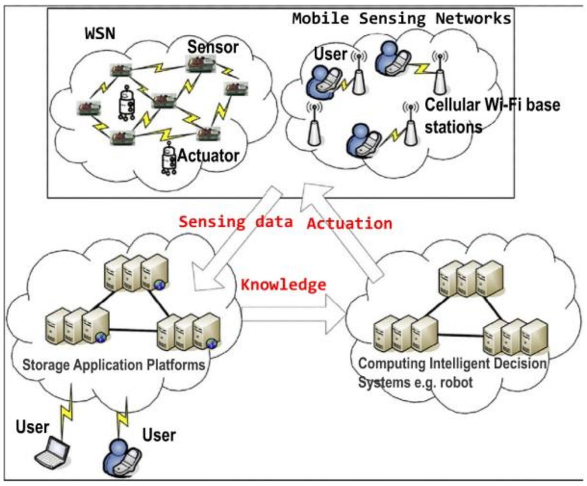

Figure 8. A CPS architecture for deterring vandalisation of facilities during WSN deployment in oil and gas fields (Source from [15])

6. The proposed intelligent control architecture for WSN-actuator cooperation

The intelligent control architecture of the proposed WSN-Actuator cooperation to detect oil and gas plant/pipeline vandalisation is depicted in the closed-loop system block diagram shown in Figure 9.

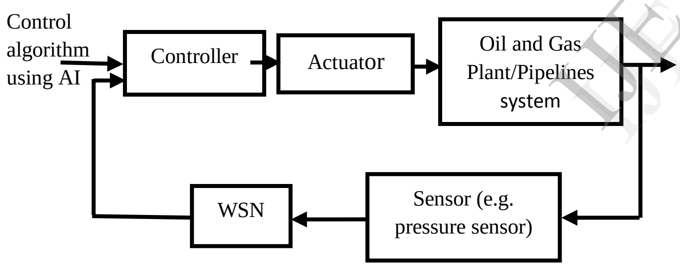

Figure 9. Closed-Loop Intelligent Control structure for the proposed WSN-Actuator cooperation in oil pipeline monitoring automation

Based on the inputs from the WSN and other sensors the controller can run an intelligent algorithm developed using Artificial Intelligence (AI) to control the Actuator to take pre-emptive or proactive action or both in the face of vandalisation event in an oil plant or pipelines. Such proactive actions can lead to the interconnection of the WSN-Actuator network to wireless IP networks to provide Common Operational Picture (COP) to the IOCs at their control room.

7. Conclusion

The massive application of Wireless Sensor Networks (WSNs) in industrial automation has started yielding positive results especially in Nigeria oil and gas sector in the monitoring for safety of crude oil pipelines in the Niger Delta region. However, technology must be improved in order to checkmate the criminal vandalisation of crude oil pipelines by vandals who first vandalize the crude oil pipelines monitors (the WSNs) before vandalizing pipelines in order to bunker crude oil in order to evade detection and arrest.

This paper examined the current spate of crude oil pipeline vandalisation in the Nigeria Niger Delta Region and found out that even the micro wireless sensors deployed by IOCs to monitor crude oil pipelines and report real-time to their base stations and control rooms can be vandalized to give room for bunkering by hoodlums without being detected. This paper therefore made the following contributions to protect both the WSNs and crude oil pipelines deployed in the Niger Delta Oil-rich region in the following ways:

1) We equally introduced an improved security framework that can help detect on time cases of crude oil pipeline vandalisation using the cooperation of WSNs and intelligent Actuators to detect and report pipeline vandalisation on time to the control room real-time or trigger robotic action (s) to pre-emptively discourage pipeline vandalisation and crude oil theft.

2) We identified proactive technological framework that can help in capturing the biometric identities (facial identities) of the vandals using Close Circuit Television (CCTV) cameras and wireless IP cameras which can capture the photographs of the vandals real-time as they try to vandalize crude oil pipelines and send the captured photographs via installed Wi-Fi base station to the control rooms of IOCs in order track and arrest the criminals.

These pre-emptive and proactive technological measures have become necessary in order to curtail the rampant vandalisation of oil and gas plants and pipelines by vandals in the Niger Delta region in order to steal crude oil and make huge profits at the expense of the national economy and that of the IOCs.

10. References

[1] Fieldbus Foundation," Foundation for Remote Operations management-transforming remote applications", 2011, pp.5.
[2] Fasasi, D. Maynard and H.Nasr, "Sensors remotely monitor wells in Nigeria swamps", Oil and Gas Journal, May 2005 pp.4.
[3] J.G.Bhatt, "Wireless Networking Technologies for Automation in Oil and Gas Sector", Electrical Engineering Department Indian Institute of Technology Roorkee, India, 2005, pp.15.
[4] F.C. Obodoeze, H.C. Inyiama and V.E. Idigo, "Wireless Sensor Network in Niger Delta Oil and Gas Field Monitoring: the security challenges and countermeasures", International

Journal of Distributed and Parallel Systems (IJDPS) vol.3, no.6, November 2012, pp.65-66.
[5] F.C. Obodoeze, H.C. Inyiama and V.E. Idigo, "Wireless Sensor Network in Niger Delta Oil and Gas Field Monitoring: the security challenges and countermeasures", International Journal of Distributed and Parallel Systems (IJDPS) vol.3, no.6, November 2012, pp.68.
[6] T.John. "TUC backs NUPENG on alleged JTF's connivance with bunkerers", Daily Sun, Thursday, 16, 2012, pp.10.
[7] T.Fasasi, D. Maynard and H.Nasr, "Sensors remotely monitor wells in Nigeria swamps", Oil and Gas Journal, May 2005, pp.2.
[8] T.Fasasi, D. Maynard and H.Nasr, "Sensors remotely monitor wells in Nigeria swamps", Oil and Gas Journal, May 2005, pp.3.
[9] E.F. Idachaba, "Remote Operation of Oil and Gas production installations in the Niger Delta" Asian Transactions on Engineering (ATE ISSN: 2221-4267) vol. 01 Issue 03, July 2011, pp. 56.
[10] K. Darymli, F. Khan and A. Mohammed, "Reliability of Wireless Sensor network for Oil and Gas Pipeline Monitoring", Sensors and Transducer Journal vol. 106, issue 7, July 2009, pp 6-26.
[11] D. Ehreneich, "Data Reliability and Data Security Considerations for SCADA systems", ENTELEC 2004 www.entelec.org
[12] CISCO Executive White paper, "Cisco Open Platform for Safety and Security: Understand the Sensing and Actuation Architecture Building Block", pp.1-2. Accessed online @ http://www.cisco.com on December 16, 2012.
[13] A. Petrovski, "Intelligent Measurements in the oil and gas industry", Robert Gordon University, Aberdeen, Scotland, July – August 2010, pp. 6.
[14] Z. Sun, X. Tian, "SCADA in oil fields", Measurement + Control, vol. 43/6, July 2010, pp. 176-8.
[15] F. Wua, Y. Kaob, Y. Tseng, "From wireless sensor networks towards Cyber Physical Systems", Elsevier Journal of Mobile Computing, March 2011, pp.7-8.

Authors Profile

Engr. Fidelis C. Obodoeze is a Doctoral Research Student in the Department of Electronic and Computer Engineering Nnamdi Azikiwe University Awka. He is currently lecturing Computer Science and Engineering at Renaissance University Enugu, Nigeria. His PhD work is on Security of Wireless Sensor Network (WSN) in Oil and Gas field monitoring Niger Delta Region. He had his Masters Degree in Control Systems and Computer Engineering at Nnamdi Azikiwe University in 2010 and B.Sc Degree in Computer Engineering at Obafemi Awolowo University Ile-Ife in 2001. He has authored several conference and research journal publications.
All correspondence to Email: fidelisobodoeze@gmail.com

Engr. Frank Ekene Ozioko is the Director of ICT office Enugu State University of Science and Technology (ESUT) and Lecturer Department of Computer and Information Science, ESUT, Nigeria. He had several years of experience in university ICT administration and engineering as well as in teaching and research. **Email:** ekene.ozioko@esut.edu.ng

Dr. Francis A. Okoye is a lecturer and former Head, Department of Computer Science and Engineering Enugu State University of Science and technology (ESUT), Nigeria. He had his Ph.D in Computer Science in 2008 at Ebonyi State University Abakaliki, Nigeria. He obtained his MSc. and BEng. in Computer Science and Engineering at Enugu State University of Science and Technology (ESUT), Nigeria in 2001 and 1996 respectively. He has several years of experience in both teaching and research. **Email:** francisced@esut.edu.ng

Mr. Samuel Chibuzor Asogwa is a Ph.D research scholar in the Department of Computer Science Nnamdi Azikiwe University Awka, Nigeria. He is currently lecturing at the Department of Computer Science Michael Okpara University of Agriculture Umudike, Nigeria. He had his Masters (MSc.) in Computer Science at Ebonyi State University Abakaliki, Nigeria in 2011 and Bachelor of Engineering (BEng.) in Computer Science and Engineering at Enugu State University of Science and Technology (ESUT), Nigeria in 1999. He was the former Acting Head of Department of Computer Science, Renaissance University, Enugu, Nigeria. He has several years of teaching and research experience. **Email**: sasogwa@gmail.com

Engr. Calista Nnenna Mba is a Lecturer and former Acting Head, Department of Computer Engineering, Caritas University Enugu, Nigeria. She is currently pursuing her Ph.D programme in Computer Science at Nnamdi Azikiwe University Awka, Nigeria. She had her MSc. Computer Science at University of Nigeria Nsukka (UNN) in 2009, Nigeria and B.Eng in Computer Science and Engineering at Enugu State University of Science and Technology (ESUT), Nigeria in 2004. **Email**: mbacally@yahoo.com