ISSN 2047-3338

A Proposed Secure Network Model for Implementing Smart Grid Applications in Ghana with WiMAX Technology

E. T. Tchao, K. Diawuo, W. K. Ofosu and I. Ghansah

***Abstract*— Advocates of Smart Grid networks implementation in Ghana believe that Smart Grids will deliver a more secure, sustainable and affordable energy for future generations of Ghanaian consumers. It is also believed that Smart Grids would underlie much of the infrastructure which makes everyday life possible. In order to realize this dream, an Ultra High Frequency (UHF) telemetry system has been used to deploy pilot Supervisory Control and Data Acquisition (SCADA) networks in the urban centres of Accra and Tema as a starting point in implementing a full nationwide Smart Grid Network for the energy generation and distribution sectors of the country. Evaluation of the deployed pilot network showed that the limited coverage range of the UHF system inhibits a full nationwide deployment. The evaluation also found serious security vulnerabilities in the deployed SCADA model. In order to achieve the aim of deploying a secure and ubiquitous intelligent SCADA network which serves as the data processing and collection infrastructure in a Smart Grid network, this paper has proposed a secure SCADA model using WiMAX technology to help improve the efficiency of current energy production, management and distribution sectors of the economy.**

***Index Terms*— Smart Grid, SCADA, WiFi, Security Vulnerabilities and WiMAX**

I. INTRODUCTION

SMART Grid could be referred to as the modernization of the electric power grid for the purpose of enabling bidirectional flows of information and electricity in order to optimize energy production, management, distribution and consumption [1]. Electrical distribution networks are becoming increasingly complex systems. The addition of embedded generation, sustainable energy projects, demand side participation schemes and smart metering require the system operator to gather an unprecedented level of information in real-time from their network [2]. Information Communication Technology (ICT), which is the basis of autonomic and intelligent systems, is being used in the energy sector to deploy Smart Grid networks. Smart Grids are intelligent systems and networks which effectively improve the efficiency of current energy production and also integrate a growing number of renewable sources [1]. Smart Grids provide consumers with diverse choices on how, when, and how much electricity they use [3].

Additionally, Smart Grids aim at providing better power quality and efficient distribution of electricity. Indeed, all these goals cannot be achieved and realized without a communication technology infrastructure that will gather, assemble, and synthesize data provided by smart meters, electrical vehicles, sensors and ICT systems.

SCADA systems, which form the data collection and processing infrastructure of these complex and intelligent networks, are used to control geographically dispersed assets, often scattered over thousands of square kilometers, where centralized data acquisition and control are critical to system operation [4]. In electrical power grids, a SCADA control center performs centralized monitoring and control for field sites over long-distance communications networks, including monitoring alarms and processing status data. Based on information received from remote stations, automated or operator-driven supervisory commands can be pushed to remote station control devices, which are often referred to as field devices. Field devices control local operations such as opening and closing valves and breakers, collecting data from sensor systems, and monitoring the local environment for alarm conditions.

In Ghana, The energy distribution network is undergoing changes to take advantage of the numerous benefits Smart Grids offer. Pilot SCADA networks have been incorporated in the power distribution systems in Accra and Tema, and have been generally successful in providing wide area situational awareness to the distribution company. These networks are gradually altering the distribution network landscape. Where previously, the distribution network could have reasonably been considered a simple unidirectional system delivering power from substation to consumer, now a typical distribution network in the Accra and Tema Municipality is a complex entity with intricate power flows as shown in Fig. 1 and Fig. 2.

E. T. Tchao and K. Diawuo are with the Dept. of Electrical and Electronic Eng., Kwame Nkrumah University of Science and Technology, Ghana

W. K. Ofosu is with the Department of Electrical Engineering Technology, Penn State Wilkes-Barre, USA

I. Ghansah is with the Dept. of Computer Science, California State University, Sacramento, USA

In order to extend the success of these pilot networks nationwide in line with the Government's agenda of building a robust economy powered by an efficient energy sector, this paper seeks to evaluate the deployed SCADA network by looking at the vulnerabilities in the network and the realistic chance of extending the current SCADA model nationwide in a bid to implement a full smart grid network. The sources of vulnerabilities in the network, the limitations of the network model and the proposed solutions have been discussed.

Fig. 1: Accra Power Grid

Fig. 2: Tema Power Grid

II. DEPLOYED SCADA NETWORK MODEL

Electricity distribution companies around the world are at different points in the Smart Grids network life cycle. Some utility companies have begun pragmatically planning holistic networks by applying new enterprise architectures to handle the demands Smart Grid applications will make on their networks [3].

In Ghana however, Smart Grid is a relatively new concept but is believed to be the solution to creating a more efficient and vibrant energy sector. As such, pilot SCADA networks have been deployed in selected cities as a starting point in deploying a nationwide Smart Grid infrastructure to help improve electricity generation, management and distribution.

The deployed SCADA networks under evaluation cover the urban centres of Accra and Tema. The electricity generation and distribution companies, thus Volta River Authority (VRA) and Electricity Company of Ghana (ECG) respectively, are owned by the Government of Ghana. They have a number of primary and secondary substations and power distribution lines interconnecting these stations which supply power to homes and industries within Accra and Tema as shown in Figures 1 and 2 respectively. The benefits of the SCADA network have been enormous. The major benefit of the SCADA network implemented in the Accra and Tema power grids is the network's ability to provide wide area situational awareness to the power generation and distribution companies. This has helped in preventing major power outages in the two cities and has also helped in providing a more reliable energy distribution network.

The deployed SCADA system serves as a monitoring mechanism which makes available in real-time, the current and voltages on each process (transformers and feeders).

It also serves as a control mechanisms which safely and remotely control circuit breakers, relays and isolators in the network.

The implemented SCADA systems hardware can be broken down into the following five major categories as shown in Fig. 3. These categories are:

- Field level instrumentation and control devices
- Remote Terminal Units (RTUs)
- Communications system
- Master stations
- Data processing computer system

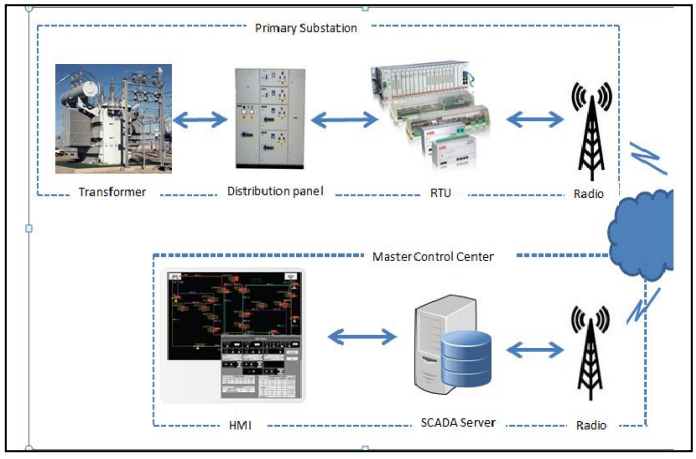

Fig. 3: Deployed SCADA hardware Architecture

A Professional Mobile Radio (PMR) system, which is a dedicated mobile communications system, is used by the

utility company to provide wireless connectivity to the field devices from the Base Station. This UHF scanning telemetry system typically offers 9.6 - 19.2 kbps throughput.

When the Government extends the success of the pilot SCADA networks to other cities and towns in the country, devices will become more dispersed in wide areas. Compliance of requirements to meet standards will become increasingly challenging. Interdependencies between computer communication systems and the physical infrastructure will also become more complex as information technologies are further integrated into other devices and networks as seen in Smart grids deployment in other countries [5]-[7].

Moreover, in assessing the feasibility of any wireless system, the range of coverage from a Base Station and the individual and aggregate throughputs are critical parameters. Although UHF scanning telemetry systems can be established without line of sight, experience in the pilot SCADA network suggests that adequate performance in range and throughput can only be achieved with line of site (LOS) of the field devices with the Base Station.

Latency of the UHF Telemetry system is of the order of seconds. Smart Grid network design parameters are specified in Table 1. In the implemented SCADA model, devices are polled in series and taking into consideration the specified parameters in Table 1, the UHF scanning telemetry system may be too slow for real-time control applications when the network size grows exponentially.

Table 1: Smart Grid network design parameters [8]

Use Case	DL (kbit/s)	UL (kbit/s)	Latency (ms)
Wide Area Situational Awareness (WASA)	1.0	5.0	1000
Monitoring	10	300	100
Control	1.0	5.0	100
Protection	150	150	20
Metering Regional Collector	5.0	64	1000
Remote Site Communications	500	500	100
Direct 4G Smart Metering (AMI)	0.5	1.0	5000

From Table 1, the UHF system cannot provide the required bandwidth to support vital Smart Grid applications and as such an alternative microwave access technology which offer greater bandwidth, reliability and extended coverage range is needed for a successful nationwide deployment.

Field trial measurements of WiFi and 3G systems carried out in outdoor locations within the pilot network showed these two systems do not have the capacity and range to help deploy these complex systems [9]. Fortunately, the Government of Ghana has successfully deployed a Fourth Generation World Wide Interoperability for Microwave Access (4G-WiMAX) network in Accra and Tema for implementing Electronic Governance applications. These WiMAX networks have been extended to other cities in the country as shown in Figure 4 with the aim of providing ubiquitous coverage to enable Electronic Governance applications reach remote parts of the country.

Performance evaluation of these deployed networks measured 1Mbps at 5km away from the Base Stations [10]. Fortunately, the deployed WiMAX networks are widely being underutilized [11]. This makes WiMAX the best microwave access technology for deploying a nationwide Smart Grid system since Long Term Evolution (LTE) systems have not been deployed in the country yet.

WiMAX has the reliability, capacity and coverage range to provide ubiquitous coverage to the increasing number of devices which will be located in wide and remote areas. This will drastically reduce the initial cost of Smart Grids deployment since there will be no need to set up new PMRs in various cities and towns.

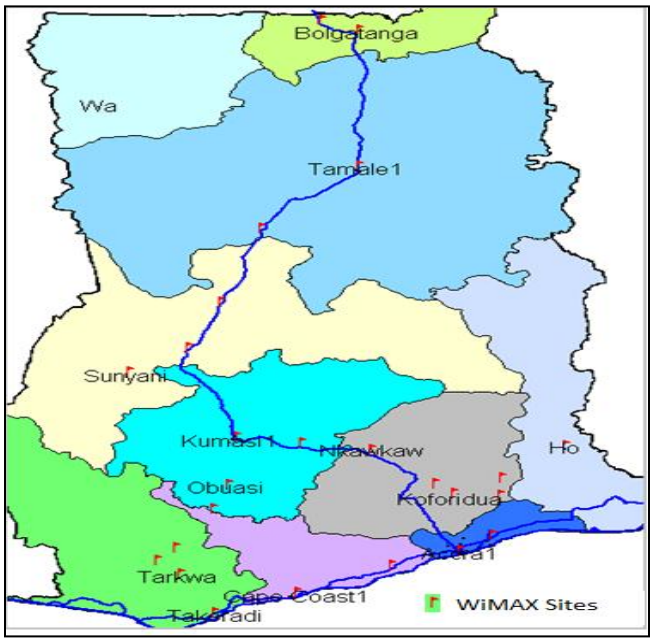

Fig. 4: Major Cities and Towns on the Electronic Government WiMAX network

III. VULNERABILITY ASSESSMENT OF THE DEPLOYED WIMAX NETWORK

Security for control and data acquisition systems is a significant and current concern [12]. Best practices for secure control system design [13]-[17] generally call for a control system network to be logically separated from the corporate network devices.

However, data and control traffic in the deployed model as shown in Fig. 5 is carried by the same networking infrastructure that carries other corporate traffic. As such, direct applications of traditional best practices for these control systems' security have not been adhered to.

Vulnerability assessment of the deployed network found no Virtual Local Area Network (VLAN) segregating the SCADA network from the corporate network. There was no logical or

physical separation and this exposes the main SCADA Servers to the corporate TCP/IP network.

Moreover, administrator credentials of the SCADA servers are commonly known to most of the workers at the Network Operation Center. Passwords being used for administrative accounts on the SCADA servers, databases and network devices were easily guessable and very weak.

There is also the issue of one-way authentication in the deployed UHF network where only the Base Station authenticates the field equipment. This makes the field devices vulnerable to rogue Base Stations. Moreover, UHF communication systems are vulnerable to traffic analysis, a technique that allows the attacker to determine the load on the communication medium by monitoring and analyzing the number and size of packets being transmitted.

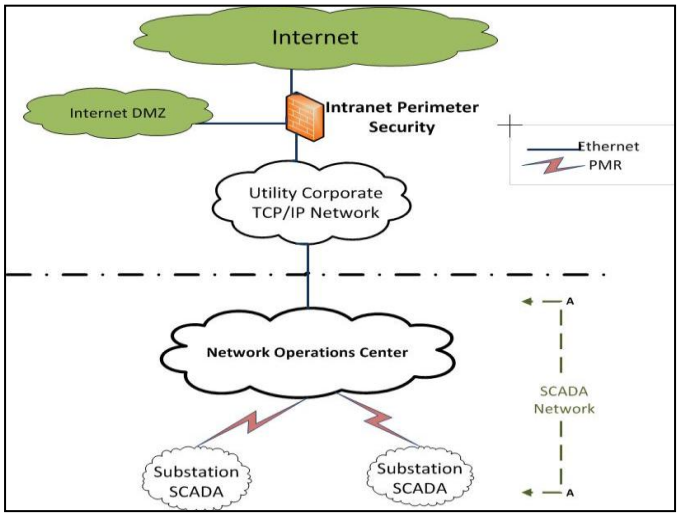

Fig. 5: Deployed SCADA Communication model

Because UHF communication systems are susceptible to passive and active eavesdropping, an attacker can listen to the wireless connections in the SCADA network as well as actively inject messages into the communication medium.

In addition, threats in wireless systems in general focus on compromising the radio links. Hence, these systems are also vulnerable to radio frequency (RF) jamming. It implies, the UHF system is susceptible to scrambling attacks, where an attacker injects RF interference while transmitting specific management data. RF interference affects proper network ranging and bandwidth sharing capabilities of wireless systems [18]. The effect of the limited coverage range, which is a denial of service caused by RF interference in the UHF system has been illustrated in the coverage simulation in Fig. 6.

SCADA devices which will be in the coverage range of the rogue Base Station will be denied access and this could be very disastrous.

These identified security vulnerabilities in the SCADA

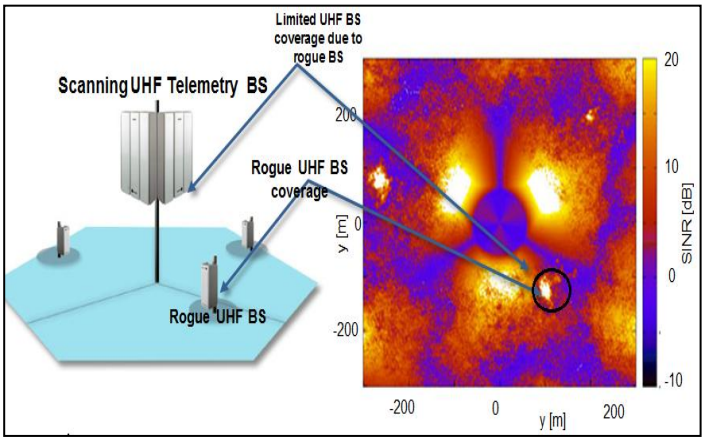

Fig. 6: UHF RF Jamming Scenario Simulation

network could seriously affect a full Smart Grid integration of the electric power grid. Millions of dollars have been spent on deploying these networks but apathy which could be attributed to the false notion that the SCADA networks are physically isolated from the corporate offices makes this critical national infrastructure vulnerable. These major security issues need to be addressed as there are plans to put more critical national infrastructure on the grid.

IV. PROPOSED SECURE NETWORK MODEL

The Government of Ghana has a major objective of improving the existing energy generation, transmission and distribution grids through the introduction of smart devices and a communication network, deployed on top of the electrical infrastructure which will enable real-time interactions among the devices, systems and operators. The aim of providing high quality energy in Ghana in the context of increased variability and complexity of the electric system requires a suitable control infrastructure based on more pervasive and secure ICT solutions into the whole electrical generation and supply chain as specified by the NIST Smart Grid conceptual model shown in Fig. 7.

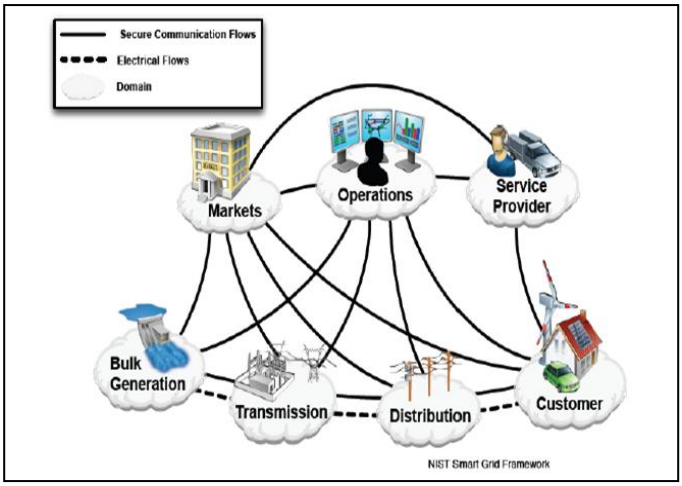

Fig. 7: NIST Smart Grid conceptual Model

A logical isolation is proposed between the SCADA and corporate TCP/IP networks by using a securely configured bridge acting as a control network perimeter security as proposed in [13], [19].

Role based access control is also recommended among the staff at the Network Operation Center of the utility company. The bridge must be securely configured and at least a 12 character password consisting of upper cases, lower cases, numbers and special characters is also recommended

WiMAX has been used as the microwave access technology for the proposed SCADA model in Figure 8 because it enables mutual authentication by both Subscriber Stations and Base Stations. This will help significantly in solving the threat of an attacker setting up rogue Base Stations and transmitting information to the field devices.

WiMAX also has extended coverage and greater Bandwidth capacity as compared to the UHF telemetry system. Eleven WiMAX Bases Stations have been used to provide ubiquitous coverage for the urban centres of Accra and Tema as shown by the coverage simulation in Figure 9 using an adaptive 4x4 Multi-Input Multi- Output (MIMO) antenna configuration.

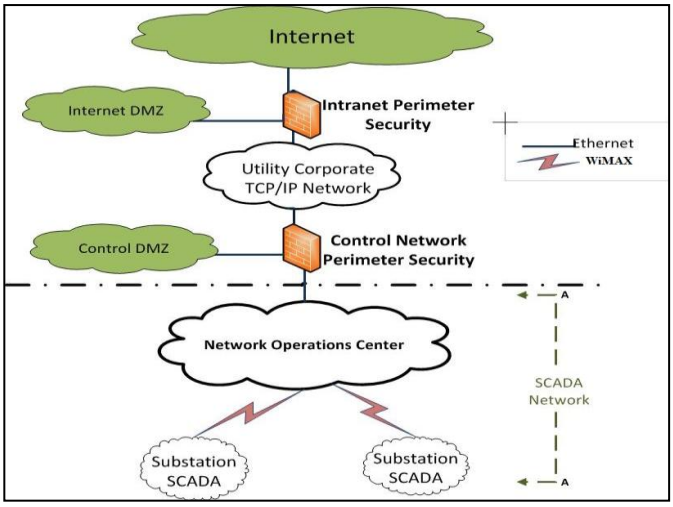

Fig. 8: Proposed Communication model for the deployed SCADA network

The existence of these WiMAX networks deployed by the Government in major cities and towns provide both technical and economic advantages. This makes such a proposal very feasibly. The distribution company can operate a Virtual Private network (VPN) over the WiMAX networks all over the country. It is possible for the utility companies to emulate a LAN over the open connections of the WiMAX network, creating virtual circuits.

The VPN eliminates the need for an expensive region by region roll-out and also allows for tunneling over other media. This makes the network communications fully transparent to the SCADA application. This will also help provide a logical separation of the communication system from the corporate TCP/IP network.

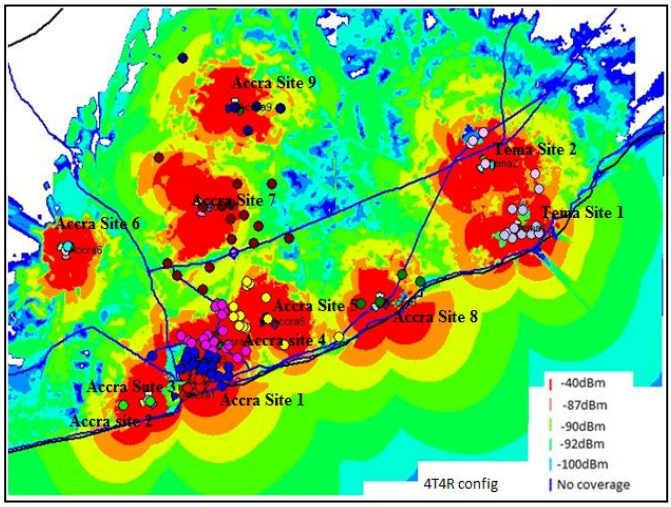

Fig. 9: Coverage Simulation of the Accra and Tema WiMAX sites [9]

The use of inverse multiplexing or network striping is proposed in the case of RF jamming. This technique will allow the construction of a high bandwidth virtual channel from a collection of multiple low bandwidth network channels. Control and data information could be sent via alternate channels with the applications on the alternate channels being oblivious of the way in which data and control information are routed to specific network channels. This is very appropriate for the SCADA applications in case the specified operating frequency of the WiMAX network is jammed.

Because the locations of some of the field devices are isolated, it is recommended that these Remote Terminal Units are physically protected.

V. CONCLUSION

Community benefits of a nationwide Smart Grid implementation in Ghana will be enormous. A journey of a thousand miles begins with a step and as such, the utility companies in Ghana have started with pilot implementation of SCADA networks in the energy generation and distribution sectors. Vulnerability assessment of the pilot networks has shown immediate concerns revolving around the security of this critical infrastructure.

UHF systems which are currently been used have serious security vulnerabilities, low throughput and limited coverage range and would be overwhelmed given the task of providing communication service to the volume of devices needing connections which will be installed on the power system in the medium to long term.

WiMAX technology has been proposed as the microwave access system for deploying the nationwide Smart Grid network because of its extensive coverage, reliability and capacity. WiMAX networks have already been deployed by the Government and this eliminates the tendency of deploying new PMRs in cities and towns to achieve the nationwide

Smart Grid deployment objective. A Virtual Private Network (VPN) operating over the WiMAX network has been proposed to provide the logical isolation the network needs.

REFERENCES

[1]. Christine Hertzog, Liz Ude, and Douglas Stuart, "Smart Grid Dictionary" 2nd Edition, 16 June, 2010.

[2]. Securing an Integrated SCADA System; Network Security & SCADA Systems Whitepaper, Published April 2007

[3]. Andrew K. Wright, Paul Kalv and Rodrick Sibery: "Interoperability and Security for Converged Smart Grid Networks"; Grid-Interop Forum proceedings, published 2010

[4]. Pertti Järventausta, Sami Repo, Antti Rautiainen, Jarmo Partanen: "Smart grid power system control in distributed generation environment", Annual Reviews in Control, Volume 34, Issue 2, December 2010, pp. 277-286

[5]. Gurlin Singh Lamba:" Smart Grid and its Development Prospects in the Asia-Pacific Region", Journal of Emerging Trends in Computing and Information Sciences, Vol.2, No. 1, pp. 62-66, January, 2011.

[6]. ISO New England, "Overview of the Smart grid – Policies, Initiatives and Needs", February 17, 2009.

[7]. Leonardo Meeus, Marcelo Saguan, (2011) "Innovating grid regulation to regulate grid innovation:From the Orkney Isles to Kriegers Flak via Italy", Renewable Energy, Volume 36, Issue 6, June 2011, pp.1761-1765.

[8]. Requirements for Smart Grids, "WiMAX Forum System Profile Requirements for Smart Grid Applications", WMF-T31-002-R010v01; WMF Approved (2013-02-05)

[9]. E.T. Tchao, W. K. Ofosu and K. Diawuo; "Radio Planning and Field Trial Measurement of a Deployed 4G WiMAX in an Urban Sub-Saharan African Environment ", conference proceeding, IEEE Wireless Telecommunications symposium, 17-19 April, 2013, Phoenix, Arizona

[10]. E.T Tchao, W.K. Ofosu and K. Diawuo; "On the Comparison Analysis of Two 4G-WiMAX Base Stations in an Urban Sub-Saharan African Environment", Journal of Communication and Computer, Vol. 10, No. 7, July, 2013

[11]. E.T Tchao, W.K. Ofosu and K. Diawuo; "A Performance Case Study of Electronic Governance Implementation in Ghana with WiMAX Technology", International Journal of Computer Applications Volume 71-No. 14, June 2013.

[12]. Stouffer, Falco, Scarfone, Guide to Industrial Control Systems (ICS) Security, Draft, National Institute of Science and Technology SP800-82, Sept. 2008.

[13]. The Smart Grid Interoperability Panel, Cyber Security Working Group, Guidelines for Smart Grid Cyber Security, Volumes 3, National Institute of Science and Technology NISTIR 7628, Sept. 2010.

[14]. Idaho National Laboratory, Control Systems Cyber Security: Defense in Depth Strategies, Homeland Security External Report No: INL/EXT-06-11478, May 2006.

[15]. NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks, National Infrastructure Security Coordination Center, London, 2005.

[16]. TR99.00.01: Security Technologies for Industrial Automation and Control Systems, ISA, 2007.

[17]. David Laverty, D. John Morrow, John O'Raw and Peter A. Crossley: "Wireless Telecoms for Distribution Networks Based on WiMAX"; 20th International Conference on Electricity Distribution, Prague, 8-11 June 2009, Paper 0856.

[18]. Gee Rittenhouse: "A 1000X of data - Technology Directions in the Wireless market", Conference proceeding, IEEE Wireless Telecommunications symposium, Phoenix, Arizona, 17-19th April 2013.

[19]. Guide to Security for Worldwide Interoperability for Microwave Access (WiMAX) Technologies, NIST SP800-127.