Migrating from Closed to Open Supervisory and Data Acquisition(SCADA) System: A Case Study of Transmission Company of Nigeria(TCN)

Awodele Oludele
Department of Computer Science
Babcock University, Nigeria
awodeleo@babcock.edu.ng

Kuyoro 'Shade
Department of Computer Science
Babcock University, Nigeria
afolashadeng@gmail.com

Alade Akinwumi
Department of Computer Sc.
Babcock University, Nigeria
akinalade2000@gmail.com
Corresponding author

Abstract— Supervisory Control and Data Acquisition (SCADA) Systems are used to control and monitor physical processes in real time. It is specifically applied to monitor and control activities from remote end covering a wide geographical area. Examples of SCADA application are found in control and supervision of devices behavior in transmission of electricity, transportation of gas and oil pipelines, water distribution, traffic lights and other systems used as bases of modern society. Transmission Company of Nigeria (TCN) SCADA System, being a closed system seems to be free from external threats, except perhaps the insider intrusion. In Nigeria, electricity industry deregulation has commenced and Independent Power Producers (IPPs) now generate electricity into TCN Grid. There are also bulk electricity traders buying electricity for sale through TCN network. Data from these new entrants into the industry would be remotely acquired through integration with TCN SCADA System. Integration with the existing SCADA System of TCN would likely be through public communication Network and internet, etc. Migrating from a fairly secure closed SCADA System to an open SCADA System comes with its security challenges. This paper examines the distinguishing characteristics of closed (isolated) and open (exposed) SCADA System using the Transmission Company of Nigeria as a case study.

Index Terms — Protocols, Remote Terminal Units (RTU), Security, Supervisory Control and Data Acquisition **(**SCADA) System.

1 INTRODUCTION

INDUSTRIAL Control System (ICS) is a general term for term for Supervisory Control and Data Acquisition tion (SCADA) Systems, Distributed Control Systems (DCS) tems (DCS) and Programmable Logic Controllers (PLC). SCADA Systems, however, differ from DCS which are generally confined within a factory floor or plant. SCADA Systems are used for geographically dispersed assets. The Transmission Company of Nigeria SCADA System covers the entire country.

SCADA Systems are typically deployed in three main areas (FORNET INC.) [1]:

1. **Industrial process management** – manufacturing, production, chemical processes, power generation, fabrication, and refining industries.
2. **Infrastructure management** – water treatment and distribution, waste water collection and treatment, oil and gas pipelines, electrical power transmission and distribution, large communication systems.
3. **Facility management** – offices, data centers, airports, ships etc; monitor and control High Voltage AC (HVAC), physical access, and energy consumption.

Processes in the fields are monitored and controlled remotely as sensors in the Remote Terminal Units (RTUs) or Intelligent Electronics Devices (IEDs) or Programmable Logic Controllers (PLCs) gather analogue data, alarm, failure indication, etc, digitalize the input and forward same to SCADA System servers. The data is compiled and formatted into form suitable for control room operation using a Human Machine Interface (HMI) to make supervisory decisions to over ride normal Remote Terminal Units (RTUs). The data may also be collected and stored.

TCN SCADA Systems is proprietary and operates on proprietary protocol for its communication. Like any SCADA System, it monitors and controls hundreds of input/output points. (Henta) [2].

With deregulation of electricity in Nigeria, an open market that allows investors to participate in power generation and distribution is exposing TCN SCADA System to potential vulnerability to attacks. As each investor integrates his Information Technology (IT) System with TCN SCADA System using open communication protocols, the TCN Transmission SCADA System would no longer be a protected closed network. It is intended to examine the distinguishing characteristics of closed and open SCADA System using the Transmission Company of Nigeria as a case study.

1.1 Related Works

Security is a major concern when a SCADA System migrates from closed to open system. It is exposed to both enterprise network of the host organization as well as other utility SCADA systems that are integrated with it.

Several researches have been conducted on this subject matter. Nordström [3], in his paper Assessment of Information Security Levels in power communication systems using Evidential

Reasoning, presented a framework for assessing information security in power communication systems.

Hentea [2], in her paper, Improving Security for SCADA Systems, provided an analysis of key development, architecture, potential vulnerabilities and security concerns including recommendations towards improving security of SCADA System. Choi et al. [4], in their paper entitled Advance – key Management Architecture for Secure SCADA Communications, opined that any damage to SCADA System can have a wide spread negative effect to society'. They went further to investigate whether the existing key-management protocols for SCADA Systems satisfy some requirements. The paper proposed advance key-management architecture fitted for SCADA communications.

Hahn et al [5], in their paper entitled An Evaluation of Cyber Security Assessment Tools on a SCADA Environment, researched into whether the methodologies and tools commonly used for traditional Information Technology (IT) systems are sufficient for the cyber security assessment needs in power systems. The paper reviewed these assessments.

Axelrod [6], in the paper entitled, Applying Lessons from Safety-critical Systems to Security-critical software, examined Systems across the full spectrum of criticality – from non-critical through security critical and safety-critical systems, in terms of how they are engineered, i.e. looking at the processes by which they are designed, built, deployed, operated, modified and decommissioned. He also discussed some of the demanding methods applied to strengthen safety-critical systems.

None of these papers examined an existing SCADA System as a case study. The purpose of this paper among others is to bridge the identified gap by using the Transmission Company of Nigeria SCADA System as a case study.

2 METHODOLOGY

This work is basically explorative. The approach adopted involved identification of the features of a closed SCADA System through the literature and by using the Transmission Company of Nigeria (TCN) SCADA System as a case study. The researchers further examined the distinguishing characteristics SCADA System.

2.1 Typical Closed SCADA System Architecture

Fig. 1 presents a pictorial representation of the components of a closed SCADA System. It basically consists of the Field and the Master Station equipment. While sensors/actuators and Remote Terminal Units (RTUs) form the field equipment, the Master Terminal Units and the other servers are in the SCADA Master Station. Communication links, such as Optic Fibre, microwave radio, telephone lines, etc are the bridges between the field and the SCADA Master station.

The field equipment that are sited in a wide geographical area through communication network and the master station SCADA servers represent a typical closed SCADA System. It is closed (isolated) as it does not interact with the utility Enterprise network (intranet LAN), internet or SCADA Systems of the Independent Power Producers, Distribution companies, etc.

A SCADA System performs four functions (SIEMENS) [7]:

1. **Data Acquisition**: Hundreds of sensors in the SCADA System measure inputs into the System such as state of a device – either 'on' or 'off'; trip wire alarms, like a power failure; changes in voltage or current of a field device; voltage level of batteries, temperature threshold alarm. The sensors' inputs are encoded into protocol format by the RTUs which then forward them to the SCADA master. Hence, RTUs are interface between the sensors and the SCADA masters.
   In turn the RTUs receive control commands in protocol format from the master and transmit electrical signals to the appropriate control relays.
2. **Data Communication**: Early SCADA networks communicated over radio, modem or dedicated serial lines. Today the trend is to put SCADA data on cyber network. This will, however, expose the SCADA System to the internet with attendant vulnerability.
   The SCADA System would then become open as would be discussed later. Communication link by optic fibre is generally widely used today because of its various advantages which include low attenuation and wide bandwidth. SCADA data is encoded in protocol format as SCADA Systems do not communicate with just simple electrical signals. Protocol commonly used in SCADA System are Modbus, Profibus and Distributed Network Protocol (DNP3). (Powell). [8].
3. **Data Presentation** – A SCADA System reports to human operators over a specialized computer that is variously called a master station, a Human Machine Interface (HMI) or as Human-computer Interface (HCI). The SCADA master station has several different functions. It continuously monitors all sensors and alerts the operator when there is 'alarm' – that is, when a control factor is operating outside its defined boundary. It also performs data processing on information gathered from sensors, maintaining report logs and summarizes historical trend.
4. **Control** - SCADA System, through the master unit, automatically regulates all kinds of industrial processes. For example, electricity production can be adjusted to meet demands on the power grid. A full-scaled SCADA System can adjust the managed sys

tem in response to multiple inputs.

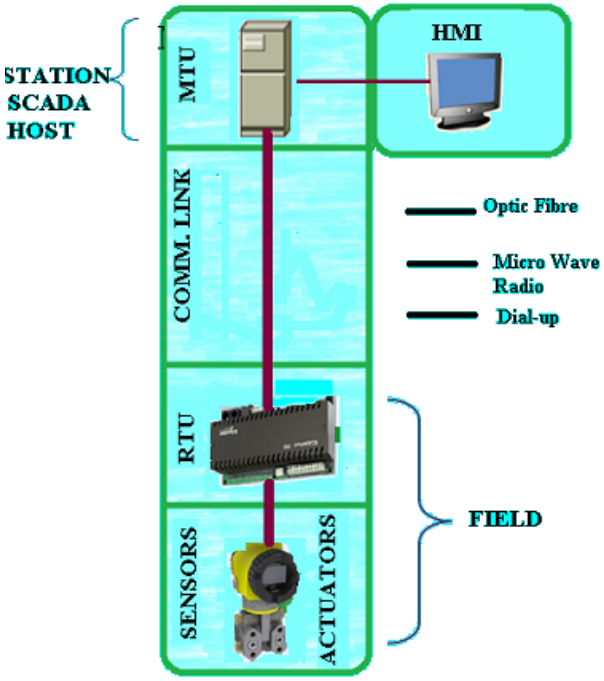

Fig. 1 Pictorial Representation of SCADA Architecture
Source: Powell [8]

.

Four components perform these functions as shown in Fig. 2. These are:

1. Sensors (either digital or analog) and control relays that directly interface with the managed system.
2. Remote Terminal Units (RTUS) – These are small computerized units deployed in the field at specific sites and locations. RTUs serve as local collection points for gathering reports from sensors and delivering commands to control relays.
3. Communication Network: It is the medium through which signals from the RTUs are transported to the SCADA Master Terminal Unit using communication means such as optic fibre, microwave, dial-up, etc.
4. SCADA Master Units: Also called Master Terminal Unit (MTU). These are larger computer consoles that serve as the central processor for the SCADA System. Master Units provide a human interface to system and automatically regulate the managed system in response to sensor inputs. It is connected to the RTUs in the field by the Communication network

2.2 TCN SCADA System as a Typical Closed System

TCN SCADA System uses software called SINAUT Spectrum by SIEMENS Company. It is a proprietary SCADA Software. The word 'SINAUT' stands for SIEMENS Automation. The software is based on up-to-date hardware for servers and workstations which use a UNIX operating system environment. UNIX offers a powerful programming environment that provides users access to a very large spectrum of application programs such as editing and text formatting tools. A specific advantage of SINAUT Spectrum is its capacity to distribute tasks over several servers and workstations. With this feature, high computer performance and larger main and external memory capacities are available.

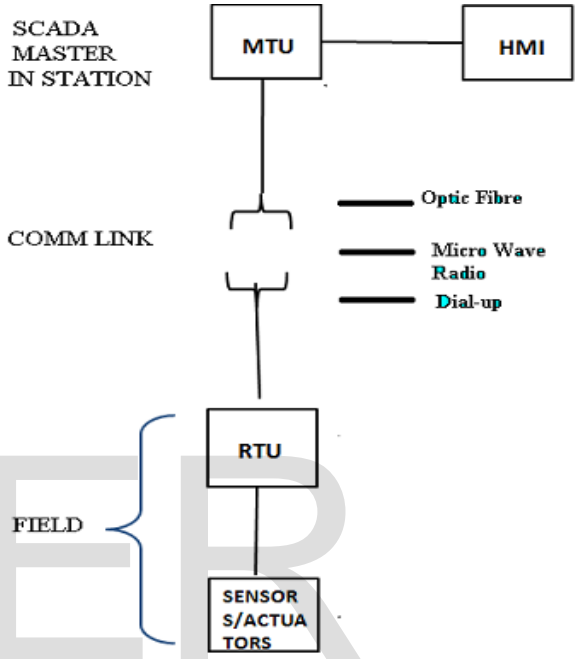

Fig. 2 Block Diagram of SCADA Architecture

Source: Powell [8]

Fig.3 below depicts the structure of SINAUT Spectrum software. There are 4 layers.
The inner most layer is UNIX operating system which is installed on each server and workstation that make up the SCADA System. Next to the innermost layer are the System programs developed by using the UNIX utilities. UNIX utilities are programs and commands which communicate with the operating soft bus/Database access System in the third layer while the fourth layer is the SCADA and EMS (Energy Management System) where SCADA operators perform his supervisory, data acquisition and control.

2.3 Architecture of TCN SCADA System

The TCN SCADA System Architecture is shown in fig. 4.

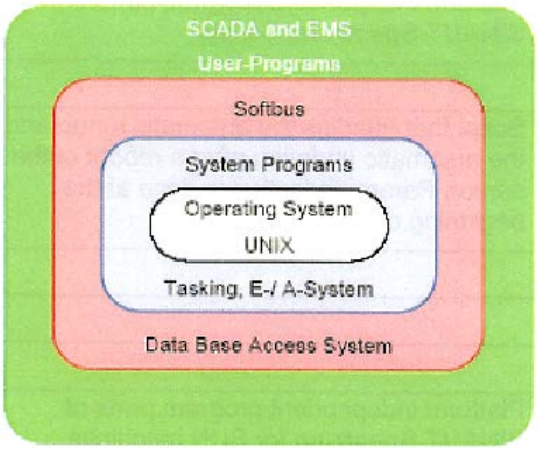

Fig. 3: Structure of SINAUT Spectrum Software
Source: SIEMENS [7]

It consists of the Field Device and the Process supervision/control layers. In the figure, RTU represents the lowest layer where the field devices are monitored. Data gathered from the field is transported through communication media with the aids of appropriate protocols.

The data is collated further on the DAS Server in the Process supervision/control layer. The following are the functions of the servers installed in the Process/control layer:

COM Server (Communicator) – It performs data processing and supervisory control.

ADM Server (ADM/HFD) – This is the database for all servers. Other servers are updated by the ADM Server. It also performs Historical and Future Data (HFD) management.

MMI (Man Machine Interface) – It mainly provides visualization and operator control functions for the network control system. It also provides various workstation services such as word processing, calendar management, spreadsheet, etc.

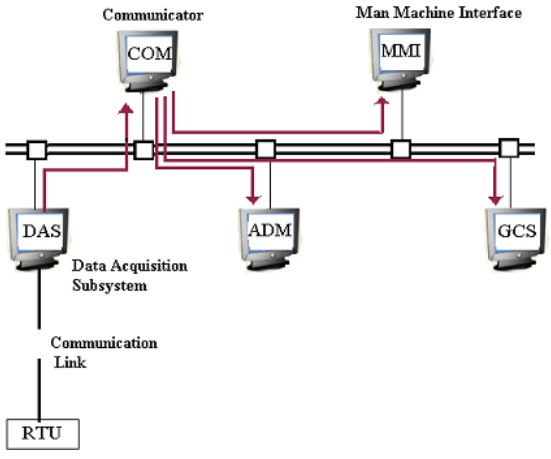

Fig. 4: TCN SCADA System Architecture
Source: SIEMENS [7]

Data Acquisition Server (DAS) – a subsystem for data gathering from the field.

Generation Control Server (GCS) – It performs control and scheduling of system generation.

2.4 Feature of Open SCADA System Architecture

Fig.5 below is a schematic diagram of an open SCADA System as conceptualized for the deregulated electricity industry in Nigeria.

It depicts integration of SCADA System of other electricity companies (Distribution and generation) with the existing closed (isolated) SCADA System of the Transmission Company of Nigeria using communication media such as optic fibre, microwave, high tension power lines, etc. These external SCADA Systems of other independent power producers and distributors of electricity must interact with the TCN System by virtue of electricity deregulation in Nigeria.

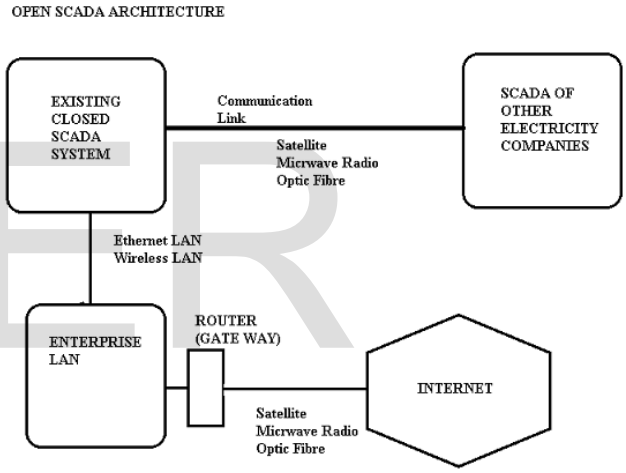

Fig. 5: Block diagram of a Typical Open SCADA System
Source: Alade [9]

Integrated with the same existing SCADA System is the Transmission Company's Enterprise LAN which through router gateway is connected to the internet.

3 DISCUSSIONS

In power system, integration of several utilities' equipment has the advantages of having

- a robust, stable, reliable and efficient interconnected network
- an economic system
- a resource sharing mechanism with the enterprise computers network and other utilities' SCADA systems

A major draw- back of an open SCADA System is its vulnerability to both internal and external threats as highlighted in the literature review.

How to secure 'safety and security-critical infrastructure' such as electricity generation, transmission and distribution equipment and building is stimulating a lot of researches recently.

As shown in Fig. 4, an open SCADA system is vulnerable to attacks from three main fronts – Fig. 5):

a. Enterprise LAN network and the closed SCADA system through the field sensors, actuators and measurands connected to the RTU and linked by communication to the master station.
b. Internet – cyber attack
c. External SCADA systems

4 Conclusion

Exposure of TCN SCADA System to enterprise LAN and integration with other SCADA systems for any reason automatically changes its status. Its defense system becomes vulnerable as an open SCADA system.

There have been several researches on SCADA system security with emphasis on building of firewalls against external attacks and general cyber security.

However, research gap has been identified in area of possible attacks from the field sensors and actuators connected to the Remote Terminal Units (RTUs) – Fig. 2. Target of such attacks will be the communication protocol between the RTU and the Master Terminal Unit (MTU). Common protocols used for SCADA system include Profibus, Modbus and Distributed Network Protocol 3 (DNP 3). These protocols vary in their complexities and vulnerability, hence comparative investigation of their vulnerabilities, threats and appropriate defence is recommended for further works.

Acknowledgment

The authors wish to thank the Management of the Transmission Company of Nigeria for availing the researchers the use of the company's document on SCADA System hosted at the National Control Centre, Osogbo, Nigeria. The researchers also appreciate a few colleagues at Babcock University, Nigeria for their inputs into the work.

References

[1] FORTINET Incorporated, "Securing SCADA Infrastructure", White paper, WP-SCADA-R1, 201010, 2010.

[2] M. Hentea, "Improving Security for SCADA Control Systems", Interdisciplinary Journal of Information, Knowledge and Management, 3, 73 – 85, 2008.

[3] L. Nordström, "Assessment of Information Security Levels in power communication systems using Evidential Reasoning", IEEE Transactions on Power Delivery, 23(3), 2008.

4] D. Choi, H. Kim, D. Won and S. Kim, "An Advanced Key-management Architecture for Secure SCADA Communications", IEEE Transactions on Power Delivery, 24(3), 1154 – 1163, 2009.

[5] A. Hahn and M. Goundarasu, "An Evaluation of Cyber security Assessment Tools on a SCADA Environment", IEEE, 5 – 11, 2011

[6] W.C. Axelrod, "Applying Lessons from Safety-critical Systems to Security-critical Software", IEEE, 2 – 11, 2011

[7] SIEMENS, "Power System Control SCADA and Energy Management System", Publication, 2006.

[8] J. Powell: Profibus and Modbus: a comparison, SIEMENS Automation Website. October 132013

[9] A. A. Alade, "Secured Framework for Supervisory Control and Data Acquisition (SCADA) System of Power Transmission Network: A Case Study of PHCN Network", M. Sc Dissertation, Babcock University, Nigeria, 2013.