Overview of the Supervisory Control and Data Acquisition (SCADA) System

Alade A. A., Ajayi O. B., Okolie S. O., Alao D. O.
Department of Computer Science
Babcock University, Nigeria
Akinalade2000@gmail.com (Correspondence Author)

Abstract— This paper, titled, "Overview of the Supervisory Control and Data Acquisition (SCADA) System" is a precursor to the subsequent papers on analytical performance model for SCADA System protocols. We examine the fundamental functions expected from a SCADA System, its components and the distinct features between SCADA System and Distributed Control System (DCS) – both are members of the set of Industrial Control System (ICS). This work is quite different from others as SCADA System is considered from different perspectives such as: a) role in monitoring and control of critical infrastructure like national electricity supply system and oil and gas pipelines; b) its layout and hierarchical architecture and c) its Master/Remote Terminal Unit (RTU) functional data/control flow. Its hierarchical model presented is compared with the Purdue Enterprise reference Architecture (PERA) which is one of the general models that visualize the entire enterprise system from the field or the plant to the apex (Computer System or production Scheduling). Compliance is confirmed.

Index Terms: Critical infrastructure, DCS, Enterprise, ICS, Model, SCADA, RTU.

1 Introduction

SUPERVISORY Control and Data Acquisition (SCADA) systems are one of the control systems type under the general term of Industrial Control System (ICS). Other notable members of the set are Distributed Control systems (DCS) and Programmable Logic Controllers (PLC). They are used in critical infrastructure and industrial sectors [1]. Local control of industrial processes is the main function of the DCS while the PLCs are designed to comfortably acquire sensors, actuators and set points information from the field. It serves both the SCADA Systems and the DCS.

SCADA Systems is, however, different from the DCS which is localized to the industrial sites as its control and monitoring functions covers wide geographical areas as it supervises devices located thousands of kilometers apart from one another and from the control centre. The critical infrastructure where they are applied include electrical power networks, natural gas and oil pipelines, roads and rail transportation systems. SCADA's primary functions are data acquisition, data processing for use by the operator, and control of remote devices by operator [2].

In SCADA System, data acquisitions, transmission systems and Human Machine Interface (HMI) software are integrated to function as a centralized control and monitoring system for processing several inputs and outputs. The collected information from the field is transferred to the computer based control centre, where with the aid of HMI it is either displayed textually or graphically.

SCADA system comprises both software and hardware. The hardware are the Master Terminal Unit (MTU) which resides at the control centre, the communication facilities such as telephone line, radio, satellite and cable, and remote terminal units (RTUs) or PLCs – distributed over wide geographical field sites to monitor sensors and control actuators. The RTUs or PLCs are in charge of the local activities by the sensors and actuators while the MTU processes and stores the information from the RTUs outputs and inputs. Through the communication hardware, information flows continually to and fro the MTU and RTUs. The software determines when to monitor, what to monitor, the acceptable parameter ranges, response type etc [3].

2 Methodology

Through extensive literature review of relevant journals (online and hard copies), printed books and search engines, SCADA System is seen in a new light. These identified features of SCADA System are discussed below.

2.1 SCADA System Components

a Master Terminal Unit (MTU) or SCADA Server: In SCADA System, the MTU is the master in a master-to-slave relationship existing between the RTUs/PLCs/IEDs. RTUs/PLCs/IEDs located in the field sites act as slaves.

b Remote Terminal Unit (RTU): RTU which also means Remote Telemetry Unit is a control and data acquisition unit placed in the remote field stations. It provides support for the SCADA System remotely. "Its primary task is to control and acquire data from processing equipment at the remote location and to transfer this data back to a central station",

[4]. Where there is no wired communication, other means of communication such as wireless radio is used to convey RTU message to the MTU. Occasionally, PLCs are deployed as field devices to replace RTUs.

c Programmable Logic Controller (PLC): PLC started as a little computer capable of executing logic functions using electrical hardware such as switches, counters/timer, and relays. It has developed in capability and can now control complex processes. It has wide application in SCADA systems and other family of Industrial Control System. Although it does not have exact capability of RTU, it is preferred by some as field device as it is economical, flexible and versatile.

d Intelligent Electronic Devices (IED): It is a "smart" actuator/ sensor having enough intelligence needed for data acquisition, communication to different devices and performance of control and processing. One device of IED may contain in one device, program memory, analog input/output and a communication system. Their deployment in SCADA system provides automatic control locally.

e Human-Machine Interface (HMI): The HMI is hardware and software which enable human operators monitor the controlled process' state, adjust the settings of the control as necessary and occasionally respond fast in case of emergency to change to override automatic control operations. The HMI also provides the necessary tool needed by the operator or the control engineer to configure the control algorithm and set points. The HMI also displays reports, historical information, process status information and other such information as may be required for smooth supervision of the field devices.

f Data Historian: This is a database placed centrally for recording all process information within the SCADA system. The stored information provides data for various analyses.

2.2 SCADA System Architecture

A typical SCADA System architecture is shown in Fig. 1. It has three segments. Starting from the left side, these segments are Field Sites, Communication Medium and Control Centre. The description follows.

a Field Sites: Field sites usually have remote access features which enables the field operators perform diagnostics and effect repairs remotely. Field Site 1(Fig. 1.) consists of Modem and PLC which connects to the sensors and other field devices through the field bus network. With the use of field bus technologies there is no need for point-to-point wiring between the PC and the field devices. The processed data from the PLC passes through the modem where it is modulated and transmitted through the communication medium to the Control Centre. "A modem is a device used to convert between serial digital data and a signal suitable for transmission over a telephone line to allow devices to communicate"[1]. Field site 2 has both WAN Card and Intelligent Electronics Device (IED) connected directly to the modem as there is no need for PLC since it has enough intelligence built into it to handle some data. Field site 3 is similar to field site except that RTU replaces the PLC. Communication between the sensors, other field devices and the RTU/PLC requires protocols. There are various types in use which will be discussed later.

b Communication Link: There is usually a long distance between the Field Sites and the Control Centre ranging from a few kilometers to hundreds of kilometers or at times thousands of kilometers. An effective communication is necessary for effective flow messages to and from the MTU and the PLCs/RTUs/IEDs [5]. As shown in Fig.1., the link can be either of the listed: Switched Telephone Leased Line; Power Line Based Communications; Radio; Microwave; cellular; Satellite and Wide Area Network (WAN).

c Control Centre: The main components here are the SCADA Server or the MTU, the HMI, Engineering Workstations, Data Historian and Communication routers. All these components are linked by Local Area Network (LAN). Information gathered by the field sites is collected by the control centre where it is logged and displayed on the HMI to enable the operator takes necessary appropriated action as dictated by the events detected. Trend analyses, central alarming and reporting are also the responsibility of the control centre [1].

In fig. 2., the Master/RTU functional Data /Control flow is presented. It is divided into three functional components viz. the Master Station where the servers of the MTU, HMI, Data Historian and Engineering WorkStation are housed; the Communication System and the Field Sites. There are communication

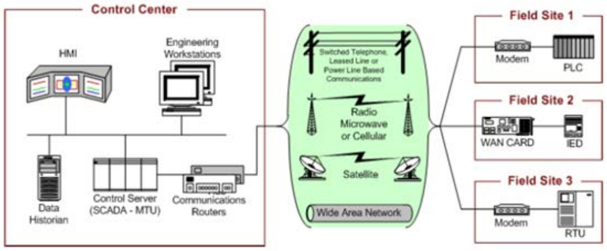

Fig. 1: SCADA System General Layout
Source: Stouffer et al [1]

interfaces between the Master Station and the Communication System and between the Communication System and the Field sites.

The information flow across the interfaces is categorized into three types. These are Supervisory information such as trip/close, raise/lower, stop/start, set point/values, parameter download, control programmes, database and alarm parameters. The second set of information required for proper functioning of the SCADA System is the standard time signal while the third are analog data, accumulated data, digital data, status, alarm, sequence of events, diagnostic results and abonomalities.

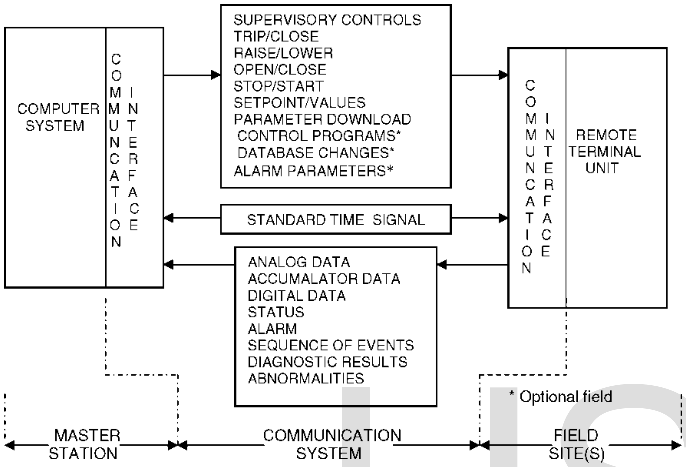

Fig. 2: Master/RTU Functional Data/Control Flow
Source: Makhija [6]

Fig. 3. is a pictorial architecture of SCADA System depicting two Remote Terminal Units (RTUs) connected to a Sub MTU through which some data acquisition and processing takes place before forwarding the output to the main Master Terminal Unit (MTU) at the control centre. Two RTUs have direct connection through a communication medium to the MTU at the Control Centers. Also shown are the HMI, the operator at the control centre and the operator at the remote station served from the Control Center via the internet.

Fig. 4. is a model of SCADA System along with the critical infrastructure such as power plant, wind power plant, water plant, oil and gas installation that are being supervised and controlled to guarantee their efficient performance and safeguard against any form of threats.

2.3 Hierarchical Model of SCADA System

In the hierarchical Model of SCADA System in fig. 6., Bailey and Wright [4] highlight the essential five levels or hierarchies that define a complex SCADA system. At the very bottom is level 0 which is the field level. Here we have the sensors, transducers and actuators directly attached to the plant being monitored. Next to this is the level where the remote RTUs that acquire the signal/information from the field equipment are. It is here that raw data from the field devices such as the sensors and the actuators are digitized and preprocessed and through communication interface forward to the sub MTUs for further processing. The RTUs are in level 1 while the sub MTUs are in level 2. The processed data from the sub MTUs are relayed to the Master Terminal Units at the sub MTUs for further processing. The RTUs are in level 1 while the sub MTUs are in level 2. The processed data from the sub MTUs are relayed to the Master Terminal Units at the SCADA control centre (level 3) through an appropriate communication medium. The fifth level is the commercial data processing system also called the Enterprise system.

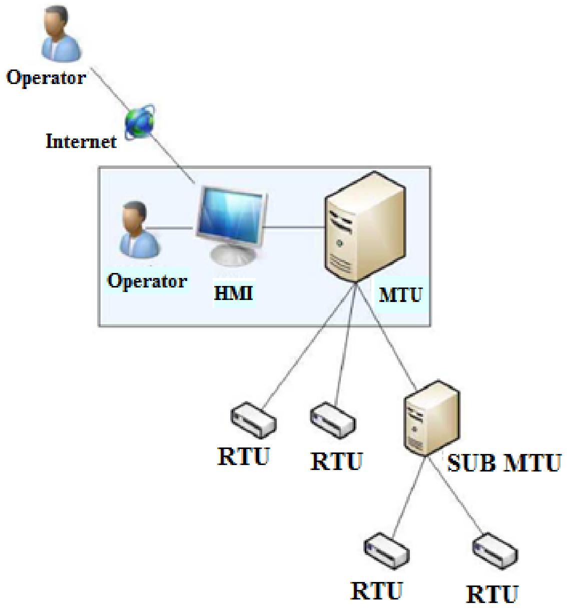

Fig. 3: SCADA System Architecture
Source: Choi et al[7]

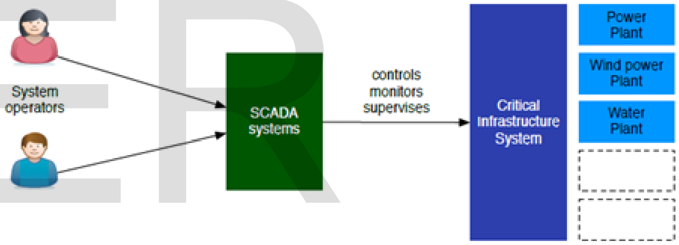

Fig. 4: SCADA and Critical Infrastructure system
Source: Queiroz [8]

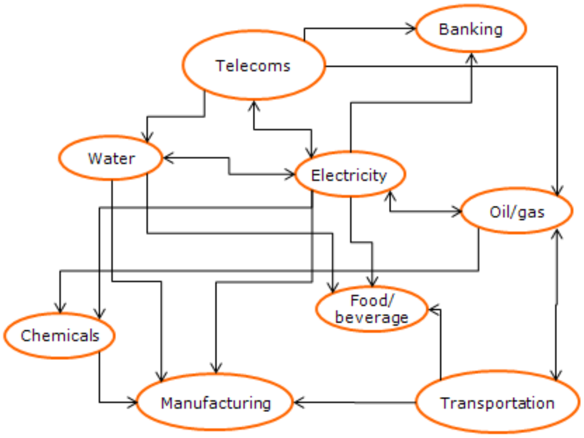

Fig. 5: Interconnection of Critical National Infrastructure
Source: https://www.citicus.com/characteristics-of-Industrial-Control-Systems [9]

2.3.1. Hierarchical Model of SCADA System Compared to PERA

The search for a model that would capture every aspect of an organization's activities had been on for several years. Among the most famous of all-comprising models for industrial process was the one developed in the 1990s by Theodore J, Williams of Purdue University. Purdue Enterprise Reference Architecture (PERA) is a 1990s reference model for enterprise architecture. The model provides a reference for enterprise control that end users, vendors and the industry can share through integration of appropriate applications at the fitting layers in the enterprise. Willliams [10] described his model known as PERA) as below:

- "Level 0 — The physical process — Defines the actual physical processes.
- Level 1 — Intelligent devices — Sensing and manipulating the physical processes. Process *sensors, analyzers, actuators and related instrumentation.
- Level 2 — Control systems — Supervising, monitoring and controlling the physical processes. Real-time controls and software; DCS, human-machine interface (HMI); supervisory and data acquisition (SCADA) software.
- Level 3 — Manufacturing operations systems — Managing production work flow to produce the desired products.Batch management; manufacturing execution/operations management systems (MES/MOMS); laboratory, maintenance and plant performance management systems; data historians and related middleware. Time frame: shifts, hours, minutes, seconds.
- Level 4 — Business logistics systems — Managing the business-related activities of the manufacturing operation. ERP is the primary system; establishes the basic plant production schedule, material use, shipping and inventory levels. Time frame: months, weeks, days, shifts".

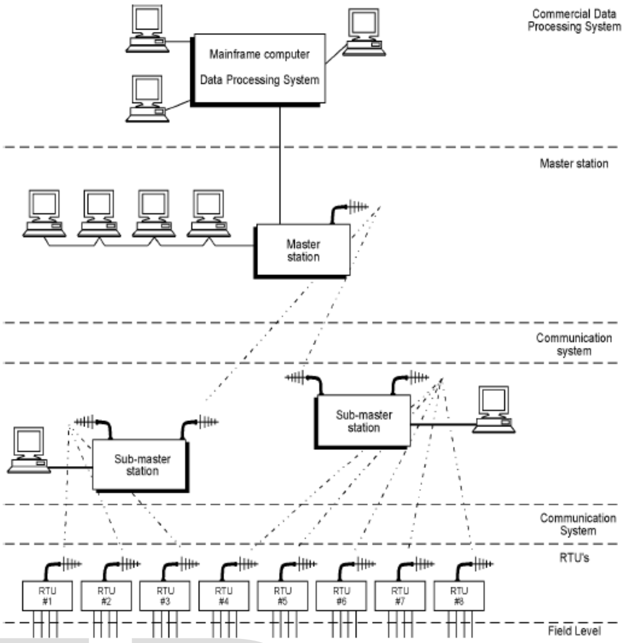

Fig. 6: Hierarchical Model of SCADA System
Source: Bailey and wright [4]

Fig. 7. depicts the enterprise architecture clearly, reflecting the five reference levels of the PERA. In comparison with the SCADA System hierarchical model, level "0" in the figure is equivalent to level "0" in the SCADA System hierarchical model as both sensors, measurands and actuators in fig. 6. and Plant in fig. 7. refer to the actual infrastructure being monitored. The direct Control label for level 1 in fig. 7. refers to similar activities performed by set of RTU in fig. 6. Level 2 in fig. 7. that models the plant supervisory functions is comparable to the similar level in fig. 6. where the Sub MTU performs corresponding supervisory control. The general oversight by the Master Control Center (where the MTU, HMI, Data Historians and the human operators reside) over the sub MTU, the RTUs and the field devices as depicted in fig. 6. is likened to Production Control functions in level 3 of the model in fig. 7. In both fig. 6 and fig. 7., the fifth level model the commercial/enterprise component of the overall industrial process, though, giving different names.

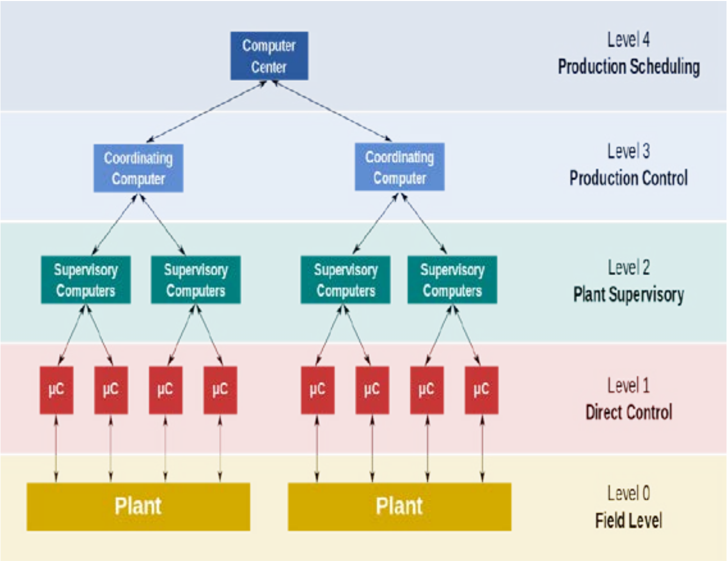

Fig. 7: The Enterprise Architecture
Source: Pugliesi [11]

3 Discussions

Fig. 5. depicts interdependence of the critical infrastructure. For instance, electricity infrastructure is connected to almost all the other infrastructure such as oil/gas, Water, telecommunications, Banking food/beverages and manufacturing. A mutual relationship is observed between electricity and water infrastructure, electricity and oil/gas and electricity and telecommunications. Implication of the observed interdependence is that the catastrophic impact of the failure of the SCADA System of any of these critical infrastructure may cascade to other infrastructure leading to huge economic loss and considerable effect on the general well being of the people. The need for prevention of this kind of situation is the motivation for thousands of the ongoing researches on SCADA System security.

4 CONCLUSION

In this preliminary study, we notice the significance of SCADA System to various infrastructure monitoring, data acquisition and control.

Obviously, a comprehensive SCADA System as reflected in fig. 5. is highly vulnerable to both external and internal threats as it interfaces with the enterprise network which is connected to the internet.

Internet gate way is a weak link through which the external saboteurs (the attackers) may exploit. Internal threat may be either intentional or unintentional. Threats, vulnerability and attacks on SCADA System have always been of major concern in SCADA System and still remain open areas requiring deeper studies.

References

[1] K. Stouffer, J. Falco, and K. Scarfone, “Guide to Industrial Control Systems (ICS) Security”, Gaithersburg, MD: National Institute of Standards and Technology, 2015, doi: 10.6028/NIST.SP.800-82r2.

[2] D.J. Gaushell and H. T. Darlington, “Supervisory Control and Data Acquisition”, Proc. IEEE, vol. 75, no. 12, pp. 1645–1658, 1987.

[3] H. Li, “Wide Area Voltage Monitoring and Optimization”, Ph. D. dissertation, Dept. Elec. Eng., Washington State University, Pullman, 2013.

[4] D. Bailey and E. Wright, “Practical SCADA for Industry”, Burlington, MA: Newnes, Elsevier, 2003.

[5] R. M. Oliveira, M.S.P. Facina, M.V. Ribeiro, and A.B. Vieira, “Performance Evaluation of In-home Broadband PLC Systems Using a Cooperative MAC Protocol”. Computer Networks vol. 95, pp. 62–76, 2016, doi: 10.1016/j.comnet.2015.12.004 1389-1286.

[6] J. Makhija, “Comparison of Protocols Used in Remote Monitoring: DNP 3.0, IEC 870 - 5 - 101 & Modbus”, M. Tech. Credit Seminar, EE Department, IIT, Bombay, 2003.

[7] D. Choi, H. Kim, D. Won, and S. Kim,”An Advanced Key-management Architecture for Secure SCADA Communications”, IEEE Transactions on Power Delivery, vol. 24. no. 3, pp. 1154 – 1163, 2009.

[8] C.A. Queiroz, “A Holistic Approach for Measuring the Survivability of SCADA Systems”, Ph D thesis, School of Computer Science and Information Technology, RMIT University, Vietnam, 2012.

[9] Citicus Inc., “Interconnection of Critical National Infrastructure”,available at https://www.citicus.com/characteristics-of-Industrial-Control-Systems, 2015.

[10] T.J. Williams, “The Purdue enterprise reference architecture”. Computers in industry, vol. 24, no. 2, pp. 141-158, 1993.

[11] D. Pugliesi, “The Enterprise Architecture”, available at https://commons. wikimedia.org/w/index.php?curid=31527335, 2015.

Acknowledgment

The authors wish to thank the Management of the Computer Science department, Babcock University, Nigeria for their supports in the course of this work. The inputs of some of the lecturers to this work are highly appreciated.