Global Scientific JOURNALS

GSJ: Volume 5, Issue 11, November 2017, Online: ISSN 2320-9186
www.globalscientificjournal.com

# A SURVEY OF THE SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) SYSTEM PROTOCOLS

Alade A. A., Ajayi O. B., Okolie S. O., Alao D. O.

*Alade A. A : Department of Computer Science, Babcock University, Nigeria, akinalade2000@gmail.com*
*Ajayi O. B: Department of Computer Science, Federal University of Agriculture, Abeokuta, Nigeria, olutayoajayi@gmail.com*
*Okolie S. O: Department of Computer Science, Babcock University, Nigeria, samuelokolie2003@yahoo.com*
*Alao D. O: Department of Computer Science, Babcock University, Nigeria, alaool@babcock.edu.ng*

**KeyWords**

DNP 3, IEC 870-5-101, Modbus, OSI Model, Profibus, Protocols, SCADA



**ABSTRACT**

Supervisory Control and Data Acquisition (SCADA) system has the primary function of collecting data from the field devices through terminal equipment such as the Remote Terminal Unit (RTU) and the Programmable Logic Unit (PLC), analyse and transmitted it to the central control area where it is displayed for monitoring, archiving and control. Unlike the Information Technology (IT) systems, SCADA Systems are generally time-critical, necessitating the need for special protocols for data acquisition and control. In this work we conducted a survey on the characteristics of SCADA System protocols, the available types, their applications and comparative features. The SCADA System protocol reference model was compared with the Open Systems Interconnection (OSI) model and found to have 3 layers as against 7 layers of OSI Model. In the course of the study, several SCADA System protocols were examined and it was discovered that some of these protocols such as Modbus, IEC 870-5-103, Profibus and IEC 6185 are suitable for communication in the fields while some like DNP 3, IEC 870-5-101 and IEEE P125 are suitable for communication outside the fields.

## 1 INTRODUCTION

A DISTINCT feature of Industrial Control Systems (ICS) when compared with Information Technology (IT) Systems is that time is of essence in ICS – services are more time-critical in ICS than in IT systems. Park, Mackay and Wright [1] capture it this way:

"For many industrial protocols the use of all the seven layers of OSI model is inappropriate as the application may require a high-speed response. Hence a simplified OSI model is often preferred for industrial applications where time critical communications is more important than full communications functionality provided by the seven-layered model. Generally, most industrial protocols are written around three layers: the Physical layer, Data link layer and Application layer" (Figure 1). In the same direction, Weiss [2] in his book titled "Protecting Industrial Control Systems from Electronics Threats" observed that in SCADA Systems continuous availability is highly important and has priority over confidentiality and integrity which are of major consideration in IT systems. In consideration of the need to meet the real-time required by the SCADA systems and simultaneously reduce cost, a simplified OSI reference model is adopted. In this model, the non-time critical and general application is removed from the model while physical layer, data link layer and application layer are reserved [3]. In comparison with OSI Reference Model, these three layers of in SCADA System protocols correspond to layers 1, 2 and 7 of the OSI architecture as depicted in Figure 2. [4]. When the number of protocol layers used in a model is reduced, greater performance can result since there will be lower overheads [5].

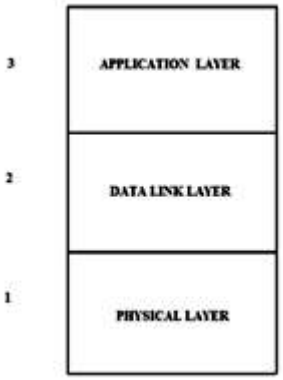


**Figure 1: SCADA Protocol Reference Model**
**Source: Park, Mackay and Wright [1]**



However, the use of only three layers in order to save time involves some compromises such as limitation in the size of the application layer messages to that allowable by the channel due to the absence of Transport layer that has breaking of data into manageable size as part of its function. Absence of the network layer implies that message routing would not be possible. There would be no duplex communication since there is no session layer and finally, there would be uniform message formats in all nodes as there is no presentation layer that is responsible for such formatting [1].

These are the distinct characteristics of the SCADA protocols that prompt the ongoing study. The survey, hence, explores the distinct characteristics of the SCADA System protocols in the following sections.

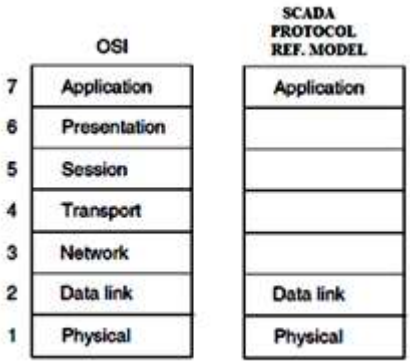


**Figure 2: SCADA Protocol Reference Model Compared with OSI Model**
**Source: Alhussein [4]**

## 2 Methodology

The first step taken in this work is to review literature from several sources on the subject. The sources used include online and offline academic journals, hard copy text books on SCADA System and various search engines. The findings are documented, discussed and concluded.

### 2.1 The need for SCADA System Protocols

Figure 3 below is a typical master/slave topology that exists between the Control centre and the field devices in a SCADA System. In most SCADA System there is only one master station where the Master terminal Unit (MTU) resides. Several field stations that are geographically spread called the slaves in the figure respond to the polling for information from the master station. The slaves here are the Remote Terminal Units that acquire field data from the field measurands, sensors and actuators. For effective communication between the master station and the slaves (Remote Terminal Unit) and communication between the slaves and the field devices there must be appropriate protocols in place. These are different from the common internet protocols as they have special time-critical functions to perform. Comer [6]'s statement that s "Protocols are to communication what programming languages are to computation" is very much relevant in SCADA system as in the general computer network.

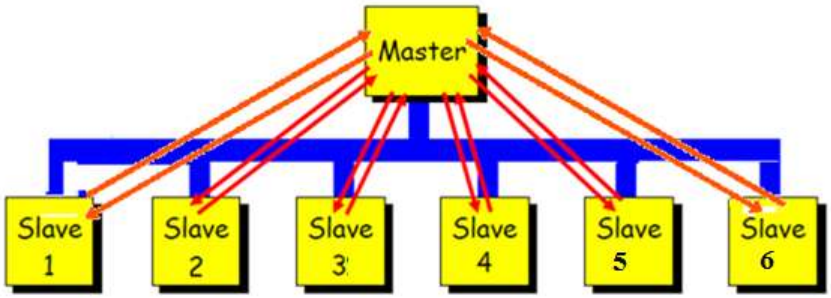


**Figure 3: Single Master/Slave System**
**Source: Hans-Petter [7]**

### 2.2 SCADA System Protocol Types

Igure et al [8] and Kalapatapu [9] remarked that there are about 200 real time SCADA platform and protocols in use. The list includes the non-proprietary and proprietary protocols some of which are:
Allen Bradley DF1,DH and DH+
GE Fanuc
Siemens Sinaut
Mitsubishi
Modbus RTU / ASCII
Omron
Toshiba
Westinghouse
Other Vendor Protocols

Devarajan [10] listed the following as some of the SCADA System protocols generally used:
Modbus
Distributed Network Protocol 3 (DNP3)
Inter-Control Center Communications Protocol (ICCP)
Utility Communications Architecture 2.0 (UCA 2.0) and International Electrotechnical Commission (IEC) 61850 Standards
Control Area Networks (CAN)
Control Information Protocol (CIP)
DeviceNet

ControlNet
OLE for Process Control (OPC)
Profibus
Makhija [11] listed communication protocols options available according to use requirements. Some protocols are suitable for communication with field devices used for protection and metering, sensors, transducers and actuators. Some are applicable for communication after the field environment, especially communication between the field and the master control centre while some are useful for communication within application (Table 1).

**Table 1: Protocols and Area of Application**

| | Area Of Application | | |
|---|---|---|---|
| **Protocols** | **Communication In The Field** | **Communication Outside The Field** | **Communication Within Application** |
| | Modbus | IEC 870 -5 - 101 | 61968 |
| | IEC 870 -5 - 103 | IEC 870 -5 - 104 | |
| | LON | DNP 3.0 | |
| | Profibus | IEC 60670- 6 (TASE .2) | |
| | IEC 6185 | IEEE P1525 | |
| | UCA | ELC OM9 | |
| | SPA (ABB) | | |
| | K- BUS (Alstom) | | |
| | VDEW (Siemens) | | |



### 2.3 SCADA Protocols Characteristics

The characteristics of DNP 3.0., IEC 870-5-101 and Modbus – the three widely applied SCADA System protocols are compared in tables 2. Table 2 was compiled by Makhija [11] from the works of [12], [13] and [14]. In the table, 12 features of SCADA protocols are considered side by side. These features are standardization, standardization organization, Architecture, Physical layer, Data Link layer, Application layer, Device addressing, Configuration parameters requirement, Application specific information model, Cyclic transmission, Dominant market, Online configurations and Open encoding solutions.
As depicted in the three tables, IEC 870-5-101 and DNP 3.0. have very similar features except a few exceptions which include the following: (a) an additional layer in the DNP 3 called User's layer making the number of layers 4. (b) unlike the IEC 879-5-101, DNP 3.0 supports multiple masters, multiple slave and peer-to-peer communication. In IEC 879-5-101, data objects and messages depend on each other while they are independent of each other in DNP 3.0. and c) while DNP 3.0 is open for encoding solution, IEC 879-5-101is not. Both rate higher than any other SCADA protocols and have broad acceptance than others. While DNP 3.0 is widely used in Asia, Latin America, North America and Australia, IEC 879-5-101 is well accepted in Europe [15] and [16].

## 3 Discussions

As SCADA System protocols are time-critical, some layers of the OSI are not necessary in order to reduce the time required to traverse the specific node or entity. These excluded layers are the presentation layer that sets the standard that control the translation of incoming and outgoing data from one format to another; the session layer standards that manage the communication between the presentation layer of the sending and receiving computer; the transport layer standards that ensure reliable completion of data transfers, error discovery/data flow control and the network layer standards that define the management of network connections. Removal of these four layers from the SCADA protocol reference model sheds the burdensome headers overhead.

The countless number of SCADA System protocols available in market (proprietary and non –proprietary) serves different purposes. Some such as DNP 3 and IEC-870-5-101 are deployed in huge critical infrastructure SCADA System while protocols like Profibus and IEC 6185 are for field device application.

An obvious difference is seen between DNP 3, IEC-870-5-101 and Modbus when features such as architecture, standardization, Application, Data link layers and configuration requirements are compared.

**Table 2: Comparison of DNP 3.0. IEC 879-5-191 and Modbus**

| Feature | IEC 870-5-101 | DNP 3.0 | Modbus |
|---|---|---|---|
| *Standardization* | IEC Standard (1995) Amendments 2000,2001 | Open industry specification (1993) | Not Applicable |
| *Standardization Organization* | IEC TC 57 WG 03 | DNP user's group | Modicon Inc. |
| *Architecture* | 3-layer EPA architecture | 4-layer architecture Also supports 7 layer TCP/IP or UDP/IP | Application layer messaging protocol |
| *Physical layer* | Balanced Mode – Point to Point Multipoint to point Implementation by X.24 / X.27 standard<br><br>Unbalanced Mode – Point to Point Point to Multipoint Implementation by V.24 / V.28 standard | Balanced mode transmission<br><br>It supports multiple masters, multiple slave and peer-to-peer communication<br><br>RS 232 or RS 485 implementation<br><br>TCP/IP over Ethernet, 802.3 or X.21 | Balanced mode of transmission<br><br>RS 232 serial interface implementation<br><br>Peer to peer communication<br><br>TCP/IP over Ethernet |
| *Data link layer* | Frame format FT 1.2 Hamming distance – 4 | Frame format FT3 Hamming distance-6 | Two types of message frames are used: ASCII mode and RTU mode |
| *Application layer* | Both IEC 870-5-101 and DNP 3.0 provides<br>• Time synchronization<br>• Time stamped events<br>• Select before operate<br>• Polled report by exception<br>• Unsolicited responses<br>• Data group/classes<br><br>Limited to single data type per message<br><br>Can control one point per message only<br><br>No internal indication bits | Remote starting / stopping of software applications<br><br>Polling by data priority level<br><br>Broadcast addressing<br><br>Multiple data types per message are allowed<br><br>Internal Indication field IID present in response header<br><br>Application layer confirms events; use of CON bit is made | Does not give time stamped events. We have sequence of events (without time but not event list with time.<br><br>Does not provide polled report by exception<br><br>Checksum ensures proper end-to-end communication |

Source: IEEE Std. 1379 (1997), Coats (1999) and Schwartz (1999 )

**Table 2: Comparison of DNP 3.0. IEC 879-5-191 and Modbus continued**

| Feature | IEC 870-5-101 | DNP 3.0 | Modbus |
|---|---|---|---|
| *Device Addressing* | Link address could be 0, 1, 2 bytes<br><br>Unbalanced link contains slave address<br><br>Balanced link is point to point so link address is optional (may be included for security) | Link contains both source and destination address (both always 16 bits)<br><br>Application layer does not contains address<br><br>32 b point addresses of each data type per device | Addresses field contains two characters (ASCII mode) or 8 bits (RTU mode)<br><br>Valid address in range 1-247<br><br>Address 0 used for broadcast |
| *Configuration Parameters required* | Baud rate<br><br>Device addresses<br><br>Balanced / unbalanced<br><br>Frame length<br><br>Size of link address<br><br>Size of ASDU address<br><br>Size/structure of point number | Baud rate<br><br>Device addresses<br><br>Fragment size | Baud rate<br><br>Mode – ASCII or RTU<br><br>Parity mode |
| *Configuration Parameters required contd...* | Size of cause of transmission | | |
| *Application Specific information model* | A few application specific data types available<br><br>Data objects and messages are not independent to each other | Permits vendors to create application specific extensions<br><br>Data objects and messages independent to each other | Allows user to create application specific model |
| *Cyclic transmission* | Eliminates static data poll message from master<br>Interrupted by event triggered communication request | Available but interval cannot be remotely adjusted | Not Applicable |

Source: IEEE Std. 1379 (1997), Coats (1999) and Schwartz (1999 )

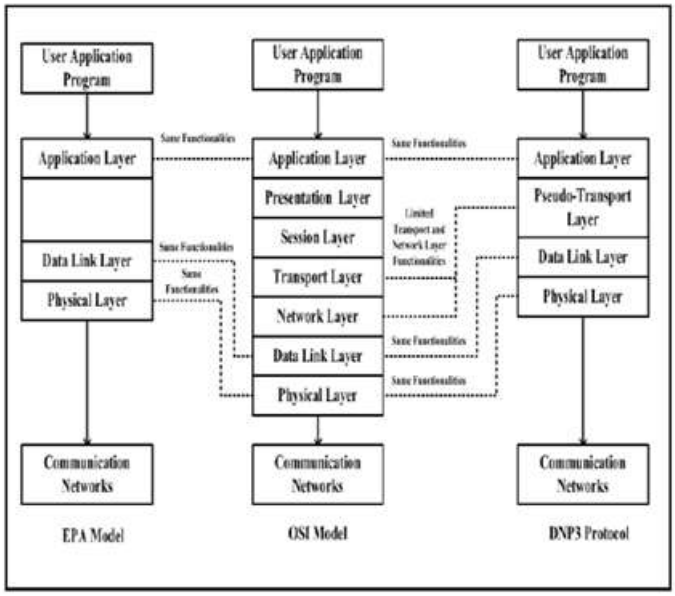


**Figure 4: Relationship between OSI, EPA and DNP3 Protocol**
**Source: Shahzad et al [17]**

## 4 Conclusion

It is established that SCADA System protocols are based on a 3-layer Enhanced Protocol Architecture (EPA). However, in order to take the numerous advantages of the widely applied TCP/IP Protocol suite that features in internet and which resolves the problem of interoperability between different networks, further researches are required to augment the existing ones on SCADA System protocols.



## Acknowledgment

The authors wish to express our appreciation to the Management of the Computer Science department, Babcock University, Nigeria, for the tremendous supports rendered in the course of this work.

## References

[1] J. Park, S. Mackay and E.Wright, "Practical Data Communications for Instrumentation and Control", Burlington, MA: Newnes, Elsevier, 2003.
[2] J. Weiss, "Protecting Industrial Control Systems from Electronic Threats", New York, NY: Momentum Press, LLC, 2010.
[3] H. Gao and W. Tong, "Analysis and Evaluation of Fieldbus Communication and Protocol Static Characteristic", Association for Computing Machinery 978-1-60558-088-3, 2008.
[4] A. M. Alihussein, "A Supervisory Control and Data Acquisition (SCADA) for Water Distribution System of Gaza City", M.Sc thesis, Electrical Engineering Department , The Islamic University of Gaza Deanery of Graduate Studies , Palestine, 2010.
[5] G.D. Law, "A Model for the Design of High Performance Protocols for A Networked Computing Environment", Edinburgh , U.K: Spider Systems Limited, 1985.
[6] D.E. Comer, "Internetworking with TCP/IP vol I: Principles, Protocols, and Architecture", Upper Saddle River, New Jersey: PrenticeHall, Inc., 2000.
[7] H. Hans-Petter, " Modbus Overview", Available at http://home.hit.no/~hansha /documents/industrial_it/resources/resources/modbus/Modbus%20Overview.pdf, 2013.
[8] V.M. Igure, S.A. Laughter, R.D. Williams and C.L. Brown, "Security Issues in SCADA Networks", Computers & Security", vol. 25, No. 26, pp. 498–506, 498–506, 2006. doi:10.1016/j.cose.2006.03.001.
[9] R. Kalapatapu, "SCADA Protocols and Communication Trends", Presented at ISA ( The Instrumentation, Systems and Automation Society) at Reliant Center Houston, Texas, 2004.
[10] G. Devarajan, "Unraveling SCADA protocol:Using Sulley Fuzzer", Available at https://www.dc414.org /download/confs/defcon15/Speakers/Devarajan/Presentation/dc-15-devarajan.pdf, 2013.
[11] 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.
[12] J. Coats, "Comparison of DNP and IEC 870-5-101", Available at www.trianglemicrowoks.com, 1999.

[13] Institute of Electrical and Electronics Engineers, "IEEE Std 1379-1997, IEEE Trial-Use Recommended Practice for Data Communications Between Intelligent Electronic Devices and Remote Terminal Units in a Substation", Available at http://ieeexplore.ieee.org /iel4/5327/14435/00660326.pdf, 1997.

[14] K. Schwarz, "Comparison of IEC 870-5-101/-103/-104, DNP3 and IEC 60870-6- TASE.2 with IEC 61850", Available at www.nettedautomation .com/news/n_44.html, 2002.

[15] A. Ortega, A. A. Shinoda, C. M. Schweitzer, F. Granelli, A.V. Ortega and F. Bonvecchio, "Performance evaluation of the DNP3 protocol for smart grid applications over IEEE 802.3/802.11networks and heterogeneous traffic", Recent Advances in Communications, 2014.

[16] S. Bagaria, S. Prabhakar and Z. Saquib, "Flexi-DNP3: Flexible distributed network protocol version 3 (DNP3) for SCADA security", Proceedings of the International Conference on Recent Trends in Information Systems (ReTIS), pp. 293-296, 2011.

[17] A. Shahzad, S. Musa, M. Irfan, A. Aborujilah, "Industrial Control Systems (ICSs) vulnerabilities analysis and SCADA security enhancement using testbed encryption", Proceedings of the IMCOM (ICUIMC) Conference, Siem Reap, Cambodia, 2014.