An Overview to Electrical Substation Automation Using SCADA

Tahoora Qureshi
M. E. *(Power Systems Engineering)*
A. C. P. C. E
Mumbai, India.
tahooraq.aiktc@gmail.com

Dr. S. R. Deore
P. H. D (Electrical Engineering)
IIT Bombay
srdeore@acpce.ac.in

***Abstract*—"Supervisory control and data acquisition (SCADA) system" is universally accepted means of control for electrical substation which involves continual real time monitoring applicable to generation, transmission and distribution systems. The heart of SCADA lies in the functioning of Remote Terminal Units (RTUs) which collects analog and status telemetry data from field devices and also communicates command signals to them. The inclusion of automation in electrical substation has resulted in a string of advantages including visibility of network operation, flexibility of controls, real time accurate and consistent data, statistical data archiving, faster fault identification, isolation and system restoration. Complex design of SCADA systems involve accurate matching of protocols and communication parameters between connecting devices. This paper aims at establishing a basic understanding of SCADA components, communication protocols and architectures, standards employed and the security risks involved in such systems.**

Keywords—SCADA, Electrical Substation Automation, Communication Protocols, SCADA standards Organisation, SCADA Architecture.

I. INTRODUCTION

"Supervisory control and data acquisition system"(SCADA) is a technology which enables user to collect data from far off locations in power system and to send control commands whenever necessary to these locations.

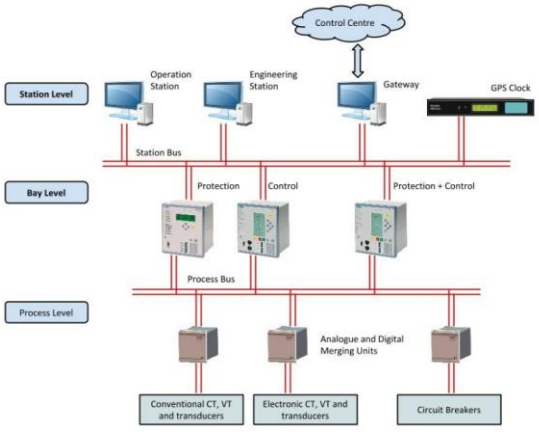

Fig. 1: The Digital Substation [2]

These systems enable automation of large electrical substations by providing effective monitoring and control functions [1]. The automation tasks involved include data acquisition, supervision and control. Signals gathered from far off remote places include status indication, analog values, alarms, and totalized meter values among other signals types. Typical signals sent from SCADA systems are usually limited to discrete binary bit changes or to analog values addressed to a device at a process. Fig. 1 shows a digitalized substation.

II. SUBSTATION AUTOMATION SYSTEM COMPONENTS

Following section provides an overview of various components used in a typical electrical system with respect to Substation Automation System (SAS).

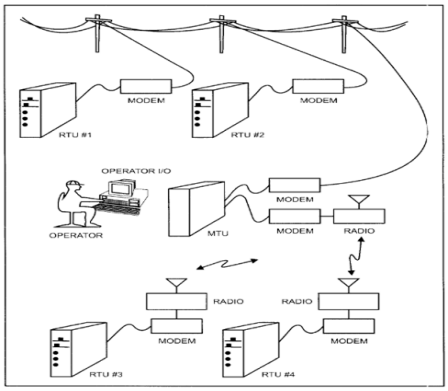

Fig. 2: Basic Components of a SCADA System [3]

A. *Server*

Unification of all substation data is performed by the server. Its functions involve data concentration, protocol conversion, providing secure access control gateway, collection of automatic fault recordings, event recording, data loggings etc.

B. *Human Machine Interface*

The substation automation system (SAS) is interfaced with humans through keyboards, monitors, mouse which is installed inside SAS room. There is a provision for portable laptop for

parametisation, configuration, system analysis, uploading/downloading data to/from intelligent electronic devices (IED).Engineering analysis of the electrical network operations, system configuration, and fault analysis is carried out by the authorized engineer from engineering work station whereas routine monitoring and control of the network is done by authorized personnel from operator workstation.

C. Remote Terminal Unit

Remote terminal unit (RTU) is microprocessor controlled electronic device. It performs two functions; provide ability to communicate to master terminal unit (MTU) and provide ability to communicate with each of field sensors and actuators connected to it. To do so, RTU must be well versed with protocol of each field devices with their names and addresses. It should also know where to store information collected from field devices so that the data will be made available to MTU whenever told so. An RTU may consist of many circuit cards including CPU or processing with communications interface(s), Ethernet Switches and one or more of the following: (AI) analog input, (DI) digital input, (DO) digital or control (relay) output, or (AO) analog output card(s).

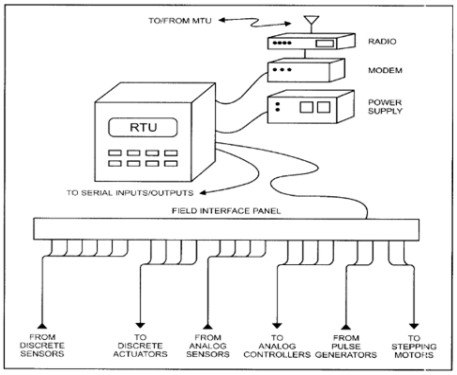

Fig. 3: The Remote Terminal Unit (RTU) [3]

D. Ethernet Switches

Ethernet switches (ES) are used to establish network connections between computers. Cables normally employed are twisted-Pair Metallic Cables, Coaxial Metallic Cables, Power Line Carriers, and Fiber Optic Cables. For high accuracy, low loss and long distance communications fiber optic cables are considered as best option.

E. Intelligent Electronic Devices (IEDs)

These normally constitute relays, meters and protocol converters. A relay is a device which senses abnormal condition in a system and signals the circuit breaker to trip and disconnect the faulted part from the healthy part of the system. The conventional electromechanical types are now replaced by microprocessor based digital relays also known as "numeric relays" offering higher accuracy with digital displays. Meters are devices used for measurement of various power system parameters. Protocol converters on the other hand are used to interface diverse control systems thereby enabling communications between devices having different communication protocols.

F. Disturbance Recorder

The relays employed in a power system are such that they are capable of recording disturbances, faults and sequence of events into their system. A disturbance recorder can access this information to permanently archive it. Thus the critical substation events are stored for troubleshooting and analysis purpose.

G. Time Synchronizing Equipment

The latest technology intelligent electronic devices (IEDs) have Ethernet connections which can be used to provide dedicated wiring for distribution of GPS, IRIG-B and 1PPS signals. With the emergence of new network protocols, new time synchronization methods are available. They are NTP/SNTP and IEEE 1588. Fig. 4 shows a schematic of distribution of IEEE 1588 time signal over the network and local conversion into IRIG-B in every IED cabinet [4].

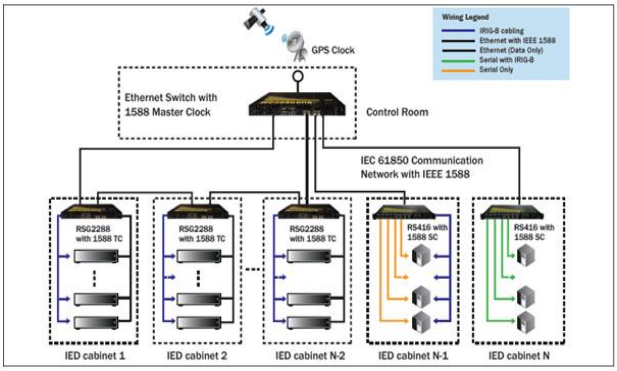

Fig. 4: Schematic of Distribution of IEEE 1588 time signal over the network and local conversion into IRIG-B in every IED cabinet [4]

III. SCADA ARCHITECTURE

SCADA architectures have been evolved keeping in mind modern computing requirements of a system. The figures show first generation (monolithic), second generation (distributed), third generation (networked) and fourth generation (internet of things) architectures.

A. The First Generation Systems

SCADA system had computing done using large minicomputers. These SCADA systems were independent with no connection to other system and with conventional communication protocols.

B. The Second Generation Systems

These systems have LAN connection provided between multiple stations where the information was shared in near real time. Here each station was allotted with certain task which reduced overall cost as compared to first generation systems.

C. The Third Generation Systems

These systems could be applied to geographically separated areas with the system spread over more than one LAN networks. It constituted the same distributed architecture as the second generation systems where complicated SCADA can be

broken down into simpler components and connected through communication protocols.

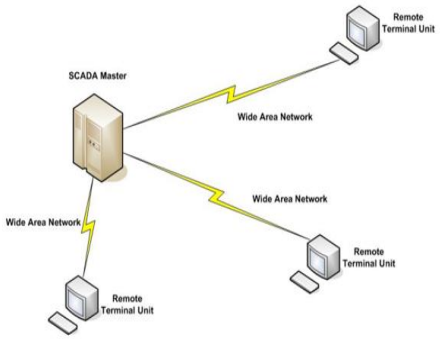

Fig. 5: The First Generation SCADA Architecture [5]

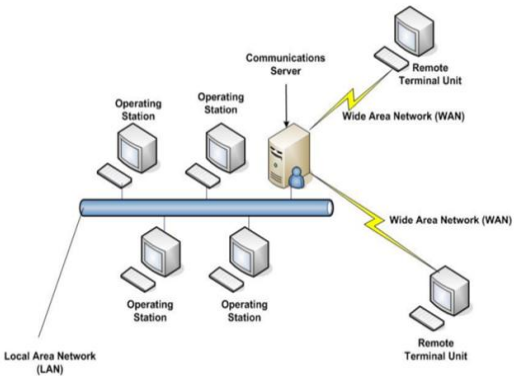

Fig. 6: The Second Generation SCADA Architecture [5]

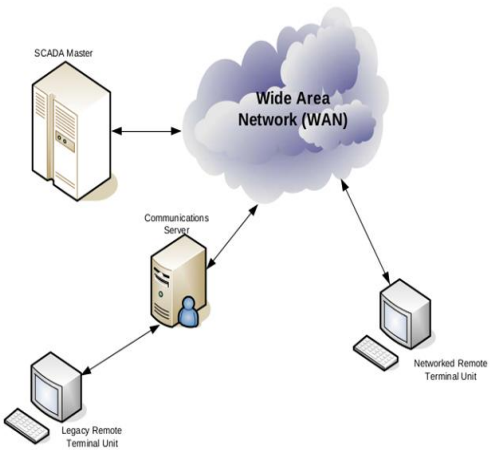

Fig. 7: The Third Generation SCADA Architecture [5]

D. The Fourth Generation Systems

These systems are latest of its kind with communications established using internet. With the recent cloud computing techniques, the "internet of things" technology has been widely adopted by SCADA systems in order to make integration and maintenance easy and to reduce infrastructure cost [6].

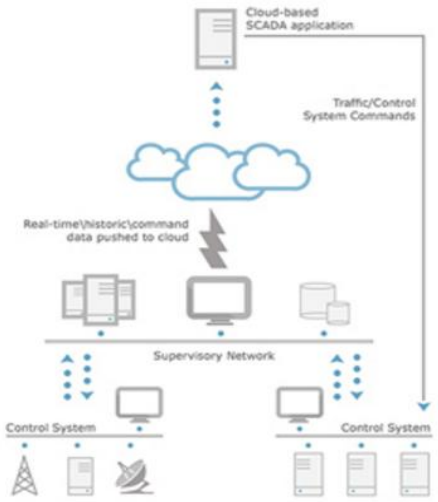

Fig. 8: The Fourth Generation SCADA Architecture [7]

IV. SCADA PROTOCOLS

A few SCADA protocols which have been in use conventionally along with more advance versions are explained in the coming section.

A. IEC 60870-5

- IEC 60870-5-1 (1990-02) specifies standards on formatting, coding and synchronizing variable and fixed lengths data frames in order to suffice data integrity requirements.
- IEC-60870-5-2 (1992-04) specifies the use of control field or optional address field for selection of link transmission procedures.
- IEC 60870-5-3 (1992-09) specifies rules for structuring application data units in transmission frames of telecontrol systems.
- IEC 60870-5-4 (1993-08) provides rules for defining information and data elements, particularly digital and analog process variables that are frequently used in telecontrol applications.
- IEC 60870-5-5 (1995-06) is involved with execution of standard procedures for telecontrol sytems by defining basic application functions.

B. Distributed Network Protocol-DNP3

DNP3 was specifically developed for SCADA RTUs for inter device communications. It was designed for both RTU-to-IED and master-to-RTU/IED communications. This protocol offers added advantages like flexible structure, high data integrity, minimized overhead, multiple application and open standard [8].

C. IEC 61850

It is a communication protocol which enables devices of different makes to talk to each other and which offers widespread features beneficial to electrical power system such as data modeling, numerous reporting schemes, fast transfer of events using GOOSE messaging, sampled data transfer etc [8],[9].

D. MODBUS RTU or American Standard Code for Information Interchange (ASCII) or TCP/IP

- Modbus is a serial communication protocol designed to meet industrial requirements. It has been built by keeping industrial applications in mind and has an ease in deploying and maintaining.
- Modbus RTU- uses compact binary data for flow of communication
- Modbus ASCII- uses ASCII characters for protocol communication.
- Modbus TCP-This is a Modbus variant used for communications over TCP/IP networks.

V. COMMUNICATION TOPOLOGIES

There are three basic ways to connect instruments with the RTU. In the "star" connection all instruments are individually connected to RTU and thus cannot talk with each other. In "Bus" type of layout, the instruments along with RTU have a common connection thereby enabling them to communicate on a common platform. Another is the "ring" type layout in which instruments and RTU are connected to form a ring and the information relayed shall be transferred from one station to another till it reaches the correct recipient.

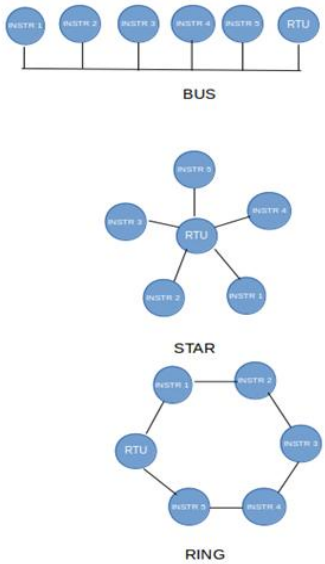

Fig. 9: Communication Topologies

VI. SCADA STANDARDS ORGANISATION

Following are the organizations involved in standardization of SCADA systems.

A. The Institute of Electrical and Electronics Engineers (IEEE)

The IEEE Standards Association is a membership organization that produces Information technology and electrical related standards that are used internationally.The following standards have been published by the IEEE with respect to SCADA systems:IEEE Std 999-1992 – IEEE Recommended Practice for Master/Remote Supervisory Control and Data Acquisition (SCADA) Communications and IEEE Std 1379-2000 – IEEE Recommended Practice for Data Communications Between Remote Terminal Units and Intelligent Electronic Devices in a Substation.

B. American National Standards Institute (ANSI)

The American National Standards Institute (ANSI) is a US based nonprofit and private organization that coordinates standardization and conformity assessment system.The Institute's goal is to enhance both the global competitiveness of U.S. quality of life and U.S. business by promoting and facilitating voluntary consensus standards and conformity assessment systems.

C. Electric Power Research Institute (EPRI)

The Electric Power Research Institute (EPRI) is a non-profit energy research consortium founded in 1973 for the benefit of utility members, their customers, and society. Their aim is to provide science and technology-based solutions of fundamental value to global energy customers. They do so by managing a far-reaching program of scientific research, technology development, and product implementation.

D. International Electro technical Commission(IEC)

The International Electro technical Commission (IEC) Technical Committee 57 Working Group 03 (TC57 WG03) was responsible to develop protocol standards for tele-control, tele-protection, and associated telecommunications for electric utility systems. It has created a group of five utility-specific protocol standards known as EC 60870-5, whoes description has been provided in the previous sections of this paper.

VII. SECURITY OF SCADA SYSTEMS

Most hardware and software vendors of SCADA systems have embraced Transmission Control Protocol/Internet Protocol (TCP/IP) and ethernet communications due to its numerous advantages. This gradual evolution towards more open standards have enable connection of diverse systems at the cost of a risk involving less access and control to technical personnel [10]. There have been several factors escalating the risks which are specific to control systems such as

- Use of standardized technologies with known vulnerabilities.
- Constraints on use of existing security technologies and practices.
- Connectivity of control systems to other networks.
- Widespread availability of technical information regarding control systems and insecure remote connections.

- Many tools and techniques have been evolved to counteract these security threats which require certain degree of flexibility in security configurations.

VIII. CONCLUSIONS AND FUTURE SCOPE

From the above it is clear that communications will be having maximum impact on SCADA systems. This is the area which will invite maximum changes as well. Apart from that the three prime most functional components namely RTU, MTU and communications equipments will also be experiencing gradual technological advances. There will be an increase in the sophistication of MTU based programming which will result in more purely automatic remote control applications being built into SCADA. The future promises improved security techniques for SCADA systems, improved quality of process instrumentation, decreasing price of computer hardware, increased used of application software to take care of process data thereby increasing affectivity and efficiency of systems.

Supervisory control and data acquisition is a broad domain with many complicated terminologies and practices. A simple lucid explanation of its basics is a must for a beginner looking to expand his knowledge in this field. The paper satisfies this requirement.

REFERENCES

[1] R. F. Khelifa and K. Jelassi, "Supervisory control and monitoring of an electric power distribution," *2015 16th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA)*, 2015.

[2] S. McFadyen, "How a digital Substation works," myElectrical Engineering, 2014. [Online]. Available: http://myelectrical.com/notes/entryid/245/how-a-digital-substation-works. Accessed: Jan. 29, 2017.

[3] S. A. Boyer, *SCADA: Supervisory control and data acquisition*, 3rd ed. Berkeley, CA, United States: ISA-The Instrumentation, Systems, and Automation Society, 2004.

[4] I. Media, *Industrial Ethernet book*. The Journal of Industrial Network Connectivity, 2010. [Online]. Available:http://www.iebmedia.com/index.php?id=7048&parentid=63&themeid=255&hft=58&showdetail=true&bb=1&PHPSESSID=7vnkp1qat4d7ih44gi90rfti00.

[5] R. Mcclanahan, "The benefits of networked SCADA systems utilizing IP-enabled networks," *2002 Rural Electric Power Conference. Papers Presented at the 46th Annual Conference (Cat. No. 02CH37360)*.

[6] D. Grozev, G. Spasov, M. Shopov, N. Kakanakov, and G. Petrova, "Experimental study of Cloud Computing based SCADA in Electrical Power Systems," *2016 XXV International Scientific Conference Electronics (ET)*, 2016.

[7] K. Wilhoit, "Next Generation SCADA?," *Control Global*.[Online].Available:http://www.controlglobal.com/industrynews/2013/wilhoit-scada-cloud-cybersecurity/.

[8] "IEEE Standard for Exchanging Information Between Networks Implementing IEC 61850 and IEEE Std 1815(TM) [Distributed Network Protocol (DNP3)]."

[9] R. Mackiewicz, "Overview of IEC 61850 and Benefits," *2005/2006 Pes Td*.

[10] A. Antonini, A. Barenghi, G. Pelosi, and S. Zonouz, "Security challenges in building automation and SCADA," *2014 International Carnahan Conference on Security Technology (ICCST)*, 2014.