Progression of Wireless Communications for SCADA Systems

Hathal Salamah A. Alwageed
Department of Computer Engineering and Network
Aljouf University, Saudi Arabia

ABSTRACT
The Supervisory Control and Data Acquisition (SCADA) systems are gathering information or data from different sensors nodes sent in remote areas and after that transmitted to a focal controller which then oversees and controls this information. Wireless communications for Supervisory Control and Data Acquisition (SCADA) is obliged to applications where wired correspondences to the remote site are excessively extravagant or it is excessively lengthy, making it impossible to build wired interchanges (communications). Draw on of wired or line communications are getting to be unfeasible as the extension is expanding broadening. We describe about the part of wireless communications for SCADA systems.

Keywords
SCADA, Protocols, Wireless communications

1. INTRODUCTION
SCADA systems are PC or computer controlled systems that screen and control industrial processes that exist in the physical world [inductiveautomation.com]. SCADA systems are included PCs, controllers, instruments; actuators, networks and interfaces that deal with the control of computerized modern procedures and permit investigation of those systems through information gathering. These processes incorporate industrial, infrastructure, and office/facility based processes, and are utilized as a part of a wide range of commercial enterprises, from electrical distribution systems to nourishment handling, to office security alerts [2]. Generally, SCADA communication occurred over radio, modem, or devoted serial lines. Normal wireless communications for a SCADA systems Point-Multipoint with one master polling multiple remote RTU's (Remote Terminal units) RTU or PLC's using RTU or PLC data communication protocols taking in protocols, for example, Modbus and DNP3. Each PLC or RTU at the remote site is modified with an interesting system address and those addresses are all designed or configured into the SCADA Host HMI. The SCADA Host then polls these addresses and stores the obtained information into its database. It will perform brought together centralized caution administration, information inclining/trend, operator control and display [M.choi et al]. Today, it is significantly more regular for SCADA communications to go over LAN or WLAN. Wireless communications can be connected to any setup where a focal or central controller needs to correspond with a remote gadget or versatile (mobile) bit of gear or equipment. Wireless communications for SCADA is obliged to applications where wired interchanges (communications) to the remote site is restrictively lavish or it is excessively time intensive, making it impossible to build wired interchanges.

2. THE SCADA SYSTEM COMMUNICATIONS
Premature SCADA systems information securing brings into play the strip chart recorders, meters panels, and lights. Not at all like the cutting edge SCADA systems there is an administrator which physically handles different control handles practiced supervisory control. These gadgets are still used to do supervisory control and information obtaining on force producing facilities, plants and industrial facilities [T. Reed] [T. h. Kim]. Telemetry is programmed transmission and estimation of information from remote sources by wire or radio or different means. It is additionally brought into play to send commands, projects and gets checking data from these remote areas. SCADA is the mix of telemetry and information/data obtaining. SCADA system is make out of gathering of the data, exchanging it to the focal site, doing any vital examination and control and afterward showing that data on the administrator screens. The obliged control activities are then gone back to the process [D. Bailey et al]. The protocols of SCADA are intended to be extremely conservative. Numerous are intended to send data just when the master station polls the RTU. Ordinary legacy SCADA protocols incorporate Modbus RTU, RP-570, Profibus and Conitel. These communication protocols are all SCADA-vendor explicit yet are broadly received and utilized. Standard protocols are IEC 60870-5-101 or 104, IEC 61850 and DNP3. These communication protocols are institutionalized and perceived by all major SCADA vendors. Large portions of these protocols now contain augmentations to work over TCP/IP. Despite the fact that the utilization of ordinary networking specifications or details, for example, TCP/IP, obscures the line in the middle of conventional and industrial networking, they each satisfy in a broad sense contrasting necessities [inductiveautomation.com]. The communication process over SCADA system includes a few distinctive SCADA system components. These incorporate the sensors and control relays, Remote Terminal Units (RTUs), SCADA master units, and the general communication system. Each of these parts is fundamental for successful SCADA communication. A system can adequately screen alerts and notices inside of the system just when these system parts work appropriately. For more finish checking of SCADA communications, administrators must convey progressed RTUs. The RTU is the place most SCADA communication is accumulated inside of the system. Values from inputs and yields, alluded to as SCADA points, and are sent from individual sensors to the RTU. The RTU is in charge of sending these SCADA communications to the master station, or Human-Machine Interface (HMI).

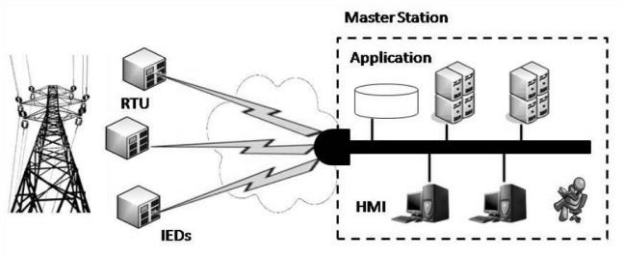

Fig 1: conventional SCADA structural design

Data securing or acquisitions begins at the RTU, IED (Intelligent Electronic Device) or PLC level and fuses meter readings and equipment status reports that are bestowed to SCADA as requisite. Data is then requested and outlined in such a course, to the point that a control room operator utilizing the HMI can settle on supervisory decisions to change or override common RTU (PLC) controls. Data may in like manner be maintained to a Historian, much of the time in view of an item or commodity Database Management System, to permit trending and other methodical investigation [T. h. Kim]. Starting late, OLE for Process Control (OPC) has transform into a by and large recognized response for intercommunicating particular hardware and software, allowing communication even between devices at first not proposed to be a bit of a industrial network. Central PC of the data securing (acquisition) system, arranged in the hydro power plant, gives estimations execution as showed by a preset system, the instrumentation existing starting now and remote exchanges by RS485 transport, using Master-Slave development displaying and IEC1107, Modbus RTU, ASCII protocols [C. Cepisca, et al]. Communication between the control center and remote destinations could be gathered into taking after four classes [gao.gov.new.items]:

1. Data acquisition: The control center sends poll "requests" messages to remote terminal units (RTU) and RTUs dump data to the control center. In particular, this joins status yield and measured value scan. The control center much of the time sends a status scan request to remote sites to get field devices status (e.g., OPEN or CLOSED or a snappy CLOSED-OPEN-CLOSED gathering) and a conscious quality yield requesting to get measured estimations of field devices. The measured values could be straightforward analogous or digitally coded values and are scaled into engineering format by the front-end processor (FEP) at the control center.
2. Control functions: The control center sends control commands to a RTU at remote site. These are accumulated into four subclasses: Individual device control, control messages to overseeing apparatus, sequential control schemes, and automatic control schemes.
3. Firmware download: The control center sends firmware downloads to remote destinations. For this circumstance, the poll message is immeasurable (e.g., greater that 64K bytes) than distinctive cases.
4. Broadcast: The control center may broadcast messages to repeat remote terminal units (RTUs). Case in point, the control center broadcasts a rising shutdown message or a set-the-clock-time message. Gotten data is subsequently checked at the control center to ensure that considered and processed values exist in sensible cutoff limits. The measure values monitored concerning rate-of-change and for steady trend monitoring. They are moreover recorded for post-faults or deficiencies examination. Status signs are seen at the control center concerning changes and time named by the RTUs. Existing communication associations between the control center and remote destinations work at low speeds could be on a solicitation of 300bps to 9600bps.

2.1. Wireless SCADA Communications

SCADA systems are made out of four critical parts: the master station or the central controller, PLC, RTU, IED to be deployed in remote stations, field-bus and sensors. Nearby the fieldbus, this setup is extended to the Internet. This setup is relative with a private system so that simply the central controller can have permission to the remote assets. The central controller also has an extension that goes about as a web server so that the SCADA customers and users can get to the data through the SCADA supplier webpage [R. J. Robles et al]. AS the system propels, SCADA systems are coming as per standard networking developments. Ethernet and TCP/IP based protocols are supplanting the more settled select standards. Though certain characteristics of frame-based network communication development (determinism, synchronization, protocol determination, environment suitability) have restricted the choice of Ethernet in a few specific applications, the predominant piece of business areas have recognized Ethernet systems for HMI/SCADA. Two or three shippers or vendors have begun offering application specific SCADA systems encouraged on remote stages over the Internet. This empties the need to setup and commission systems toward the end-customer's facility and endeavors security incorporates formally open in Internet development, SSL and VPN's. A couple concerns take in security [controleng.com], Internet connection reliability, and dormancy/latency.

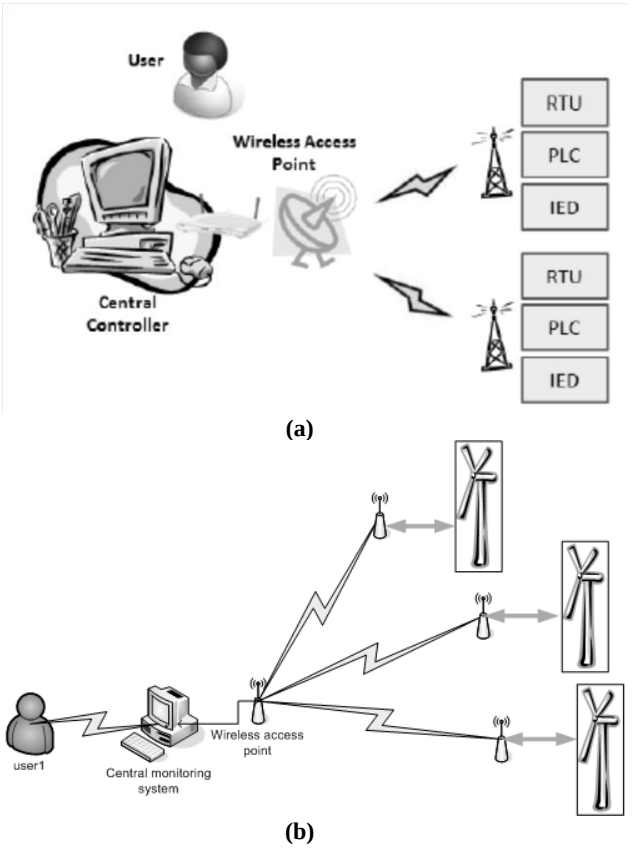

Fig 2 (a,b): Wireless SCADA

3. COMMUNICATION PROTOCOLS OF SCADA

As far as communication is concern so it is discriminating in SCADA systems. In communication, protocols are mandatory to be executed to keep up a key separation from miscommunications, hailing and acceptance slip-ups, and distinctive issues [R. J. Robles et al]. All together for SCADA systems to get its value, it needs a protocol for transmitting data. A rate of the SCADA protocols joins Modbus RTU, RP-570, Profibus and Conitel. These communication protocols are all SCADA-vendor specific yet are extensively gotten and exercised. Standard protocols are IEC 61850, IEC 60870-5-101 or 104, and DNP3. These communication protocols are systematized and saw by all major SCADA vendors. A noteworthy number of these protocols is presently enhanced and restrain expansions to work over TCP/IP [R. J. Robles et al]. Three of the most indispensable bit of a SCADA system are Master Station, Remote Terminal (RTU, PLC, IED) and the communication between them. Remembering the finished objective to have extraordinary communication between them, there must be a communication protocol. T101 and DNP3 are two of the most broadly perceived protocols at the moment. It is fundamental to make sense of which protocol should be associated if you are masterminding a SCADA system.

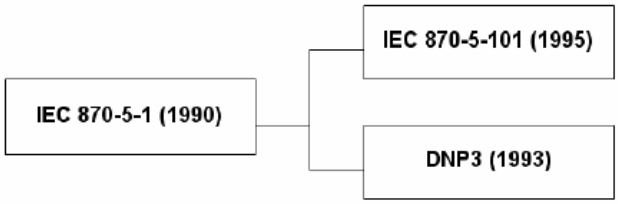

Fig 3: Expansion of Standard Protocol

These two open communication protocols that oblige interoperability between systems for telecontrol applications. Both are in no time fighting within the world business segment. DNP is extensively used as a piece of North America, South America, South Africa, Asia and Australia, while IEC 60870-5-101 or T101 is immovably reinforced in the Europe [R. J. Robles et al].

3.1. Standards

A) IEC 60870-5

IEC 60870-5 is the compilation of standards conveyed by the IEC (International Electro-technical Commission). It was made to give an open standard to the transmission of SCADA telemetry control and information [R. J. Robles et al]. It gives a point by point helpful portrayal to telecontrol equipments and systems for controlling topographically vast processes especially for SCADA systems. The standard is gotten ready for application in the electrical business ventures, and has data addresses that are especially proposed for such applications. It is similarly suitable to general SCADA applications in any industry. Regardless, IEC 60870-5 protocol is essentially used as a piece of the European countries electrical industries [C. Clarke, et al][Station Automation]. Right when the IEC 60870-5 was at initially completed in 1995 with the appropriation of the IEC 870-5-101 profile; it secured only transmission over reasonably low bandwidth bit-serial communication circuits. With the evidently limitless use of network communications advancement, IEC 60870-5 now also suits communication over systems employing the protocol suite of TCP/IP. This same gathering of change happened for DNP3 [R. J. Robles et al][Station Automation].

B) Distributed Network Protocol (DNP3)

The DNP3 or Distributed Network Protocol is an arranged set of communication protocols brought into play between components as a piece of process automation system [Station Automation][DNP Users Group]. It is by and large used is as a piece of utilities, for instance, water and electric associations. It is furthermore really possible to bring into play it in diverse utilities. It was especially made to empower trades between diverse sorts of data obtainment and control systems. It expects a basic part in SCADA system. It is utilized by SCADA Master Stations or Control Centers, RTU'S, and IED's. It is on a very basic level exercised for exchanges between a master station and IEDs or RTU's. DNP3 holds up multiple-master, multiple-slave and peer-to-peer communications. It holds up the operational strategies for polled and calm maneuver. The later is moreover suggested as reporting by exceptional case [R. J. Robles et al] [DNP Users Group].

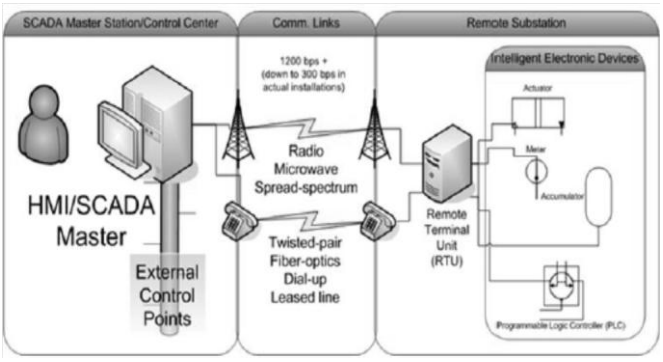

Fig 4: DNP3 general idea [DNP Users Group]

4. CONCLUSION

Actualizing or implementing a wireless infrastructure is especially helpful to new generation locales or offices since introducing wireless hardware can radically lessen establishment cost and time, diminish grant expenses, and take out trenching and running channel, while minimizing wire disappointment because of degradation and other ecological elements. Once more, using remote innovation lessens starting cost by totally uprooting the requirement for long separation direct internment simple (4-20 mA) cabling. Moreover, I/O analog to digital converter modules commonly utilized as a part of hardwire control instrumentation loops used by PLCs or RTUs are additionally diminished. SCADA systems wireless communications are a practical plan and is mandatory for applications when line or wire correspondences (communications) to the remotely sent units is prohibitively unrestrained or it is unreasonably repetitive, making it difficult to fabricate. It can supplant or extend the fieldbus to the web and decrease the setup outlays. This paper presents remote correspondence building configuration for SCADA systems.

5. REFERENCES

[1] What is SCADA? https://inductiveautomation.com/what-is-scada.

[2] Security for Critical Infrastructure SCADA Systems: http://www.sans.org/reading_room/whitepapers/warfare/1644.php.

[3] Supervisory Control And Data Acquisition (SCADA) Communication: http://www.dpstele.com/dpsnews/techinfo/scada/scada_communication.php.

[4] ”T. Reed”, “At the Abyss: An Insider’s,History of the Cold War, PresidioPress, (2004)March.

[5] ”T. h. Kim”, “Weather Condition Double Checking in Internet SCADA Environment”, WSEAS TRANSACTIONS on SYSTEMS and CONTROL, vol. 5, Issue 8, (2010) August, ISSN: 1991-8763, pp. 623.

[6] ”D. Bailey et al..”, “Practical SCADA for Industry”,(2003).

[7] ”C. Cepisca, et al...”, “Remote Data Acquisition System for Hydro Power Plants”,Proceedings of the 6th WSEAS International Conference on Power Systems, Lisbon, Portugal, (2006) September 22-24, pp. 59-64.

[8] ”R. J. Robles,et al...”, “Communication Security solution for internet SCADA”,Korean Institute of Information Technology 2010 IT Convergence Technology - Summer workshops and Conference Proceedings, (2010) May, pp. 461-463.

[9] Control Engineering: ”http://www.controleng.com/article/CA321065.html”.

[10] ”M.choi et al”, http://www.sersc.org/journals/IJSH/vol7_no5_2013/1.pdf”.

[11] GAO-04-628T - US Government Accountability Office: http://www.gao.gov.new.items/d04628t.pdf”.

[12] ”R. J. Robles, et al...”, “The Taxonomy of SCADA Communication Protocols”, Proceedings of the 8th KIIT IT based Convergence Service workshop & Summer Conference, Mokpo Maritime University (Mokpo, Korea), ISSN 2005-7334, pp. 23.

[13] ”C. Clarke, et al...”, “Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems”,(2004).

[14] ”Station Automation COM600 3.4 IEC 60870-5-101 Master (OPC) User's Manual”.

[15] ”DNP Users Group, “Overview of the DNP3 Protocol”,(2011), http://www.dnp.org/About/Default.aspx”.