International Journal of Smart Home
Vol. 7, No. 5 (2013), pp. 1-8
http://dx.doi.org/10.14257/ijsh.2013.7.5.01

# Wireless Communications for SCADA Systems Utilizing Mobile Nodes

Minkyu Choi

*Security Engineering Research Support Center, Daejon, Republic of Korea*

*freeant7@naver.com*

***Abstract***

*The Supervisory Control and Data Acquisition (SCADA) systems are collecting data from various sensors nodes deployed in remote locations and then transmitted to a central controller which then manages and controls this data. Wireless communications for SCADA is required to applications where wired communications to the remote site is too expensive or it is too time consuming to construct wired communications. Utilization of wired or line communications is becoming impractical as the scope is increasing widening. This paper discusses the role of wireless communications for SCADA systems.*

***Keywords:*** *SCADA systems, wireless communications, communication protocols*

## 1. Introduction

SCADA (supervisory control and data acquisition) systems are computer controlled systems that monitor and control industrial processes that exist in the physical world [1]. SCADA systems are comprised of computers, controllers, instruments; actuators, networks, and interfaces that manage the control of automated industrial processes and allow analysis of those systems through data collection. These processes include industrial, infrastructure, and facility-based processes, and are used in all types of industries, from electrical distribution systems, to food processing, to facility security alarms [2].

Traditionally, SCADA communication took place over radio, modem, or dedicated serial lines. Typical wireless communications for a SCADA system Point-Multipoint with one Master polling multiple remote RTU's (Remote Terminal Units) or PLC's using RTU or PLC data communication protocols including protocols such as Modbus and DNP3. Each PLC or RTU at the remote site is programmed with a unique system address and those addresses are all configured into the SCADA Host HMI. The SCADA Host then polls these addresses and stores the acquired data into its database. It will perform centralized alarm management, data trending, operator display and control [10].

Today, it is much more common for SCADA communications to travel over LAN or WLAN. Wireless communications can be applied to any setup where a central controller needs to communicate with a remote device or mobile piece of equipment. Wireless communications for SCADA is required to applications where wired communications to the

ISSN: 1975-4094 IJSH

remote site is prohibitively expensive or it is too time consuming to construct wired communications.

The rest of this paper is organized as follows: Section 2 SCADA systems communication and the conventional installation of the system are discussed. The architecture for wireless SCADA is presented in Section 3 and the concluding remarks in Section 4.

## 2. Communications for SCADA Systems

Early Supervisory Control and Data Acquisition (SCADA) system's data acquisition uses strip chart recorders, panels of meters, and lights. Unlike the modern SCADA systems, there is an operator which manually operates various control knobs exercised supervisory control. These devices are still used to do supervisory control and data acquisition on power generating facilities, plants and factories [4, 5]. Telemetry is automatic transmission and measurement of data from remote sources by wire or radio or other means. It is also used to send commands, programs and receives monitoring information from these remote locations.

SCADA is the combination of telemetry and data acquisition. Supervisory Control and Data Acquisition system is compose of collecting of the information, transferring it to the central site, carrying out any necessary analysis and control and then displaying that information on the operator screens. The required control actions are then passed back to the process [6].

SCADA protocols are designed to be very compact. Many are designed to send information only when the master station polls the RTU. Typical legacy SCADA protocols include Modbus RTU, RP-570, Profibus and Conitel. These communication protocols are all SCADA-vendor specific but are widely adopted and used. Standard protocols are IEC 60870-5-101 or 104, IEC 61850 and DNP3. These communication protocols are standardized and recognized by all major SCADA vendors. Many of these protocols now contain extensions to operate over TCP/IP. Although the use of conventional networking specifications, such as TCP/IP, blurs the line between traditional and industrial networking, they each fulfill fundamentally differing requirements [1].

The process of communication over a SCADA system involves several different SCADA system components. These include the sensors and control relays, Remote Terminal Units (RTUs), SCADA master units, and the overall communication network. Each of these parts is necessary for effective SCADA communication. A system can effectively monitor alarms and status updates within the network only when all of these system components function properly. For more complete monitoring of SCADA communications, operators must deploy advanced RTUs.

The RTU is where most SCADA communication is gathered within the system. Values from inputs and outputs, referred to as SCADA points, are sent from individual sensors to the RTU. The RTU is responsible for forwarding these SCADA communications to the master station, or Human-Machine Interface (HMI).

 

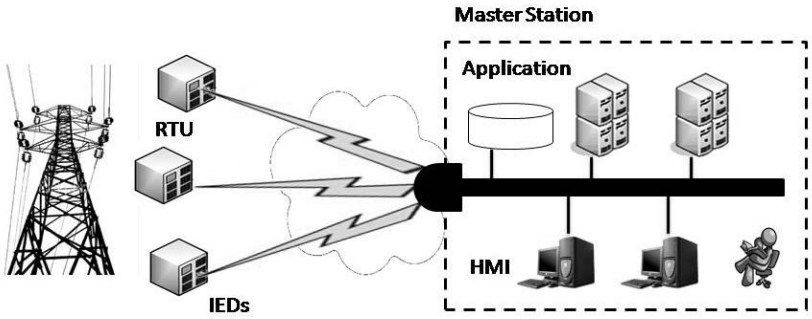


**Figure 1. Conventional SCADA Architecture**

Data acquisition begins at the RTU, IED (Intelligent Electronic Device) or PLC level and includes meter readings and equipment status reports that are communicated to SCADA as required. Data is then compiled and formatted in such a way that a control room operator using the HMI can make supervisory decisions to adjust or override normal RTU (PLC) controls. Data may also be fed to a Historian, often built on a commodity Database Management System, to allow trending and other analytical auditing [5].

Recently, OLE for Process Control (OPC) has become a widely accepted solution for intercommunicating different hardware and software, allowing communication even between devices originally not intended to be part of an industrial network. Central computer of the data acquisition system, located in the hydro power plant, provides measurements performance according to a preset program, the instrumentation existing at this time and remote communications by RS485 bus, using Master-Slave architecture and IEC1107, Modbus RTU, ASCII protocols [7].

Communication between the control center and remote sites could be classified into following four categories [11]:

- *Data acquisition:* the control center sends poll (request) messages to remote terminal units (RTU) and RTUs dump data to the control center. In particular, this includes status scan and measured value scan. The control center regularly sends a status scan request to remote sites to get field devices status (*e.g.*, OPEN or CLOSED or a fast CLOSED-OPEN-CLOSED sequence) and a measured value scan request to get measured values of field devices. The measured values could be analog values or digitally coded values and are scaled into engineering format by the front-end processor (FEP) at the control center.

- *Control functions:* the control center sends control commands to a RTU at remote sites. Control functions are grouped into four subclasses: individual device control (*e.g.*, to turn on/off a remote device), control messages to regulating equipment (*e.g.*, RAISE/LOWER command to adjust the remote valves), sequential control schemes (a series of correlated individual control commands), and automatic control schemes (*e.g.*, closed loop controls).

- *Firmware download:* the control center sends firmware downloads to remote sites. In this case, the poll message is large (*e.g.*, larger that 64K bytes) than other cases.
- *Broadcast:* the control center may broadcast messages to multiply remote terminal units (RTUs). For example, the control center broadcasts an emergent shutdown message or a set-the-clock-time message. Acquired data is automatically monitored at the control center to ensure that measured and calculated values lie within permissible limits. The measured values monitored with regard to rate-of-change and for continuous trend monitoring. They are also recorded for post-fault analysis. Status indications are monitored at the control center with regard to changes and time tagged by the RTUs. Existing communication links between the control center and remote sites operate at very low speeds (could be on an order of 300bps to 9600bps).

## 3. SCADA Communication Protocols

Communication is very important in SCADA systems. In communication, protocols are needed to be implemented to avoid miscommunications, signaling and authentication errors, and other problems [12]. In order for SCADA systems to obtain its functionality, it needs a protocol for transmitting data. Some of the SCADA protocols include Modbus RTU, RP-570, Profibus and Conitel. These communication protocols are all SCADA-vendor specific but are widely adopted and used. Standard protocols are IEC 61850 (in which T101 branched out), IEC 60870-5-101 or 104, and DNP3. These communication protocols are standardized and recognized by all major SCADA vendors. Many of these protocols is now improved and contain extensions to operate over TCP/IP [12].

Three of the most important part of a SCADA system are Master Station, Remote Terminal (RTU, PLC, IED) and the communication between them. In order to have good communication betweens them, there must be a communication protocol. DNP3 and T101 are two of the most common protocols today. It is important to determine which protocol should be applied if you are planning a SCADA system. The Standard Protocol Development is shown in Figure 8.

These two open communication protocols that provide for interoperability between systems for telecontrol applications. Both are now competing within the world market. DNP is widely used in North America, South America, South Africa, Asia and Australia, while IEC 60870-5-101 or T101 is strongly supported in the Europe [12].

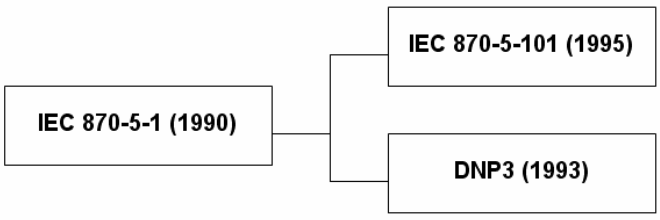


**Figure 2. Standard Protocol Development**

 

### 3.1. IEC 60870-5 Standards

IEC 60870-5 is the collection of standards produced by the IEC(International Electrotechnical Commission). It was created to provide an open standard for the transmission of SCADA telemetry control and information [12]. It provides a detailed functional description for telecontrol equipment and systems for controlling geographically widespread processes specifically for SCADA systems. The standard is intended for application in the electrical industries, and has data objects that are specifically intended for such applications. It is also applicable to general SCADA applications in any industry. But IEC 60870-5 protocol is primarily used in the electrical industries of European countries [13, 14].

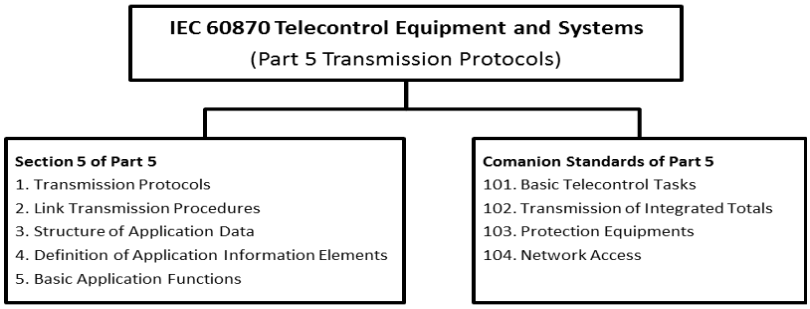


**Figure 9. IEC 60870 Structre**

When the IEC 60870-5 was initially completed in 1995 with the publication of the IEC 870-5-101 profile, it covered only transmission over relatively low bandwidth bit-serial communication circuits. With the increasingly widespread use of network communications technology, IEC 60870-5 now also provides for communications over networks using the TCP/IP protocol suite. This same sequence of development occurred for DNP3 [12, 14].

### 3.2. DNP3 Protocol

The DNP3 or Distributed Network Protocol is a set of communications protocols used between components in process automation systems [14, 15]. It is usually used is in utilities such as water and electric companies. It is also technically possible to use it in other utilities. It was specifically developed to facilitate communications between various types of data acquisition and control systems. It plays a crucial role in SCADA systems. It is used by SCADA Master Stations or Control Centers, Remote Terminal Units, and Intelligent Electronic Devices. It is primarily used for communications between a master station and IEDs or RTU's. DNP3 supports multiple-slave, peer-to-peer and multiple-master communications. It supports the operational modes of polled and quiescent operation. The latter is also referred to as reporting by exception [12, 15].

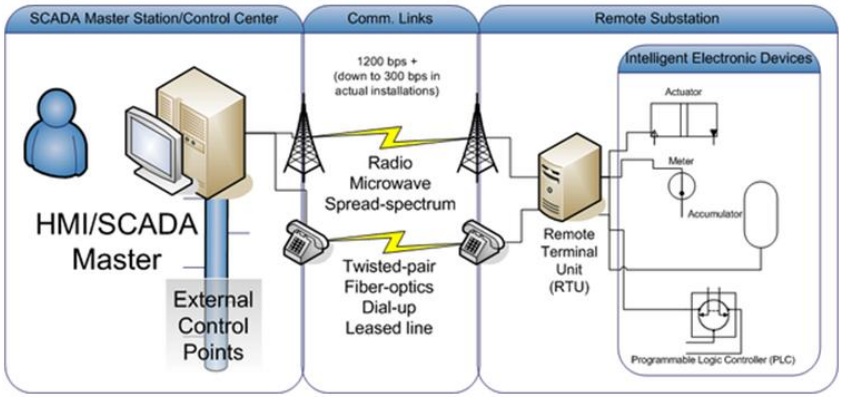


**Figure 10. Overview of the DNP3 Protocol [16]**

## 4. Wireless SCADA Communications

SCADA systems are composed of four major components: the master station or the central controller, plc/rtu/ied (deployed in remote stations), fieldbus and sensors. In Figure 2, the architecture of SCADA system that replaces the fieldbus with wireless communication. Along with the fieldbus, this setup is extended to the Internet. This setup is similar with a private network so that only the central controller can have access to the remote assets. The central controller also has an extension that acts as a web server so that the SCADA users and customers can access the data through the SCADA provider website [8].

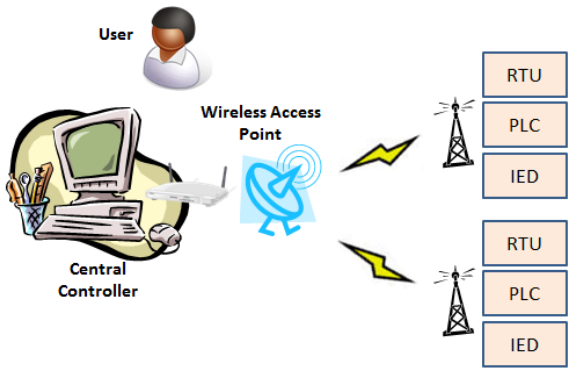


**Figure 3. Wireless Communications for SCADA Systems**

AS the system evolves, SCADA systems are coming in line with standard networking technologies. Ethernet and TCP/IP based protocols are replacing the older proprietary standards. Although certain characteristics of frame-based network communication technology (determinism, synchronization, protocol selection, environment suitability) have restricted the adoption of Ethernet in a few specialized applications, the vast majority of markets have accepted Ethernet networks for HMI/SCADA.

 

A few vendors have begun offering application specific SCADA systems hosted on remote platforms over the Internet. This removes the need to install and commission systems at the end-user's facility and takes advantage of security features already available in Internet technology, VPNs and SSL. Some concerns include security [9], Internet connection reliability, and latency.

## 5. Conclusion and Future Works

Wireless communications for SCADA systems is a practical solution and is required for applications when wired or line communications to the remotely deployed units is prohibitively expensive or it is too time consuming to construct. It can replace or extend the fieldbus to the internet and reduce the cost of installation. This paper presents wireless communication architecture for SCADA systems.

## References

[1] http://en.wikipedia.org/wiki/SCADA.
[2] A. Hildick-Smith, "Security for Critical Infrastructure SCADA Systems," SANS Reading Room, GSEC Practical Assignment, Version 1.4c, Option 1, (2005) February, http://www.sans.org/reading_room/whitepapers/warfare/1644.php.
[3] http://www.dpstele.com/dpsnews/techinfo/scada/scada_communication.php.
[4] T. Reed, "At the Abyss: An Insider's History of the Cold War", Presidio Press, **(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 and E. Wright, "Practical SCADA for Industry", **(2003)**.
[7] C. Cepisca, H. Anrei, E. Petrescu, C. Pirvu and C. Petrescu, "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, K. -T. Seo and T. -h. Kim, "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] D. Wallace, "Control Engineering. How to put SCADA on the Internet", **(2003)**, http://www.controleng.com/article/CA321065.html.
[10] http://www.scadalink.com/support/wireless-scada.html.
[11] GAO-04-628T, "Critical infrastructure protection; Challenges and efforts to secure control systems", Testimony Before the Subcommittee on Technology Information Policy, Intergovernmental Relations and the Census, House Committee on Government Reform, (2004) March 30, http://www.gao.gov.new.items/d04628t.pdf.
[12] R. J. Robles, M. -k. Choi and T. -h. Kim, "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, D. Reynders and E. Wright, "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.
[16] http://en.wikipedia.org/wiki/DNP3.