Integration of Wireless SCADA through the Internet

Tai-hoon Kim1*

*Corresponding Author
[1]Multimedia Engineering Department, Hannam University
133 Ojeong-dong, Daeduk-gu, Daejeon, Korea
taihoonn@hnu.kr

Abstract: - Supervisory Control and Data Acquisition systems collects data from various sensors at a factory, plant or in other remote locations and then sends this data to a central computer which then manages and controls the data. Traditionally, SCADA was designed to be in a private network utilizing line communication. As the scope becomes larger, and utilizing line communication becomes impractical therefore integrating wireless communication to SCADA was introduced. This work describes an Architecture of SCADA in wireless mode. The transmission of communication through the internet, its advantages and disadvantages are also discussed.

KeyWords: - Control Systems, SCADA, Mobility, Wireless

I INTRODUCTION

Control Systems like SCADA or Supervisory Control and Data Acquisition systems are computers, controllers, instruments; actuators, networks, and interfaces that manage the control of automated industrial processes and allow analysis of those systems through data collection .They are used in all types of industries, from electrical distribution systems, to food processing, to facility security alarms. [1]

Conventional SCADA communications has been Point-to-Multipoint serial communications over lease line or private radio systems. With the advent of Internet Protocol (IP), IP Technology has seen increasing use in SCADA communications. The connectivity of can give SCADA more scale which enables it to provide access to real-time data display, alarming, trending, and reporting from remote equipment.

In the following sections of this paper, SCADA systems is defined is discussed. The conventional installation of the system and the architecture for wireless SCADA is discussed.

II SCADA

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 terminal 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. [2]. Typically SCADA systems include the following components: [3]

1. Operating equipment such as pumps, valves, conveyors and substation breakers that can be controlled by energizing actuators or relays.Instruments in the field or in a facility that sense conditions such as pH, temperature, pressure, power level and flow rate.

2. Local processors that communicate with the site's instruments and operating equipment. This includes the Programmable Logic Controller (PLC), Remote Terminal Unit (RTU), Intelligent Electronic Device (IED) and Process Automation Controller (PAC). A single local processor may be responsible for dozens of inputs from instruments and outputs to operating equipment.

3. Short range communications between the local processors and the instruments and operating equipment. These relatively short cables or wireless connections carry analog and discrete signals using electrical characteristics such as voltage and current, or using other established industrial

communications protocols.

4. Host computers that act as the central point of monitoring and control. The host computer is where a human operator can supervise the process; receive alarms, review data and exercise control.

5. Long range communications between the local processors and host computers. This communication typically covers miles using methods such as leased phone lines, satellite, microwave, frame relay and cellular packet data.

The measurement and control system of SCADA has one master terminal unit (MTU) which could be called the brain of the system and one or more remote terminal units (RTU). The RTUs gather the data locally and send them to the MTU which then issues suitable commands to be executed on site. A system of either standard or customized software is used to collate, interpret and manage the data.

Supervisory Control and Data Acquisition (SCADA) is conventionally set upped in a private network not connected to the internet. This is done for the purpose of isolating the confidential information as well as the control to the system itself. Because of the distance, processing of reports and the emerging technologies, SCADA can now be connected to the internet. This can bring a lot of advantages and disadvantages which will be discussed in the sections.

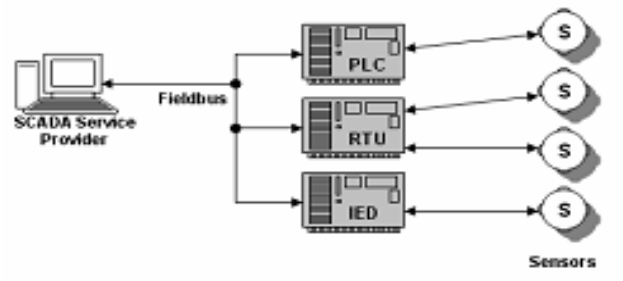

Figure 1. Conventional SCADA Architecture

Conventionally, relay logic was used to control production and plant systems. With the discovery of the CPU and other electronic devices, manufacturers incorporated digital electronics into relay logic equipment. Programmable logic controllers or PLC's are still the most widely used control systems in industry. As need to monitor and control more devices in the plant grew, the PLCs were distributed and the systems became more intelligent and smaller in size. PLCs (Programmable logic controllers) and DCS (distributed control systems) are used as shown in Figure 1.

III SCADA Components

SCADA systems typically have 3 major components: The Hardware Components, Software Components, and the Human Machine Interface. [4]

3.1 Hardware

Supervisory Control and Data Acquisition Systems usually have Distributed Control System components. PLCs or RTUs are also commonly used; they are capable of autonomously executing simple logic processes without a master computer controlling it. A functional block programming language, IEC 61131-3, is frequently used to create programs which run on these PLCs and RTUs. This allows SCADA system engineers to perform both the design and implementation of a program to be executed on an RTU or PLC. From 1998, major PLC manufacturers have offered integrated HMI/SCADA systems, many use open and non-proprietary communications protocols. Many third-party HMI/SCADA packages, offering built-in compatibility with most major PLCs, have also entered the market, allowing mechanical engineers, electrical engineers and technicians to configure HMIs themselves. [9]

The communications system provides the pathway for communication between the master station and the remote sites. This communication system can be wire, fiber optic, radio, telephone line, microwave and possibly even satellite. Specific protocols and error detection philosophies are used for efficient and optimum transfer of data.

The master station (or sub-masters) gather data from the various RTUs and generally provide an operator interface for display of information and control of the remote sites. In large telemetry systems, sub-master sites gather information from remote sites and act as a relay back to the control master station.

3.2 Software

Supervisory Control and Data Acquisition software can be divided into proprietary type or open type. Proprietary software are developed and designed for the specific hardware and are usually sold together. The main problem with these systems is the overwhelming reliance on the supplier of the system. Open software systems are designed to communicate and control different types of hardware. It is popular because of the interoperability they bring to the system. [1] WonderWare and Citect are just two of the open software packages available in the market for SCADA systems. Some packages are now including asset management integrated within the SCADA system.

3.2.1 SCADA Communication

SCADA systems have traditionally used combinations of radio and direct serial or modem connections to meet communication requirements, although Ethernet and IP over SONET / SDH is also frequently used at large sites such as railways and power stations. The remote management or monitoring function of a SCADA system is often referred to as telemetry. [10]

This has also come under threat with some customers wanting SCADA data to travel over their pre-established corporate networks or to share the network with other applications. The legacy of the early low-bandwidth protocols remains, though. SCADA protocols are designed to be very compact and many are designed to send information to the master station 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. It is good security engineering practice to avoid connecting SCADA systems to the Internet so the attack surface is reduced. [10]

RTUs and other automatic controller devices were being developed before the advent of industry wide standards for interoperability. The result is that developers and their management created a multitude of control protocols. Among the larger vendors, there was also the incentive to create their own protocol to "lock in" their customer base. A list of automation protocols is being compiled here.

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.

3.3 HMI

Many third-party HMI/SCADA packages, offering built-in compatibility with most major PLCs, have also entered the market, allowing mechanical engineers, electrical engineers and technicians to configure HMIs themselves.[11]

The goal of human-machine interaction engineering is to produce a user interface which makes it easy, efficient, and enjoyable to operate a machine in the way which produces the desired result. This generally means that the operator needs to provide minimal input to achieve the desired output, and also that the machine minimizes undesired outputs to the human.

Ever since the increased use of personal computers and the relative decline in societal awareness of heavy machinery, the term user interface has taken on overtones of the (graphical) user interface, while industrial control panel and machinery control design discussions more commonly refer to human-machine interfaces. [11]

The design of a user interface affects the amount of effort the user must expend to provide input for the system and to interpret the output of the system, and how much effort it takes to learn how to do this. Usability is the degree to which the design of a particular user interface takes into account the human psychology and physiology of the users, and makes the process of using the system effective, efficient and satisfying.

Usability is mainly a characteristic of the user interface, but is also associated with the functionalities of the product and the process to design it. It describes how well a product can be used for its intended purpose by its target users with efficiency, effectiveness, and satisfaction.

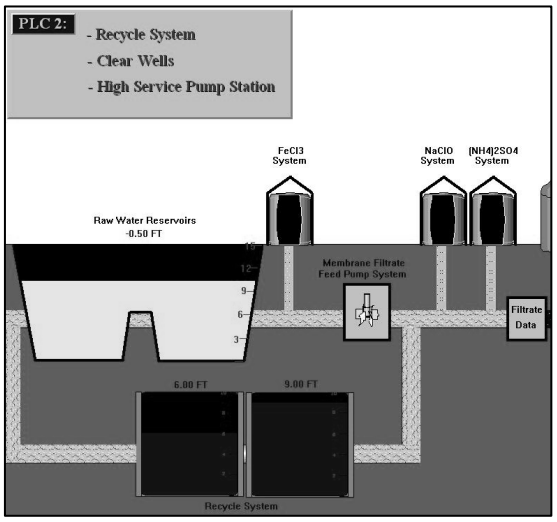

Figure 2. An Example of a SCADA Human Machine Interface

SCADA system includes a user interface which is usually called Human Machine Interface (HMI). The HMI of a SCADA system is where data is processed and presented to be viewed and monitored by a human operator. This interface usually includes controls where the individual can interface with the SCADA system. HMI's are an easy way to standardize the facilitation of monitoring multiple RTU's or PLC's (programmable logic controllers). Usually RTU's or PLC's will run a pre programmed process, but monitoring each of them individually can be difficult, usually because they are spread out over the system. Because RTU's and PLC's historically had no standardized method to display or present data to an operator, the SCADA system communicates with PLC's throughout the system network and processes information that is easily disseminated by the HMI. HMI's can also be linked to a database, which can use data gathered from PLC's or RTU's to provide graphs on trends, logistic info, schematics for a specific sensor or machine or even make troubleshooting guides accessible. In the last decade, practically all SCADA systems include an integrated HMI and PLC device making it extremely easy to run and monitor a SCADA system.

The HMI package for the SCADA system typically includes a drawing program that the operators or system maintenance personnel use to change the way these points are represented in the interface. These representations can be as simple as an on-screen traffic light, which represents the state of an actual traffic light in the field, or as complex as a multi-projector display representing the position of all of the elevators in a skyscraper or all of the trains on a railway.

3.4 Installation of SCADA Systems

SCADA systems are highly distributed systems used to control geographically dispersed assets, often scattered over thousands of square kilometers, where centralized data acquisition and control are critical to system operation. They are used in distribution systems such as water distribution and wastewater collection systems, oil and gas pipelines, electrical power grids, and railway transportation systems. A SCADA control center performs centralized monitoring and control for field sites over long-distance communications networks, including monitoring alarms and processing status data. Based on information received from remote stations, automated or operator-driven supervisory commands can be pushed to remote station control devices, which are often referred to as field devices. Field devices control local operations such as opening and closing valves and breakers, collecting data from sensor systems, and monitoring the local environment for alarm conditions.[3][4]

3.4.1 Conventional Supervisory Control and Data Acquisition

The function of SCADA is collecting of the information, transferring it back to the central site, carrying out any necessary analysis and control and then displaying that information on a number of operator screens. Systems automatically control the actions and control the process of automation.

Conventionally, relay logic was used to control production and plant systems. With the discovery of the CPU and other electronic devices, manufacturers incorporated digital electronics into relay logic equipment. Programmable logic controllers or PLC's are still the most widely used control

systems in industry. As need to monitor and control more devices in the plant grew, the PLCs were distributed and the systems became more intelligent and smaller in size. PLCs (Programmable logic controllers) and DCS (distributed control systems) are used as shown in Figure 3.

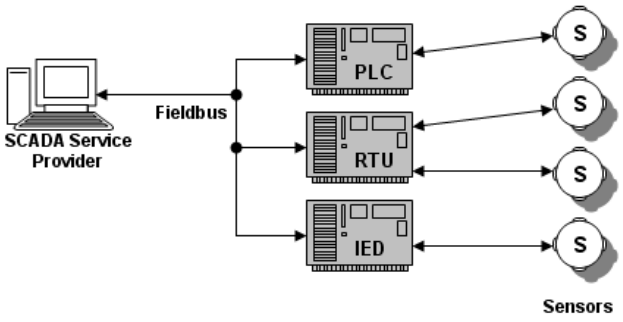

Figure. 3 Common SCADA Installation utilizing Remote Terminals (PLC/DCS, Sensors) and Master Station connected using a fieldbus.

IV Wireless Technology

Wireless communication is the transfer of information without the use of wires.[6] The distances involved may be short (a few meters as in television remote control) or long (thousands or millions of kilometers for radio communications). The term is often shortened to "wireless". It encompasses various types of fixed, mobile, and portable two-way radios, cellular telephones, personal digital assistants (PDAs), and wireless networking. Other examples of wireless technology include GPS units, garage door openers and or garage doors, wireless computer mice, keyboards and headsets, satellite television and cordless telephones. [7]

4.1 Wireless Services

The term "wireless" has become a generic and all-encompassing word used to describe communications in which electromagnetic waves or RF (rather than some form of wire) carry a signal over part or the entire communication path. Common examples of wireless equipment in use today include: [12]

- Professional LMR (Land Mobile Radio) and SMR (Specialized Mobile Radio) typically used by business, industrial and Public Safety entities.
- Consumer Two way radio including FRS Family Radio Service, GMRS (General Mobile Radio Service) and Citizens band ("CB") radios.
- The Amateur Radio Service (Ham radio).
- Consumer and professional Marine VHF radios.
- Cellular telephones and pagers: provide connectivity for portable and mobile applications, both personal and business.
- Global Positioning System (GPS): allows drivers of cars and trucks, captains of boats and ships, and pilots of aircraft to ascertain their location anywhere on earth.
- Cordless computer peripherals: the cordless mouse is a common example; keyboards and printers can also be linked to a computer via wireless.
- Cordless telephone sets: these are limited-range devices, not to be confused with cell phones.
- Satellite television: Is broadcast from satellites in geostationary orbit. Typical services use digital broadcasting to provide multiple channels to viewers.
- Wireless gaming: new gaming consoles allow players to interact and play in the same game regardless of whether they are playing on different consoles. Players can chat, send text messages as well as record sound and send it to their friends. Controllers also use wireless technology. They do not have any cords but they can send the information from what is being pressed on the controller to the main console which then processes this information and makes it happen in the game. All of these steps are completed in milliseconds.

Figure. 4 Wireless communication between devices

4.2 IEEE 802.11

IEEE 802.11 has been used interchangeably with Wi-Fi, however Wi-Fi has become a superset of IEEE 802.11 over the past few years. Wi-Fi is used by over 700 million people, there are over 750,000 hotspots (places with Wi-Fi Internet connectivity) around the world, and about 800 million new Wi-Fi devices every year. Wi-Fi products that complete the Wi-Fi Alliance interoperability certification testing successfully can use the Wi-Fi CERTIFIED designation and trademark. [12]

Not every Wi-Fi device is submitted for certification to the Wi-Fi Alliance. The lack of Wi-Fi certification does not necessarily imply a device is incompatible with Wi-Fi devices/protocols. If it is compliant or partly compatible the Wi-Fi Alliance may not object to its description as a Wi-Fi device though technically only the CERTIFIED designation carries their approval.

Wi-Fi certified and compliant devices are installed in many personal computers, video game consoles, MP3 players, smartphones, printers, digital cameras, and laptop computers. [12]

Wi-Fi technology builds on IEEE 802.11 standards. The IEEE develops and publishes some of these standards, but does not test equipment for compliance with them. The non-profit Wi-Fi Alliance formed in 1999 to fill this void — to establish and enforce standards for interoperability and backward compatibility, and to promote wireless local-area-network technology. As of 2010[update] the Wi-Fi Alliance consisted of more than 375 companies from around the world. Manufacturers with membership in the Wi-Fi Alliance, whose products pass the certification process, gain the right to mark those products with the Wi-Fi logo.

Specifically, the certification process requires conformance to the IEEE 802.11 radio standards, the WPA and WPA2 security standards, and the EAP authentication standard. Certification may optionally include tests of IEEE 802.11 draft standards, interaction with cellular-phone technology in converged devices, and features relating to security set-up, multimedia, and power-saving.

In the early 2000s, many cities around the world announced plans for city-wide Wi-Fi networks. This proved to be much more difficult than their promoters initially envisioned with the result that most of these projects were either canceled or placed on indefinite hold. A few were successful, for example in 2005, Sunnyvale, California became the first city in the United States to offer city-wide free Wi-Fi. In May, 2010, London, UK Mayor Boris Johnson pledged London-wide Wi-Fi by 2012.Both the City of London, UK and Islington already have extensive outdoor Wi-Fi coverage.

Wi-Fi also allows communications directly from one computer to another without the involvement of an access point. This is called the ad-hoc mode of Wi-Fi transmission. This wireless ad-hoc network mode has proven popular with multiplayer handheld game consoles, such as the Nintendo DS, digital cameras, and other consumer electronics devices.

Similarly, the Wi-Fi Alliance promotes a pending specification called Wi-Fi Direct for file transfers and media sharing through a new discovery- and security-methodology.

As of 2010, Wi-Fi technology has spread widely within business and industrial sites. In business environments, just like other environments, increasing the number of Wi-Fi access points provides network redundancy, support for fast roaming and increased overall network-capacity by using more channels or by defining smaller cells. Wi-Fi enables wireless voice-applications (VoWLAN or WVOIP). Over the years, Wi-Fi implementations have moved toward "thin" access points, with more of the network intelligence housed in a centralized network appliance, relegating individual access points to the role of "dumb" transceivers. Outdoor applications may utilize mesh topologies. [12]

V WIRELESS SCADA ARCHITECTURE

Wireless SCADA replaces or extends the fieldbus to the internet. This means that the Master Station can be on a different network or location. In Figure 3, you can see the architecture of SCADA which is connected through the internet. Like a normal SCADA, it has RTUs/PLCs/IEDs. Along with the fieldbus, the internet is an extension. The main problem in extending SCADA to a larger scope are the lines that will connect the field devices such as RTU, PLC, IED and sensors. It could be very costly and may encounter communication loss because of the distance. It is also impractical to connect. That is why having wireless communication can solve this problems.

The Wireless SCADA could also include the user-access to SCADA website. This is for the smaller SCADA operators that can avail the services provided by the SCADA service provider. It can either be a company that uses SCADA exclusively. Another component of SCADA is the Customer Application which allows report generation or billing.

This is setup like a private network so that only the master station can have access to the remote assets. The master 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.

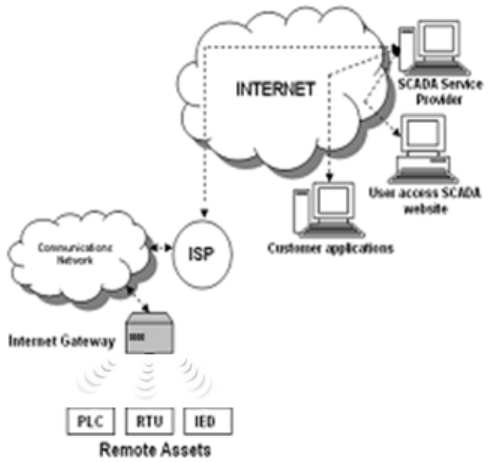

Figure 4. Wireless SCADA Architecture

VI Pros and Cons

Connecting SCADA wirelessly may carry on the vulnerability of a wireless network. Communication between devices can be easily intercepted and altered specially if it is not encrypted. Outsiders may gain control of the wireless network and control the devices. Also wireless network are less stable compared to wired network.

One may ask why we need to connect SCADA on even though there are a lot of issues surrounding it. The answer is because of many advantages it presents [8].

- Wide area connectivity and pervasive
- Routable
- Parallel Polling
- Redundancy and Hot Standby
- Large addressing range
- Integration of IT to Automation and Monitoring Networks
- Standardization

7 Conclusion

As of 2010, Wireless technology has spread widely within business and industrial sites. Wireless SCADA is required in those applications when wireline communications to the remote site is prohibitively expensive or it is too time consuming to construct wireline communications. In particular types of industry like Oil & Gas or Water & Wastewater, wireless SCADA is often the only solution due to the remoteness of the sites. Wireless SCADA replaces or extends the fieldbus to the internet. It can reduce the cost of installing the system. It is also easy to expand. In this paper we described an Architecture of SCADA in wireless mode. The transmission of communication through the internet, its advantages and disadvantages are also presented.

Acknowledgement. This work was supported by the Security Engineering Research Center, granted by the Korean Ministry of Knowledge Economy.

References

[1] Hildick-Smith, Andrew, “Security for Critical Infrastructure SCADA Systems,” (SANS Reading Room, GSEC Practical Assignment, Version 1.4c, Option 1, February 2005), http://www.sans.org/reading_room/whitepapers/warfare/1644.php

[2] D. Bailey and E. Wright (2003) Practical SCADA for Industry

[3] Andrew Hildick-Smith (2005) Security for Critical Infrastructure SCADA Systems

[4] Randy Dennison, "SCADA System Assessment", http://www.epgco.com/scada-system-assessment.html Accessed: October 2010

[5] Ramon Martinez-Rodriguez-Osorio, Miguel Calvo-Ramon, Miguel A. Fernandez-Otero, Luis Cuellar Navarette, "Smart control system for LEDs traffic-lights based on PLC", Proceedings of the 6th WSEAS International Conference on Power Systems, Lisbon, Portugal, September 22-24, 2006, pp. 256-260

[6] "Wireless Communication". sintef.no. http://www.sintef.no/content/page1____11881.aspx. Accessed: March 2008

[7] Wikipedia "Wireless", http://en.wikipedia.org/wiki/Wireless Accessed: October 2010

[8] Internet and Web-based SCADA http://www.scadalink.com/technotesIP.htm Accessed: January 2009

[9] Rosslin John Robles, Tai-Hoon Kim, "Communication Security for SCADA in Smart Grid Environment", WSEAS/CIEO International Conference on DATA NETWORKS, COMMUNICATIONS, COMPUTERS (DNCOCO '10), Faro, Algarve, Portugal, November 3-5, 2010

[10] Rosslin John Robles, Tai-Hoon Kim, "Architecture for SCADA with Mobile Remote Components", 12th WSEAS International Conference on AUTOMATIC CONTROL, MODELLING & SIMULATION (ACMOS '10), Catania, Italy, May 29-31, 2010

[11] Rosslin John Robles, Tai-Hoon Kim, "Double Checking Weather Condition in Internet SCADA Environment", 12th WSEAS International Conference on AUTOMATIC CONTROL, MODELLING & SIMULATION (ACMOS '10), Catania, Italy, May 29-31, 2010

[12] Wikipedia "Wi-Fi", http://en.wikipedia.org/wiki/Wi-Fi Accessed: October 2010

Prof. Tai-hoon Kim received B.E., M.E., and Ph.D. degrees from Sungkyunkwan University. Now he is a professor, School of Information & Multimedia, Hannam University, Korea. His main research areas are security engineering for IT products, IT systems, development processes, and operational environments.