Architecture of Wireless Supervisory Control and Data Acquisition System

Rosslin John Robles[1], Tai-hoon Kim[1*]
[*]Corresponding Author
[1]Multimedia Engineering Department, Hannam University
133 Ojeong-dong, Daeduk-gu, Daejeon, Korea
rosslin_john@yahoo.com, taihoonn@hnu.kr

Abstract: - SCADA is a system that 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. On its early days, SCADA was designed to be in a private network utilizing line communication. As the scope becomes larger, utilizing line communication becomes impractical therefore integrating wireless communication to SCADA was introduced. This paper describes an Architecture of SCADA in wireless mode. The transmission of communication through the internet, its advantages and disadvantages are also discussed.

Key-Words: - SCADA, Mobility, Wireless, Control Systems

1 Introduction

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.

2 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.

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.

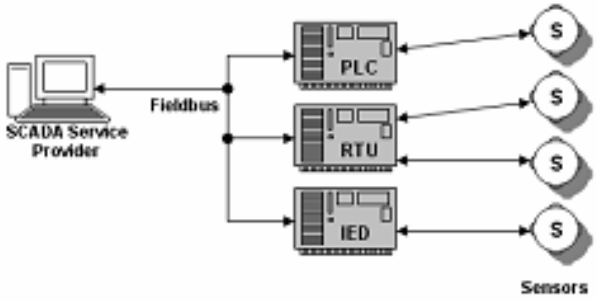

Figure 1. Conventional SCADA Architecture

3 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. The accurate and timely data allows for optimization of the plant operation and process. Other benefits include more efficient, reliable and most importantly, safer operations. These results in a lower cost of operation compared to earlier non-automated systems. Many other hardware are also based its functionality to those of PLC's. [5]

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.

3.2 Software

SCADA or 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.

3.3 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.

The goal of human-machine interaction engineering is to produce a user interface which makes it easy, efficient,

ISBN: 978-960-474-257-8

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.

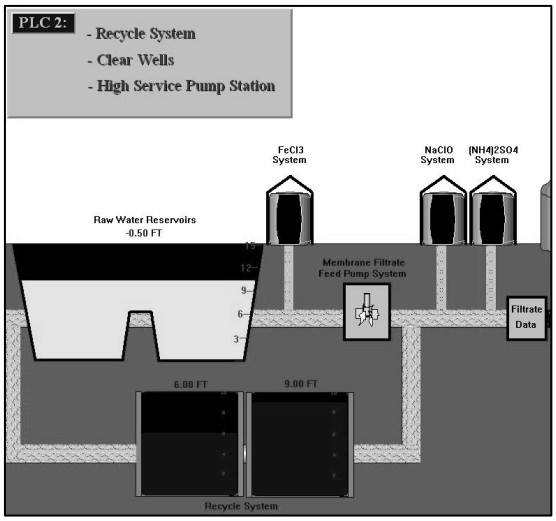

Figure 2. An Example of a SCADA Human Machine Interface

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.

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.

4 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]

5 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

ISBN: 978-960-474-257-8

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.

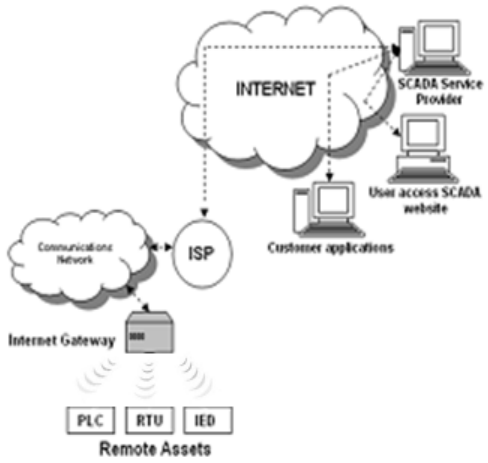

Figure 3. Wireless SCADA Architecture

6 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

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 discussed.

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