



Trends in SCADA for Automated Water Systems

Synchrony

Published: November 2001

Abstract

This paper provides a technical overview of recent trends in Supervisory Control and Data Acquisition (SCADA) for water and wastewater systems. By implementing new technologies developed for industrial applications, it is possible to reduce acquisition costs, improve system performance, and increase the options for technical support. An overview of SCADA technologies is presented from a historical perspective. Representative technologies are described and contrasted. Finally, practical information is presented to help prospective SCADA users design a system and choose a system vendor.

© 2001 Synchrony Inc. All rights reserved. Synchrony and Synchrony Industrial Controls are trademarks of Synchrony Inc.

Contents

- Introduction..... 2**

- What is a SCADA system? 3**
 - History of SCADA 3
 - Master Terminal Unit (MTU) 3
 - Remote Terminal Unit (RTU) 4
 - Communications Equipment 4

- Communication Options..... 7**
 - Atmospheric Media 7
 - Public Transmission Media 8
 - Advantages and Disadvantages of Media Types 9

- SCADA System Trends 15**
 - Proprietary RTU History 15
 - Non-Proprietary PLC History 15
 - SCADA Software 15
 - Future Trends 17

- Features, Benefits, and Current Issues..... 18**
 - Features 18
 - Benefits 19
 - Current Issues 19

- Conclusion 22**

- References 23**

- Glossary 24**

Introduction

The purpose of this white paper is to present recent trends in SCADA so that operators of water and wastewater systems can make informed decisions about the design of new systems and/or the upgrade of existing systems. The paper is written so that decision makers can quickly access relevant and up-to-date information without the burden of countless engineering details. Available technologies are presented, compared, and contrasted. Also presented is “real-world” experience so that owners with little SCADA experience can avoid many of the common pitfalls. This includes interesting advice and opinions from current operators of SCADA systems.

There are nearly 55,000 community water systems in the United States. Roughly 93% of these systems serve communities of less than 10,000 people. With the advent of open-architecture, PLC-based control and monitoring systems, cost-effective, high performance SCADA systems are available for even the smallest of water systems.

What is a SCADA system?

Supervisory control and data acquisition (SCADA) is a system that allows an operator to monitor and control processes that are distributed among various remote sites. There are many processes that use SCADA systems: hydroelectric, water distribution and treatment utilities, natural gas, etc. SCADA systems allow remote sites to communicate with a control facility and provide the necessary data to control processes. For many of its uses, SCADA provides an economic advantage. As the distance and inaccessibility to remote sites increases, SCADA becomes a better alternative than an operator or repairman's visiting the site for adjustments and inspections. Distance and accessibility are two major factors for implementing SCADA systems.

History of SCADA

SCADA can be traced to the development of telemetry from the first half of the century. Telemetry is the transmission and collection of data obtained by sensing real-time conditions. The technology of rockets and aircraft afforded man with the opportunity to investigate weather and planetary data. This required a simple way to get data from space that observers could not normally achieve. Manned stations on the surface of the Earth such as lighthouses, post offices, weather stations, etc., were able to collect and monitor data on weather. However, for accurate weather prediction, more detailed information was needed from the atmosphere. There were two questions to be answered. How could accurate data be gathered from the atmosphere and communicated back to a facility on the Earth's surface? And, how might data be gathered from a number of sites in one centralized location to record, analyze, and then predict the weather.

Typically, there are three major elements that make up a SCADA system:

1. The master terminal unit (MTU)
2. The remote terminal unit (RTU)
3. The communications equipment

The MTU monitors information from remote sites and displays information for the operator (Figure 1). The relationship between MTU and RTU is typically defined as a "master and slave" and refers to the communications protocol. The simplest form of a SCADA system is where a single MTU and RTU reside in the same building such as a small water treatment plant. The three major elements are further defined in the following sections.

Master Terminal Unit (MTU)

At the heart of the system is the master terminal unit (MTU). The master terminal unit initiates all communication, gathers data, stores information, sends information to other systems, and interfaces with operators. The major difference between the MTU and RTU is that the MTU initiates virtually all communications between the two.

The MTU also communicates with other peripheral devices in the facility like monitors, printers, and other information systems. The primary interface to the operator is the monitor or CRT that portrays a representation of valves, pumps, etc. As incoming data changes, the screen is updated.

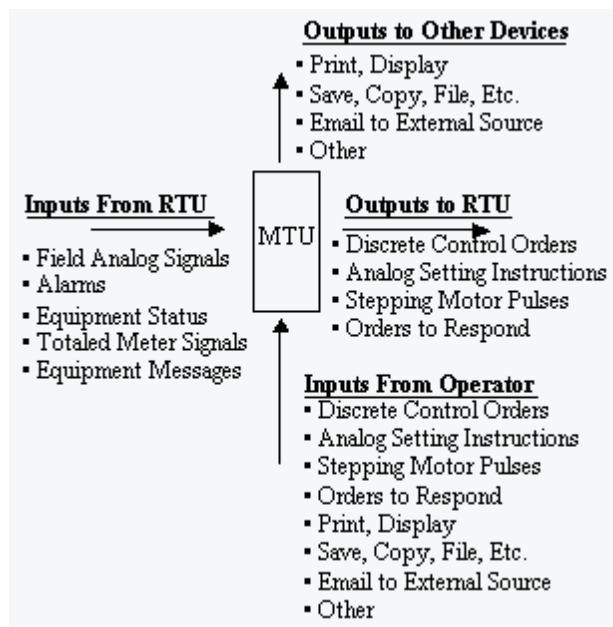


Figure 1. Inputs and Outputs of an MTU

Remote Terminal Unit (RTU)

Remote terminal units gather information from their remote site from various input devices, like valves, pumps, alarms, meters, etc. Essentially, data is either analog (real numbers), digital (on/off), or pulse data (e.g., counting the revolutions of a meter). Many remote terminal units hold the information gathered in their memory and wait for a request from the MTU to transmit the data. Other more sophisticated remote terminal units have microcomputers and programmable logic controllers (PLC) that can perform direct control over a remote site without the direction of the MTU. Figure 2 shows an example of outputs of the RTU to the MTU and to the field devices.

The RTU central processing unit (CPU) receives a binary data stream from the protocol that the communication equipment uses. Protocols can be open, like Transmission Control Protocol and Internet Protocol (TCP/IP) or proprietary. The RTU receives its information because it sees its node address embedded in the protocol. The data is then interpreted, and the CPU directs the appropriate action at the site.

Communications Equipment

Communication equipment is required for bi-directional communications between an RTU and the MTU. This can be done through public transmission media or atmospheric means. Figure 3 depicts the topology for SCADA and water supply for a small city. Note that it is quite possible that systems employ more than one means to communicate to remote sites. SCADA systems are capable of communicating using a wide variety of media such as fiber optics, dial-up, or dedicated voice grade telephone lines, or radio. Recently, some utilities have employed Integrated Services Digital Network (ISDN). Since the amount of information transmitted is relatively small (less than 50K), voice grade phone lines, and radio work well.

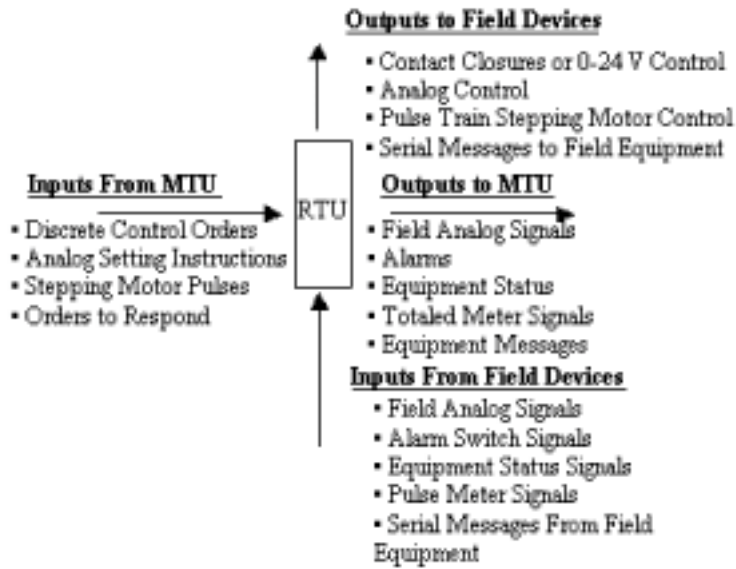


Figure 2. Inputs and Outputs of an MTU

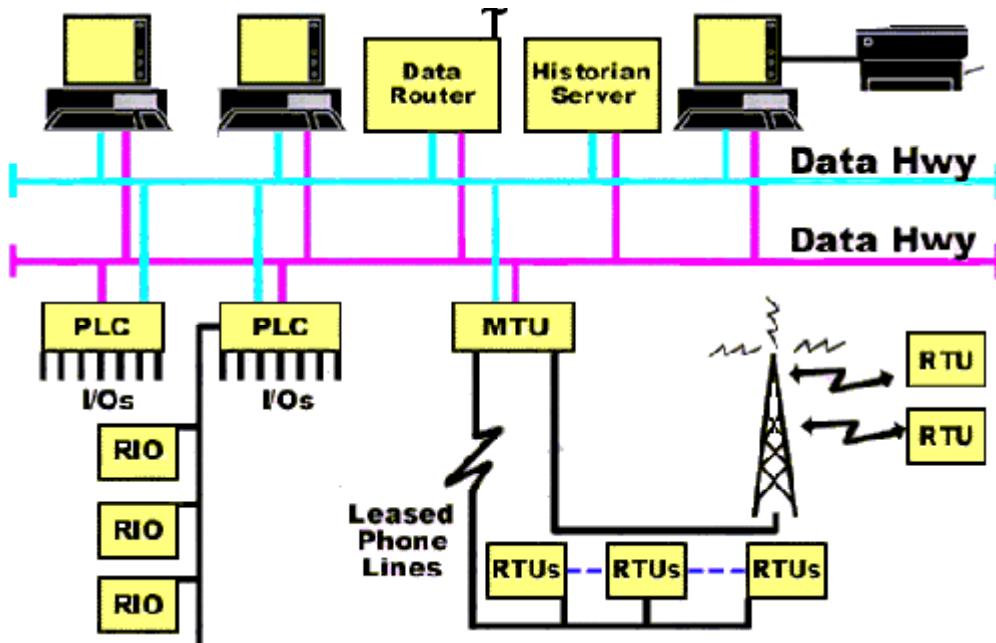


Figure 3. Topology of a SCADA

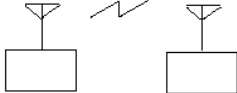

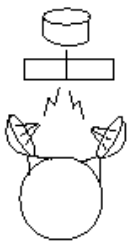
The topology of a SCADA system is the way a network is physically structured. For example: a ring, bus, or star configuration. It is not possible to define the typical SCADA system topology because it can vary with each system. Some topologies provide redundant operation and others do not. A redundant topology is highly recommended for water treatment plants and other critical control functions.

Communication Options

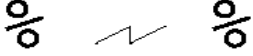


There are many options to select from when choosing the appropriate communication equipment. In this section, the options are classified according to whether or not a public medium is used. In all cases, the technology allows bi-directional communication between RTUs and MTUs.

Atmospheric Media

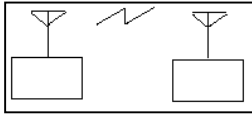
These are commonly referred to as “wireless” systems. Descriptions for the most common types of wireless systems are shown in the table below.

Type		Description
VHF/UHF Radio		VHF/UHF radio is a high-frequency electromagnetic wave transmission. Radio transmitters generate the signal, and a special antenna receives it.
Microwave Radio		Microwave radio is a high-frequency (GHz), terrestrial radio transmission and reception medium that uses parabolic dishes as antennas. The dishes are usually mounted on towers or on tops of tall buildings, since this is a line-of-sight technology.
Geosynchronous Satellite		Geosynchronous satellites use a high-frequency (GHz) radio transmission to route transmissions between sites. The satellite's orbit is synchronous with the earth's orbit so the satellite remains in the same position with respect to the earth. Satellites receive signals from and send signals to parabolic dish antennas.

Public Transmission Media

Type		Description
Switched Lines - Public Switched Telephone Network (PSTN) - Generally Switched Telephone Network (GSTN)		The dial-up network is furnished by a telephone company. This telephone line is the one that we commonly use to carry voice and data transmissions.
Private Leased Line (PLL)		PLL is a dedicated telephone line that is a permanent connection between two or more locations that is used for analog data transmission. The line is available 24 hours a day. For the line to be used for voice communication, a voice option must be installed.
Digital Data Service (DDS)		DDS is a special wide-bandwidth private leased line that uses digital techniques to transfer data at higher speeds and at a lower error rate than private leased lines. The line is available 24 hours a day.

Advantages and Disadvantages of Media Types



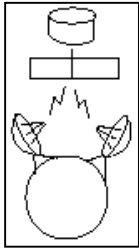
VHF/UHF Radio

Advantages/Capabilities	Disadvantages	Equipment Needed
<ul style="list-style-type: none"> ▪ The media links geographically-remote areas that are not accessible by phone lines. ▪ A constant connection exists. ▪ Transmissions can occur over rough terrain and over distances of less than 30 miles. ▪ There are monthly service fees because the equipment is owned. The only expense is operating and maintenance costs. ▪ Minimal transmission delay times exist. ▪ Newer “spread spectrum” type radios require no licensing from the FCC and can co-exist with other spread spectrum radios. 	<ul style="list-style-type: none"> ▪ Needs repeaters to extend transmission range over distances larger than 15 miles. ▪ Older radio types use frequencies that are allocated and regulated by the FCC. ▪ An initial expense is incurred for equipment, although much less expensive than microwave or satellite. 	<ul style="list-style-type: none"> ▪ transmitters ▪ receivers ▪ antennas ▪ repeaters needed to transmit longer distances and over hills and mountains



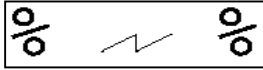
Microwave

Advantages/Capabilities	Disadvantages	Equipment Needed
<ul style="list-style-type: none"> ▪ The media links geographically-remote areas that are not accessible by phone lines. ▪ A constant connection exists. ▪ Transmissions can occur over very long distances over rough terrain. ▪ There are no monthly service fees because the equipment is owned. The only expense is operating and maintenance costs. ▪ Low transmission delay times. ▪ The larger bandwidth permits multiplexing many channels over one antenna. ▪ It is possible to lease circuits from other private companies. 	<ul style="list-style-type: none"> ▪ Transmission is limited to line-of-sight, i.e. you cannot transmit through mountains. The signal can experience distortion and interference. Also, atmospheric conditions (rain, snow, fog) can affect the signal. ▪ Most microwave link frequencies are allocated and regulated by the Federal Communications Commission (FCC). In urban areas, fewer data-transmission frequencies are available. ▪ Often, there is a large initial expense for equipment. 	<ul style="list-style-type: none"> ▪ transmitters ▪ receivers ▪ parabolic dish antennas ▪ repeaters needed to transmit longer distances and over hills and mountains



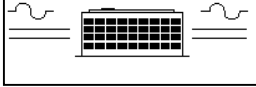
Geosynchronous Satellite

Advantages/Capabilities	Disadvantages	Equipment Needed
<ul style="list-style-type: none"> ▪ The transmissions can link sites almost anywhere on Earth. ▪ A constant connection exists. ▪ There is a monthly service fee. ▪ You can lease circuits just like you can lease dedicated telephone lines from a telephone. ▪ Company rates can be competitive with leased lines, depending on the total distance, remote station locations, and amount of data being transmitted. ▪ The media offers high reliability and data integrity. ▪ You do not need to “group” remote sites because the communication media usually is accessible. 	<ul style="list-style-type: none"> ▪ You can encounter longer transmission delays, measured in seconds rather than milliseconds. ▪ You incur a large initial cost for the satellite dish and supporting equipment. 	<ul style="list-style-type: none"> ▪ access to satellite ▪ satellite transmitters ▪ Earth-bound receiving parabolic-dish antennas



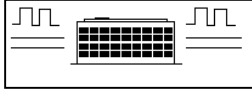
Switched Telephone Network

Advantages/Capabilities	Disadvantages	Equipment Needed
<ul style="list-style-type: none"> ▪ The media is cost effective for applications that require the following: <ul style="list-style-type: none"> – short, occasional data collection from remote sites that have access to a PSTN – a site that calls into a central location ▪ Often point-to-point applications have a dial-up connection as a back-up to the main link media. ▪ The phone company charges a monthly fee based on use - the number of local connections made and/or the time and distance of each long distance connection. ▪ The network supports communications rates of up to 33,600 bps. ▪ The network is a 2-wire connection that supports half-duplex modems and 2-wire, full-duplex modems. The topology is point-to-point. 	<ul style="list-style-type: none"> • Transmission is costly for long, frequent data collection from remote sites. • The lines can contain impairments that can cause modems to have error rates of less than 1 error per 1,000,000 bits. • The media cannot be used in areas that do not have access to the network, such as an offshore oil or gas well. <ul style="list-style-type: none"> ▪ Time is required to dial and establish each connection. ▪ Additional logic is required to automatically initiate a connection. ▪ Reliability is dependent on the local phone company. ▪ Monthly telephone fees. ▪ Quickly running out of phone numbers. 	<p>Use standard Bell or Consultive Committee for International Telephone and Telegraph (CCITT) modems.</p>



Private Leased Line (PLL)

Advantages/Capabilities	Disadvantages	Equipment Needed
<ul style="list-style-type: none"> • The media is cost effective for applications that require large amounts of data to be frequently collected from remote sites and/or require remote sites to have a constant connection to the master station. • Regardless of how much you use the line, the phone company charges a flat, monthly fee based on the following: <ul style="list-style-type: none"> – distance between sites – area of the country – type of line conditioning ▪ Leased lines have different levels of conditioning, or grades - the higher the grade, the greater the modem data rate that can be supported by the link, and the more the phone company charges for it. • The standard, unconditioned line, supports speeds of up to 28,800 bps. • Private leased lines provide a 4-wire connection. You can purchase modems that operate the circuit in either half- or full-duplex mode. You can also order a 4-wire multi-drop line. 	<ul style="list-style-type: none"> • The media cannot be used in areas that do not have access to the network, such as remote wells or tanks. • The lines can contain impairments that can cause modems to have error rates of more than 1 error per 1,000,000 bits. • Reliability is dependent on the local phone company • Monthly telephone fees 	<p>Use standard Bell or CCITT modems.</p>



Digital Data Services (DDS)

Advantages/Capabilities	Disadvantages	Equipment Needed
<ul style="list-style-type: none"> • DDS is a digital network that offers higher transmission rates and minimal, if any, line impairments. • The media is useful when an application requires very large amounts of data to be transferred between sites and needs a low data error rate. • Regardless of use, the phone company charges you a flat, monthly fee based on the distance between sites, the speed of the service, and the area of the country. • A constant connection exists. • Asynchronous communication rates are 2.4k, 4.8k, 9.6k, 19.2k, 38.4k, and 57.6k bps. • The network provides a four-wire connection and can be configured as a multi-drop. 	<ul style="list-style-type: none"> ▪ The media is costly for applications not needing to transmit large amounts of data quickly and at a low data error rate. • Reliability is dependent on the local phone company • Monthly telephone fees 	<p>Use standard integrated service unit, ISU (also called a data service unit [DSU] or channel service unit [CSU]). The ISU data rate must match that of the digital data service line, which operates at a fixed rate.</p>

SCADA System Trends

Proprietary RTU History

In the 1960s, many manufacturers started developing proprietary printed circuit boards that combined the RTU and communication functions in one small package. These circuit boards were engineered to perform a very specific function for a moderate cost. Various municipalities around the United States readily accepted these “all-in-one” proprietary RTU circuit boards. These RTUs have a fixed amount of inputs and outputs in which to monitor and control digital and analog field devices. These RTUs require constant communications with the MTU in order to function and they have a limited amount of on-board memory. They generally used a wide variety of programming languages that were not well known or supported. These proprietary “all-in-one” RTUs dominated the US market until the late 1980s, at which time the first “micro” PLCs were introduced.

Non-Proprietary PLC History

In the mid 1970s, driven by requirements in the automotive, steel, and nuclear power industries, many electrical equipment manufacturers like Allen-Bradley, General Electric, Square D, and Modicon developed large PLCs for automated systems. These PLCs were engineered to perform a very wide variety of functions and were industrially-hardened to survive extremely harsh environments. However, at that time, the PLCs were large, heavy and expensive. This changed in the late 1980s with the introduction of very small and cost-competitive “micro” PLCs. These new non-proprietary PLCs used a relatively common “ladder” programming language that was already well supported and understood in many industries. The PLCs are generally modular in nature and can be expanded to monitor and control additional field devices. As such, they are ideal for RTUs in SCADAs. For instance, they can be programmed to function even if communication with the MTU is lost.

SCADA Software

A SCADA system often includes a Human Machine Interface (HMI) to visualize the state of system variables, change setpoints, alert operators of critical conditions, and archive and present data trends. The trend is to use software packages developed originally for industry and develop applications specific to water systems. Some commonly used packages are RSVIEW (Rockwell Automation), IFIX (Intellution), InTouch (Wonderware), and Cimplicity (GE-Fanuc). With the advent of Windows NT, the HMI software can be reliably installed on common PC hardware in an office environment.

Figures 4 and 5 show two screens from a SCADA consisting of 16 remote sites. In the overview screen, the status of all sixteen sites is presented in a clear and precise manner. In addition to presenting the state of all pumps and the levels in the tanks, the status of all communications is presented. Figure 5 presents a more detailed look at one site in the system. From this screen, the current state of system variables can be monitored, past values of parameters can be visualized, and the control setpoints can be modified. The screens are specifically designed for ease of use for the operator.

The trend is to provide much of this capability using Web-based technology. In this case, a browser such as Internet Explorer or Netscape displays HTML pages from a web server that dynamically creates the web page using realtime data collected by the SCADA. These pages would then be published on the LAN of the water system operator, or if desired, on the Internet.

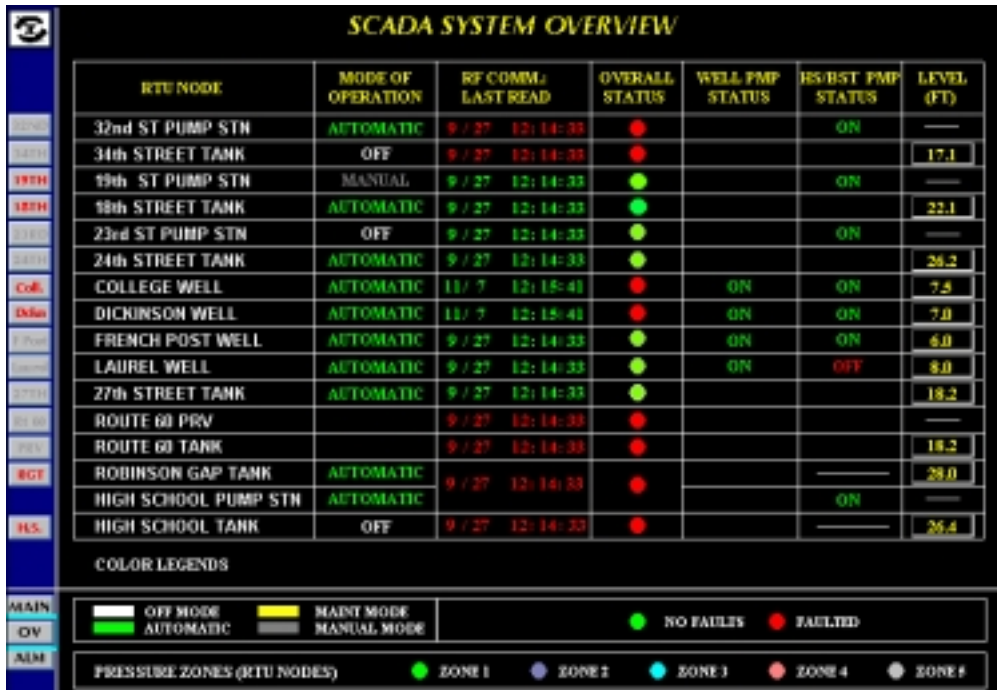


Figure 4. SCADA screen showing an status of several remote sites



Figure 5. SCADA screen showing status of a well site

Future Trends

The overall trend in the last decade has been to migrate toward a non-proprietary, open-architecture, PLC-based SCADA system. Some manufacturers like Allen-Bradley now make “micro” PLCs specifically for SCADA applications.

A PLC has more intelligence than an “all-in-one” RTU circuit board. Unlike an RTU, a PLC is able to control sites without the direction of a master.

An electrical controls magazine editor recently wrote, “the trend towards [PLCs as RTUs] becoming more functional and powerful will continue with advancements in the SCADA software.” This transfer of control away from master stations to increasingly “intelligent” remote PLCs will hasten the extinction of proprietary RTUs as users replace older proprietary systems with open architecture control systems based on industry standard components.

Features, Benefits, and Current Issues

This section details just some of the features and benefits of a properly engineered SCADA system. It also contains actual advice and opinions from operators of small and large water systems.

Features

Armed with some basic knowledge, an operator can specify a SCADA system that is quite functional. However, many operators are not familiar with some of the features of a PLC-based SCADA system. When a PLC-based SCADA is supplied by an experienced vendor, the following advantages can be realized:

- Because PLCs are industrially-hardened and contain no moving parts, they are extremely reliable and robust.
- A PLC-based RTU can be programmed for “intelligent” stand-alone operation during periods when there is a loss of communications with the MTU.
- The PLC programs can be completely documented with simple and extensive descriptions for easy understanding and troubleshooting of the system by technicians in the field.
- The modularity of a PLC can provide room for future growth and expansion.
- Security monitoring devices such as door switches, heat and motion detectors, and other security sensors can be integrated in the PLC program. The SCADA system can then automatically notify the proper authorities in a prescribed manner.
- The SCADA can be designed so that nearly all of the electrical components are available from local and national electrical distributors.
- Complete and extensive documentation can be provided with each PLC, including technical programming and support manuals.
- Standard on-board diagnostics can continuously monitor and display all status and fault information in easy to understand text.
- The Human Machine Interface (HMI) software for PLCs can provide extensive on-screen documentation and technical documents that include operator manuals, wiring diagrams, programs etc.
- PLC-based SCADAs can automatically collect and report required state and local data in a variety of formats including Microsoft’s Excel and Access.
- Reporting data can be collected and stored in the PLCs and also in the SCADA database at the MTU. This redundant collection of data provides a more robust reporting system.
- Through the use of automatic e-mail, paging and dial-up calling features, the SCADA can be designed to be extremely flexible and with enough power to keep operators and managers informed day and night.
- Integration of existing or future instrumentation such as valves, flow and turbidity meters can be performed easily and economically.
- “Web-based” access, which allows multiple users to access all data and setpoints from remote offices and homes, can be economically integrated into the SCADA.

Benefits

When supplied by an experienced vendor, water system operators typically realize some of the following benefits with PLC-based SCADAs:

- Drastically reduced number of customer complaints because of low system pressure or poor water quality. The condition of the water system and the water quality is known to the operators well before customers.
- Reduced number of man-hours required to troubleshoot a pump or other electrical device that did not operate as designed.
- Automated report generation is a major labor saving feature and facilitates compliance with local, state, and Federal regulatory agencies.
- Increased water quality because of the “intelligent” programming provided within each of the RTUs. Closed-loop monitoring of chlorine residual levels save chemicals and unnecessary wear on chemical feed systems.
- Reduced operating costs of a PLC-based SCADA translate to a superior return on investment (ROI) when compared to the typical proprietary system.
- Expensive service calls can be eliminated because of the complete documentation and troubleshooting guides provided with each system.
- An extensive network of state and national distributors supports nearly all non-proprietary hardware and software components.
- Local system integrators and electrical distributors can provide support.
- Local community colleges and technical schools have been teaching PLC programming and troubleshooting for years, thereby guaranteeing an adequate supply of trained technicians.
- Local industries have skilled electricians and technicians with experience in PLCs, also increasing the supply of trained technicians.

Current Issues

This section contains actual advice and opinions from current water system operator. Many operators have been quite vocal when asked to explain outstanding issues with their current SCADA systems. These hard-learned “lessons” have been broken down into those related to communication equipment, system design, technical support, and associated expenses.

Communication Equipment

- The reliability of communication is often a problem due to the use of obsolete hardware. A lot of the dial-up systems now in use have exceeded their design life and are not supported.
- If possible, avoid using a wireless radio frequency modem system that uses a single fixed frequency. For instance, systems located near major interstate highways may have problems due to CB radio interference.

- When possible, do not use “cell-based” systems for critical communication. It is possible for the cell switch to be overloaded with calls due to a local accident, fire or storm etc. For instance, a small accident on the interstate typically floods the cell communications system with a continuous stream of callers.
- Directional (yagi) antennas provide higher gain at the expense of the need for alignment, which can be difficult. If possible, avoid the use of directional antennas.
- A single lightning strike on a telephone pole can easily take out two dial-up modems at the same time. Be prepared by stocking spare modems during the summer months.

System Design

- Work with your SCADA vendor to help design the system at an early stage.
- Do not hesitate to visit or call other operators with SCADA systems in your region and ask their opinions about equipment and vendors.
- Think about the future! More local, state, and Federal regulations are coming and the SCADA system must be able to be expanded and easily accommodate the changes.
- Many operators say their SCADA systems are too complex for them to understand and support. Try to “keep it simple” whenever possible.
- Get the operators involved in the initial design of the SCADA system. They are the best source of day-to-day operation and planning information
- Many SCADA systems are not capable of operating in a “stand alone” or “intelligent” manner when communications are lost between the RTUs and the MTU. This is the most common fatal design flaw.
- Make sure that all RTU setpoints such as tank levels and pressures can be changed through the MTU by the operator without the need for outside support from a vendor.
- Lightning strikes account for most of the damage associated with RTUs. Be sure that the electrical equipment is properly protected. However, be aware that even a properly designed system may be damaged if directly hit by a lightning strike.
- Do not use electronic parts or components from consumer electronics stores or sources of similar quality. They may cost less than industrial-grade products but will certainly not survive as long.
- Check the age and history of the hardware. Is the hardware supplied by your vendor already obsolete before it is installed?

Support and Vendors

- Investigate the background and corporate stability of each SCADA system vendor. Look for long-term employees and verify the experience level of the engineers who are actually doing the work.
- Many vendors withhold essential documentation that would allow internal resources to support the system so that service fees may be collected for such routine tasks as changing setpoints. Be sure that your vendor agrees to deliver full technical documentation. If possible, ask to see examples of documentation that was delivered for previous projects.

- Do everything you can to learn, support and program the SCADA system with internal resources. This is the best defense against constant vendor headaches.
- Know the name and phone number of the telephone repair person that is most familiar with your local phone system. This person will be your best source of support if you have a dial-up modem system.
- Users of proprietary SCADA systems are vulnerable to lack of support and inability to replace failed components due to the obsolescence of proprietary products or the disappearance of a company due to consolidation or shakeout in the industry.

Associated Expenses

- Make sure you have a budget laid out for reasonable technical support and maintenance of the system.
- Be sure there is a budget available to send operators and technicians to training schools. Training internal resources can pay dividends later on due to decreased service calls by outside vendors.
- An expensive service contract does not always guarantee prompt and professional service. Some SCADA systems have been down for a month while waiting for a single source of technical support to arrive.
- Do not always go with the lowest bidder. The quality of the work and components suffer when vendors are “racing to the bottom” to win the low bid.
- The cost of operating and maintaining a SCADA system can be very expensive when the system is based on an “all-in-one” type circuit board.
- When you install a series of proprietary RTUs, do not be surprised when the price increases once a proprietary RTU is chosen as the “standard” for the system. A customer can be held “hostage” and be forced to pay an inflated price when dealing with proprietary equipment vendors.

Conclusion

The trend in automated water systems is to use SCADA systems based on PLCs, advanced communication systems, and PC-based software. This paper presents the basic knowledge needed to choose technology, design a system, and select a SCADA vendor.

For further information about SCADAs for automated water systems, please feel free to contact us at Synchrony. We have served government and industry since 1993, providing custom automation systems, automated water systems, production management software, magnetic bearing systems, and technology development. Synchrony has worked with many consulting engineering firms and water system operators in specifying, designing, integrating, installing, and maintaining automated water systems. In this area we offer:

- Control system architecture, design, and specification generation
- CAD-based layout and design of control enclosures and RTUs
- Fabrication of control panels in a UL-certified shop
- SCADA software programming from leading vendors
- Integration of industrially-hardened PLC-based control systems
- Field start-up, calibration, and training services
- Support and maintenance services for existing systems
- Project management services

Synchrony

6410 Commonwealth Drive

Roanoke, Virginia 24018

Phone: (540) 989-1541

Fax: (540) 989-0467

E-mail: info@synchrony.com

References

Boyer, Stuart, A. SCADA: Supervisory Control and Data Acquisition, Instrument Society of America, Research Triangle, NC. 1993.

Byrne, Bob, SCADA Mail List, "Email with Mr. Byrne", SCADA expert, scada@gospel.iinet.au (May 1997).

Engst, Adam, C. Internet Starter Kit, Macmillan Computer Publishing, Indianapolis, IN, 1996.

Ezell, Barry, "Supervisory Control And Data Acquisition Systems For Water Supply and Its Vulnerability to Cyber Risks" available on the internet at: <http://watt.seas.virginia.edu/~bce4k/home.html>. (August 1997).

Ezell, Barry, "Scenarios One and Two: Source to No 1 PS to No 1 Tank to No 2 PS to No 2 tank (High level) for a Master-Slave SCADA System", SCADA Consultants, SCADA Mail List, scada@gospel.iinet.au (August 1997).

Lambert, Robert, "An Interview in Newport News, Va.", President, Automation, Inc., June 12, 1997.

National Security Telecommunications Advisory Committee (NSTAC), "Information Assurance Task Force Risk Assessment", http://www.ncs.gov/n5_hp/reports/EPRA.html (October 10, 1997).

Rockwell Automation SCADA System Selection Guide Allen-Bradley, Publication AG-2.1. 1998.

Glossary

The following major terms are associated with most SCADA systems and related communications.

ACK See Acknowledgment.

Acknowledgment An ASCII control character that indicates the transmission and acceptance of data.

Asynchronous transmission A method of serial transmission where characters may be transmitted at unequal time intervals. Asynchronous transmission requires that each character contains start/stop elements so the receiver can detect the start and end of each character.

BCC Block-Check Character. The 2's complement of the 8-bit sum (modulo-256 arithmetic sum) of all data bytes in a transmission block. It provides a means of checking the accuracy of each message transmission.

Bridge An interface between links in a communication network that routes messages from one link to another when a station on one link addresses a message to a station on another link.

CRC Cyclic redundancy check. An error detection scheme where all of the characters in a message are treated as a string of bits representing a binary number. This number is divided by a predetermined binary number (a polynomial) and the remainder is appended to the message as a CRC character. A similar operation occurs at the receiving end to prove transmission integrity.

CTS Clear-To-Send. A signal from the DCE that tells the transmitting device (DTE) to start transmitting data.

DCD Data Carrier Detect; a signal indicating that the carrier is being received from a remote DCE.

DCE Data Communication Equipment 1) Equipment that provides the functions required to establish, maintain, or terminate a connection. 2) The signal conversion and coding required for communication between data terminal equipment and data circuits. Examples include modems, line drivers, coaxial cable, satellite links, etc. DCE may or may not be an integral part of a computer.

DCS Distributed Control System, a system which while being functionally integrated, consists of subsystems which may be physically separate and remotely located from one another. This type of control system does not rely upon a SCADA PC in order to function.

DF1 The Allen-Bradley asynchronous protocol.

Digital Data Service (DDS) A special wide-bandwidth Private Leased Line (PLL) that uses digital techniques to transfer data at higher speeds and lower error rate than voice-band, analog PLLs. The line is available 24 hours a day.

DSR Data-Set-Ready. A signal that indicates the modem is connected, powered up, and ready for data transmission.

DTE Data Terminal Equipment. Equipment that is attached to a network to send or receive data, or both. Programmable controllers, work-stations, and interface modules are examples of DTEs.

DTR Data-Terminal-Ready. A signal that indicates the transmission device (terminal) is connected, powered up, and ready to transmit.

EOT End Of Transmission; an ASCII control character that indicates the end of a data transmission.

FCC Federal Communication Commission (United States).

Full-Duplex Circuit A physical circuit that allows simultaneous, bi-directional transmission of data; also called a "four-wire" circuit.

Full-Duplex Modem A modem that is capable of simultaneous, bi-directional transmissions.

Full-Duplex Protocol 1) A mode of operation for a point-to-point link with two physical circuits, in which messages or transmission blocks can be sent in both directions at the same time. 2) Contrasted with two-way alternate.

General Switched Telephone Network International version of a Public Switched Telephone Network.

Half-Duplex Circuit A physical circuit that allows transmission of data in either direction but not at the same time.

Half-Duplex Modem A modem that sends and receives messages on carriers of the same frequency. Therefore, simultaneous, bi-directional transmissions are not possible.

Half-Duplex Protocol 1) A mode of operation for a point-to-point or multipoint baseband link with two physical circuits, in which messages or transmission blocks can be sent in one direction or the other but not both at the same time. 2) Contrasted with two-way simultaneous. The master station-to-remote station communication uses a half-duplex protocol.

Handshake A series of signals between a computer (DTE) and a peripheral device (DCE; e.g., a modem) that establishes the parameters required for passing data.

Integrated Service Unit (ISU) Data communication equipment for a digital data network, which serves as the data transmitting and receiving device. An ISU is a combination of a digital service unit (DSU) and a channel service unit (CSU).

I/O Rack An I/O addressing unit that corresponds to 8 input image table words and 8 output image table words.

Link A data channel established between two or more stations.

Master Station A device (programmable controller with I/O modules or a workstation) that sends data to and collects data from devices connected on a point-to-multipoint, half-duplex network.

Modem A device that modulates digital information from a programmable controller or computer to an analog signal that is transported over phone lines, radio waves, and satellite transmissions and demodulates the analog data back into digital data at the receiving site.

Modem Handshaking A signaling protocol used for transferring information between devices in a synchronized manner at a rate acceptable to both devices. It may be accomplished by hardware or software.

Multidrop Link 1) A link that has more than 2 stations. 2) Contrasted with point-to-point link.

NAK Negative Acknowledgment. An ASCII control character transmitted by a receiver as a negative response to the sender.

Node A station on a network.

Octal Numbering System A numbering system that uses only the digits 0-7; also called base-8.

Packet The transmission unit exchanged at the network layer.

Packet Radio Modem An intelligent radio modem that organizes the data it receives from the transmitting station into packets. The modem places a header and a trailer around the data before it transmits the data to the destination device. The header can also contain routing information. Packet radio modems also perform their own data error checking and will re-transmit the data if an error is encountered.

PAD Packet assembler/disassembler. Equipment used to assemble and disassemble data packets for transmission on a packet-switching network such as a satellite system.

Parallel port An electrical connection on a computer capable of transmitting or receiving two or more bits of data at one time; the communications port to which such devices as parallel printers can be attached.

PLC. A programmable logic controller (PLC) is a solid-state member of the computer family, using integrated circuits instead of electromechanical devices to implement control functions. They are capable of operating in very harsh environments and are extremely reliable. PLCs have inputs, a central processing unit and outputs. The central processing unit reads the inputs, executes the program and then writes to the outputs according to the program.

Point-to-multipoint A network where connections exist between one master station and multiple remote stations.

Point-to-point A network where a connection is made between two and only two terminal installations.

Poll When the master station sends a message to a remote station that allows the remote station an opportunity to return a response to the master or another remote station. In this manual, when the master polls a remote station, it is not initiating a read request.

Polling cycle The order and frequency in which network nodes in a poll list are polled.

Poll List A list of nodes or stations on a network to be polled on a regular and repeated basis.

Protocol A set of conventions governing the format and timing of data transmission between communication devices, including handshaking, error detection, and error recovery.

Private Leased Line Network (PLL) A dedicated voice-band telephone line between two or more locations primarily used for data transmission.

Processors A collective name used to refer to programmable logic controllers (PLCs). See PLCs.

Proprietary System A control system made up of unique components from a manufacturer(s) that limits end-user access to developed protocol, programming, parts and technical information. Distributors of proprietary components are usually the only source for the special parts and technical support within an assigned geographical sales area.

Public Switched Telephone Network (PSTN) The standard dial-up telephone network originally used for voice communication.

Redundancy The ability of certain components of a system to assume functions of failed components without adversely affecting the performance of the system itself. An example of redundancy in SCADA is additional communication mediums between the master and remote terminal unit.

Robustness The degree of insensitivity of a system design to errors in the estimates of those parameters affecting design choice. Robustness reduces the sensitivity of the system to extraordinary conditions. In

SCADA, robustness may best be characterized in systems where remote terminal units operate under conditions where communication from the master terminal unit is delayed or interrupted. In general, SCADA systems with distributed intelligence are inherently more robust than centrally controlled systems.

Security The ability of certain components of the system to deter, detect, and defend against attacks. In water supply systems security is multifaceted. There are numerous examples like fences, locks, alarms, and sensors. In SCADA, sensors, and alarms provide feedback on water quality. Some SCADA systems also have features that work to prevent unauthorized access or use. In general, secure systems have properties that reduce the likelihood of successful attacks.

RS-232 An EIA electrical connection standard, most often used as a standard interface for serial binary communication between data terminal equipment and data communications equipment.

RTS Request To Send. A request from the DTE module to the modem to prepare to transmit. In response, the modem typically sends out a data carrier signal and turns on CTS.

RTU Remote Terminal Unit. See remote station.

RXD Received Data; a serialized data input to a receiving device.

Remote Station A device (programmable controller with I/O modules) that is located in a remote site away from the master station and that controls I/O points at the remote site. A remote station accepts commands from and can send data (if capable) to a master station via a telemetry network.

SCADA Supervisory Control and Data Acquisition.

Security The ability of certain components of the system to deter, detect, and defend against attacks. In water supply systems security is multifaceted. There are numerous examples like fences, locks, alarms, and sensors. In SCADA, sensors, and alarms provide feedback on water quality. Some SCADA systems also have features that work to prevent unauthorized access or use. In general, secure systems have properties that reduce the likelihood of successful attacks.

Slave See remote station.

Slave Protocol See Half-Duplex Protocol.

Serial Port An electrical connection on a computer that handles data bits one after another; the communications port (COM1 or COM2) to which devices such as a modem, a mouse, or a serial printer can be attached.

Spurious Character A false or unexpected character received when none is expected.

Standard Radio Modem A standard radio modem is an assembly that contains both a radio and a modem, which transmits data without any special handling. Data error checking is the responsibility of the receiving station (DTE).

Station Any programmable controller, computer, or data terminal connected to, and communicating by means of, a data channel; a device on a network.

Station Addressing The syntax allowing packets to be routed correctly between master and remote stations.

Synchronous Transmission A type of serial transmission that maintains a constant time interval between successive events.

Telemetry Transmission and collection of data obtained by sensing real-time conditions.

Topology The way a network is physically structured. Example: a ring, bus, or star configuration.

Transceiver An electronic device that operates as both a radio transmitter and receiver.

TXD Transmitted Data; an output from the module that carries serialized data.