

The Sage Advisor

SCADA, SECURITY & AUTOMATION NEWSLETTER

Volume 22, Issue 1 • Spring/Summer 2012

A Publication of Sage Designs, Inc.

SCADA Security: Challenges and Solutions

Protecting Critical Infrastructure Includes Secure SCADA

Supervisory Control and Data Acquisition (SCADA) systems are typically used for monitoring and controlling geographically remote operations. In relative obscurity, these extensive control systems perform behind-the-scenes, collecting sensor measurements and operational data from the field, processing and displaying this information, and relaying control commands to local or remote equipment. Although SCADA systems are employed around the world in numerous industries, the average citizen is unaware of their critical importance. However, this is quickly changing, as more information about the cyber vulnerabilities of utility SCADA systems is publicly available.

There is good reason why SCADA systems are getting the attention of hostile governments and competitors, terrorist groups, disgruntled employees, and other malicious intruders—they offer the huge

potential to acquire confidential data and disrupt operations.

SCADA systems control some of the most vital infrastructure in industrial and energy sectors, from oil and gas pipelines to nuclear facilities to water treatment plants. Critical infrastructure is defined as the physical and IT assets, networks and services that if disrupted or destroyed would have a serious impact on the health, security, or economic wellbeing of citizens and the efficient functioning of a country's government.¹ One does not have to look far for examples of disruptions that have cost organizations time, resources, and possibly lives. Added to this is the fact that many SCADA systems are vulnerable. It is therefore imperative that system security and risk mitigation be at the forefront of the minds of all SCADA system users.

The Growing Vulnerability of Control Systems

Historically, security concerns over



control systems were limited to physical attacks. SCADA system operators rationalized that if the management consoles were adequately isolated and only authorized personnel had access to the network, the system was intrinsically secure. There was little risk of tampering since few people had technical expertise of the system and the data communication paths remained isolated.

SCADA has been hidden behind its cloak of obscurity for the past four decades, with information technology managers convinced that these systems would never be accessed through corporate networks or from remote access points. The modern SCADA system has evolved

significantly. Utility companies recognize the lower costs, easier accessibility, and improved efficiency gained through connecting their TCP/IP networks to their SCADA systems. These next generation systems, integrated with corporate networks and the Internet, face many challenges in their quest to becoming secure.

Several factors have contributed to the growing vulnerability of control systems, including:

1. The networking of control systems—Enterprises have increased connectivity through the integration of their control systems and enterprise networks. Breaches in enterprise security can arise if appropriate security controls are not put in place for both networks.
2. Insecure remote connections—Access links such as dial-up modems and wireless communications are used for remote diagnostics, maintenance, and examination of system status. If encryption or authentication mechanisms are not utilized, the integrity of the transmitted

Continued on page 4

¹ Myriam Dunn, "Critical Infrastructures: Vulnerabilities, Threats, Responses", *CSS Analyses in Security Policy*, Vol. 2, No. 16, June 2007. Typically, each country has their own definition of Critical Infrastructure. For more information on the 17 U.S. sectors visit http://www.dhs.gov/files/programs/gc_1189168948944.shtm.

Powermetrics Introduces a UPS / Power Supply for SCADA-RTU Applications

Powermetrics Inc (Cleveland, Ohio) introduces the PM-UPS-12-24-15. This UPS / Power supply operates from 85-264 VAC or a 12 volt battery, and provides a regulated 24VDC output and a regulated adjustable 12VDC-15VDC output. In addition, the unit incorporates a temperature compensated two mode battery charger for charging the 12 volt battery.

The unit is designed for powering a PLC and radio in RTU applications. The built in Modbus/RTU interface allows a remote host to enable and disable the individual output voltages; and to adjust the 12V-15VDC output to optimize radio operation. In addition, a number of other parameters may be monitored and adjusted remotely.

A watchdog timer can be programmed, either through the service port or over the MODBUS interface, which can be used

to reset the system if communications is lost for a programmed period of time. The PLC can also send a Modbus instruction to the UPS to disable the internal AC/DC power supply which forces the UPS to battery backup mode for testing purposes.

Although the power section of PM-UPS will operate as a stand-alone UPS, it is intended to operate along with a microprocessor subsystem which provides a variety of control and monitoring functions. For applications not requiring remote monitoring and control, the unit can be purchased without the microprocessor board.

The microprocessor subsystem communicates with an external PLC using MODBUS protocol over an RS485 interface. In addition a USB service port is provided to allow configuration of the system's programmable parameters.

Most of these parameters can also be set or changed using MODBUS commands through the RS485 interface.

The UPS may be interrogated by the remote host to report nine analog and seven digital inputs. Analog inputs include output voltages and currents, battery voltage, battery charge and discharge current, remote battery temperature, and AC voltage. Digital outputs include AC voltage present, battery charger status, DC outputs in range, and whether the unit is AC powered or battery powered.

For further information contact Sage Designs.



Inside This Issue

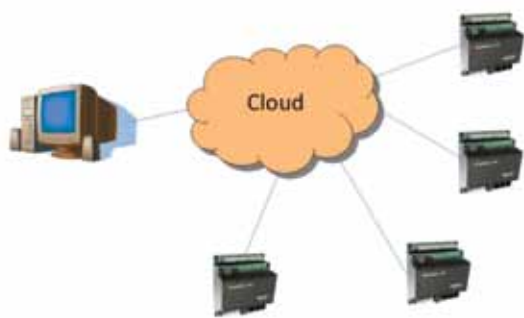
- SCADA Security: Challenges & Solutions
- SCADA Basics (Part 2)
- SCADA System at SSWD
- Firetide Wireless Bridges
- Wireless Product of the Year
- Training Classes

SCADA Basics Part 2

Part 2 of a continuing series of articles about SCADA issues where we discuss one of the many communications options that may be a part of a SCADA system. These articles deal with widely distributed SCADA systems rather than in-plant systems where communications issues differ widely from those discussed here.

the emergence of digital leased-line communication products available from the phone company, has greatly improved the reliability of the wired system while in the past, the only options other than installing your own direct wire were dial-up and leased lines.

Dial-up and leased line systems use the same phone lines but differ in that leased lines are continually off-hook



Bell-202 Network

Communications Options

As anyone in the remote SCADA industry can tell you, communications to your remotes is the most challenging issue facing the end user or systems integrator. In the best of circumstances, any of the available choices can work well, providing a reliable link to field assets for proper monitoring and control of your processes. In the worst cases, they can be a constant source of frustration for technicians and operators alike as they are central to the success of a SCADA system and often the most difficult part to troubleshoot and keep in operation.

Wired Communications

Wired communications may sound like the best choice, but often, this is not the case. There are several options for a wired system which include dial-up modems, leased line modems, digital phone lines, fiber optic cable and direct wire. Of these, owner-installed direct wire or fiber are the only types that probably have no monthly fees. In recent years,

and are often bridged in a point to multipoint topography. The modems for leased lines are considerably different from dial-up modems, as the Bell-202 standard is limited to 1200 baud while dial-up can operate at 28,800 (28.8 Kbps) to 57,600 (57.6 Kbps) and even faster sometimes. The advantages of the leased line option over the dial-up are: (1) no dial delay, (2) easier to configure modems, and (3) are somewhat more secure. The biggest problem with the leased line option is that phone company technicians are notorious for disconnecting them and leaving you without communications with your remote for days or even weeks at a time.

While advanced digital phone lines don't often get accidentally disconnected by phone technicians, entire systems have been known to come down because one lead on one remote goes to ground. They offer high data rates and good reliability; however, their cost can be prohibitive. Also keep in mind that all of these systems are susceptible to fires, bad drivers or infrastructure problems not of your making.

In summary, wired systems usually carry a monthly charge, may be expensive to obtain or install and can be unreliable, but may be a necessary part of your system.



Security Products Magazine Names Firetide Mobility Infrastructure Family 2011 New Wireless Product of the Year

Firetide's Mobility Infrastructure has been selected as the winner of Security Products magazine's '2011 New Product of the Year Award' in the wireless technology category.

Firetide's Mobility Infrastructure, which includes the HotPort 7000 and FMC-2000, delivers reliable, uninterrupted Internet connectivity from virtually any moving vehicle including first responders, trains, buses, and more, enabling a range of exciting new applications that were not possible before. Essentially any standard Ethernet or Wi-Fi-enabled device such as iPhones, laptop computers, even video security cameras, can maintain continuous network connectivity, even while travelling at high speeds.

"The New Product of the Year contest gets better every year with a wider array of products and incredible technologic advances," said Ralph C. Jensen, editor-in-chief at Security Products magazine. *"This year, participation focused on more product verticals that captured every segment of the security industry. We appreciate the entrants and their willingness to share the newest innovations of security products with us and our readers."*

"Winning the Security Products New Wireless Product of the Year is a welcomed reward that highlights Firetide's dedication in developing the very best in wireless broadband products," said Bo Larsson, CEO of Firetide. *"We have worked tirelessly to create highly reliable and*


secure solutions that have a great deal of flexibility in deployment and are cost effectively utilized for a wide range of applications, from security to municipal services to public access. It's an honor to be recognized by an industry leading security publication."

The Security Products New Product of the Year Award honors the outstanding product development achievements of security equipment manufacturers whose products are considered to be particularly noteworthy in their ability to improve security. To view all of this year's winners, you can visit the Security Products' presentation.

About Firetide Inc.

Firetide is the leading provider of wireless infrastructure mesh networks that enable concurrent video, voice and data for government, transportation and commercial applications. Firetide provides reliable high-performance wireless infrastructure mesh and access solutions for video surveillance, Internet access, public safety networks and temporary networks wherever rapid deployment, mobility and ease-of-installation are required. Headquartered in Los Gatos, Calif. with offices in Asia Pacific, Firetide is a privately held company with worldwide product distribution. www.firetide.com



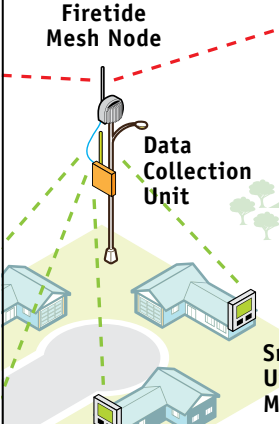


Firetide HotPort® 7000 Series Wireless Mesh Nodes


- Reliable, High-Performance Networks in Challenging Wireless Environments
- Street-Level Connectivity
- Encryption for End-to-End Security

Security Products Magazine 2011 New Product of the Year


Firetide Mesh Node



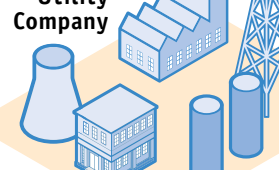
Firetide Backhaul Wireless Mesh



Smart Utility Meter



Utility Company



SCADAwise™ Training Classes

ClearSCADA

SCADAPack

ClearSCADA Training Course

June 4-7, 2012 - Mill Valley, CA
October 22-25, 2012 - Mill Valley, CA (TBA)

- Day 1 (8AM - 4PM) Installing ClearSCADA, Introduction to ClearSCADA, Components, Using ViewX, Using WebX, ClearSCADA Help
- Day 2 (8AM - 4PM) Configuring using ViewX, Database Organization, Basic Telemetry Configuration, Creating Mimics, Creating Trends
- Day 3 (8AM - 4PM) Configuring using ViewX, Templates & Instances, Logic Languages, Security, Communications Diagnostics
- Day 4 (8AM - 4PM) Reports, System Configuration, System Architecture, Questions

Cost: ClearSCADA Training Course \$1,890

(28 Contact Hours)

SCADAPack Telepace Studio Training Course

May 1-3, 2012 - Mill Valley, CA
October 16-18, 2012 - Mill Valley, CA

An optional SCADAPack 350, SCADAPack 334 or SCADAPack 32 is available at a special price with the course—an excellent way to get started using SCADAPack controllers.*

- Day 1 (8AM - 4PM) SCADAPack controller operation, Series 5000 I/O, Telepace Studio introduction
- Day 2 (8AM - 4PM) Telepace Studio advanced programming techniques and advanced functions
- Day 3 (8AM - 2PM) Controller communications, Modbus Master/Slave protocol, Diagnostics, Modems

Cost: SCADAPack Telepace Studio Course \$1,340

- * Optional SCADAPack 350 Training Kit – adds \$1040
- * Optional SCADAPack 334 Training Kit – adds \$1040
- * Optional SCADAPack 32 Training Kit – adds \$1,100

(20 Contact Hours)



Schedule Your Own

ClearSCADA Test Drive



Free Hands-On Test Drive

Call to Schedule a Test Drive

Call 1-888-ASK-SAGE

email: info@sagedesignsinc.com

Instructors: ClearSCADA & SCADAPack Telepace classes will be taught by Tony Sannella, Sage Designs, a Factory-Certified Instructor. The ClearSCADA Test drives will be conducted by Sage Designs or a factory representative.

Location: See individual course registration form. Those requiring overnight accommodations should call the hotel directly for reservations.

What should I bring? Laptop computer with minimum requirements as shown on the specific course registration forms, plus necessary permissions to install software on your computer.

What is provided? Lunch and coffee, soft drinks and snacks each day.

***Optional Training Kits at special course pricing (Telepace class only): Limit one (1) for every two (2) students per organization.** Training Kits will be shipped N/C to training facility, provided your registration is received approximately 4 weeks before the first day of the course, or shipped to you after the course when available. Training kits include a SCADAPack 350, SCADAPack 334 or SCADAPack 32 Controller, Telepace Studio Software, Hardware Manual (on CD-ROM), I/O Simulator board, AC/2 Transformer, & programming cable. Prices do not include applicable California sales taxes.

Download the Registration form at: <http://www.sagedesignsinc.com/events/index.htm>

Please send me the Registration Form

ClearSCADA: June 4-7, 2012 – Mill Valley, CA

October 22-25 2012 – Mill Valley, CA

SCADAPack Telepace: May 1-3, 2012 – Mill Valley, CA

October 16-18, 2012 – Mill Valley, CA

Name (please print):	Title:
Company:	Phone:
Address:	Fax:
	Email:
City/State/Zip:	

*** * * Registration Deadline: 2 weeks before 1st day of course * * ***

All registrations are subject to cancellation fees. A confirmation notice will be sent to all registrants on or before the deadline date.

Firetide Point-To-Point Bridges - Make Any Network Device Wireless

Firetide FWB-205 outdoor wireless Ethernet bridges provide low-cost, high-capacity connectivity between two locations. FWB-205 utilizes the MIMO technology to provide increased throughput and performance for a backhaul link. FWB-205 is software-configurable to operate in 5 and 4.9 GHz and can deliver up to 150 Mbps of UDP throughput.

Complete Infrastructure Solution

FWB-205 product line is a natural expansion of Firetide's core wireless infrastructure technology. Firetide's expertise in large-scale wireless mesh networks for video, data and voice applications in harsh environments ensures that its bridges are optimized to provide the highest performance, security and reliability in the industry.

Concurrent Voice, Video, Data

FWB-205 bridge is optimized to provide high-capacity and low-latency connectivity for demanding data, voice and video applications. Point-to-point connectivity is critical for municipalities, public safety, industrial installations and campus environments. In addition to these markets, this product serves the needs of wireless Internet service providers and telecom operators

FWB-205 provides true bridging functionality and is agnostic to the types of client or protocols on the network. FWB-205 supports transparent overlay of multiple subnet (VLANs) over the point-to-point link. It also provides seamless transport of multicast and broadcast traffic over the point-to-point link, including IPTV distribution, video on demand, video surveillance and video conferencing. In addition, to prevent bandwidth abuse, FWB-205 provides advanced tools such as multicast rate limits.



FWB-205

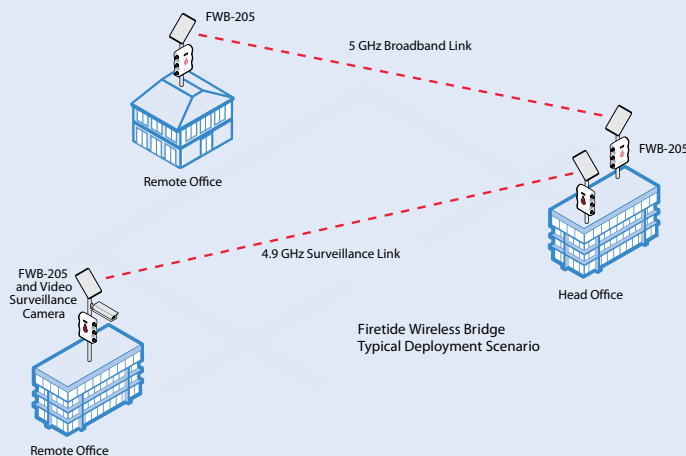
Privacy and Security

FWB-205 supports the industry's highest level of security to ensure privacy for communications and reduce liability for service providers. Like all components of the Firetide wireless mesh and access infrastructure, FWB-205 offers WPA2-PSK (Wi-Fi Protected Access) encryption for an unmatched, solid, and trusted network.

Flexibility of Deployment

Deployed as a standalone solution, the FWB-205 link is managed via a browser-based management interface. Customers can also integrate the FWB-205 links into a larger Firetide mesh network managed by HotView Pro™ network management software. Designed for an easy "out-of-the-box" installation experience, the unit pair is shipped preconfigured and with all accessories included. The FWB-205 is bundled with two external 3-in-1 MIMO antennas for 4.9 and 5 GHz. An integrated antenna alignment tool provides step-by-step guidance in achieving maximum signal

Continued on page 7



SCADA Security: Challenges and Solutions

Continued from page 1

- information is vulnerable.
- Standardized technologies— Organizations are transitioning to standardized technologies, such as Microsoft's Windows, in order to reduce costs and improve system scalability and performance. The result is more people armed with the knowledge and tools able to attack a system, and an increase in the number of systems vulnerable to an attack.
- Availability of technical information— Public information about infrastructures and control systems is readily available to potential hackers and intruders. Design and maintenance documents and technical standards for a critical system can all be found on the internet, greatly jeopardizing overall security.²

With so much riding on SCADA systems, it should come as no surprise that shortly after September 11, 2001, government officials found evidence of terrorist groups visiting websites that offer software and programming instructions for the digital equipment that run power, water, transport and communications grids. Furthermore, it has since been proven that the inner controls of critical infrastructure systems have been the target of cyber attacks. For example, in 2006 a water filtration plant near Harrisburg, Pennsylvania had its security system hacked. Malicious software that had the capability of disrupting the water treatment operations was planted from an outside source into the computer system.³

Most recently to shake the cyber security world was the "Stuxnet" malware, discovered in June 2010.

On Nov 29, 2010, Iran's president Mahmoud Ahmadinejad publicly disclosed that the Stuxnet cyber-threat had affected his country's uranium enrichment efforts. It is believed that the code was designed to sabotage nuclear plants, specifically targeting an individual company's configuration software and control devices. This intelligent worm was primarily spread via USB sticks but was found to also infect systems through network shares and SQL databases. According to Symantec, the worm would search for specific models of frequency converter drives made by two firms. Once the worm found the right configuration, it sabotaged operations by introducing subtle changes to the speed of the frequency drives over several weeks,

while displaying normal readings to maintain its stealth.

The Stuxnet malware began infecting systems in January 2009 and reports indicate that more than 100,000 computer systems have been infected worldwide. Historic data from the early days of the attack showed that 58.85% of infections occurred in Iran, 18.22% occurred in Indonesia, and 8.31% occurred in India.⁴ Although no serious damage was caused to any utility sectors, this sophisticated malware highlights the risks modern SCADA systems face with respect to connectivity, insecure remote connections, standardized technologies, and readily available technical information. Cyber security is a topic for utility experts and manufacturers that can no longer be ignored.⁵

Proactive Cyber Security is Smart Business

Ensuring cyber security in control systems may at first seem like a daunting task, as it requires a commitment from the entire organization. Upper management needs to recognize the numerous benefits of a secure SCADA system. These advantages include ensuring system uptime, reliability and availability. Implementing good cyber security is smart business because a secure system is a trusted system, and customer retention and loyalty is built around trust. Vendors, system integrators, IT and control engineers all share in the responsibility.

There are many resources available now to help critical infrastructure SCADA systems enhance their security. For example, the standard ISA99 – Industrial Automation and Control Systems Security, establishes best practices, technical reports, and related information to define procedures for implementing and assessing electronically secure systems. Compliance with this standard can improve manufacturing and control system electronic security, help identify and address vulnerabilities, and reduce the risk of compromised confidential information and system degradation.⁶

Government regulations also exist and continue to evolve with the goal of securing critical infrastructure industries. The most ambitious for influencing government policy is the non-profit North American Electric Reliability Corporation (NERC) – Critical Infrastructure Protection (CIP) standard. Known as NERC-CIP, this standard has its roots in the Electricity Modernization Act which

Continued on page 6

² United States General Accounting Office, "Critical Infrastructure Protection, Challenges and Efforts to Secure Control Systems", GAO-04-354, March 2004.

³ Philip Leggiere, "Infrastructure Security, Securing SCADA", HSToday, www.hstoday.us, September 2008.

⁴ Jarrad Shearer, "W32.Stuxnet", Symantec, www.symantec.com, September 17, 2010.

Telemetry Solutions for Water & Wastewater

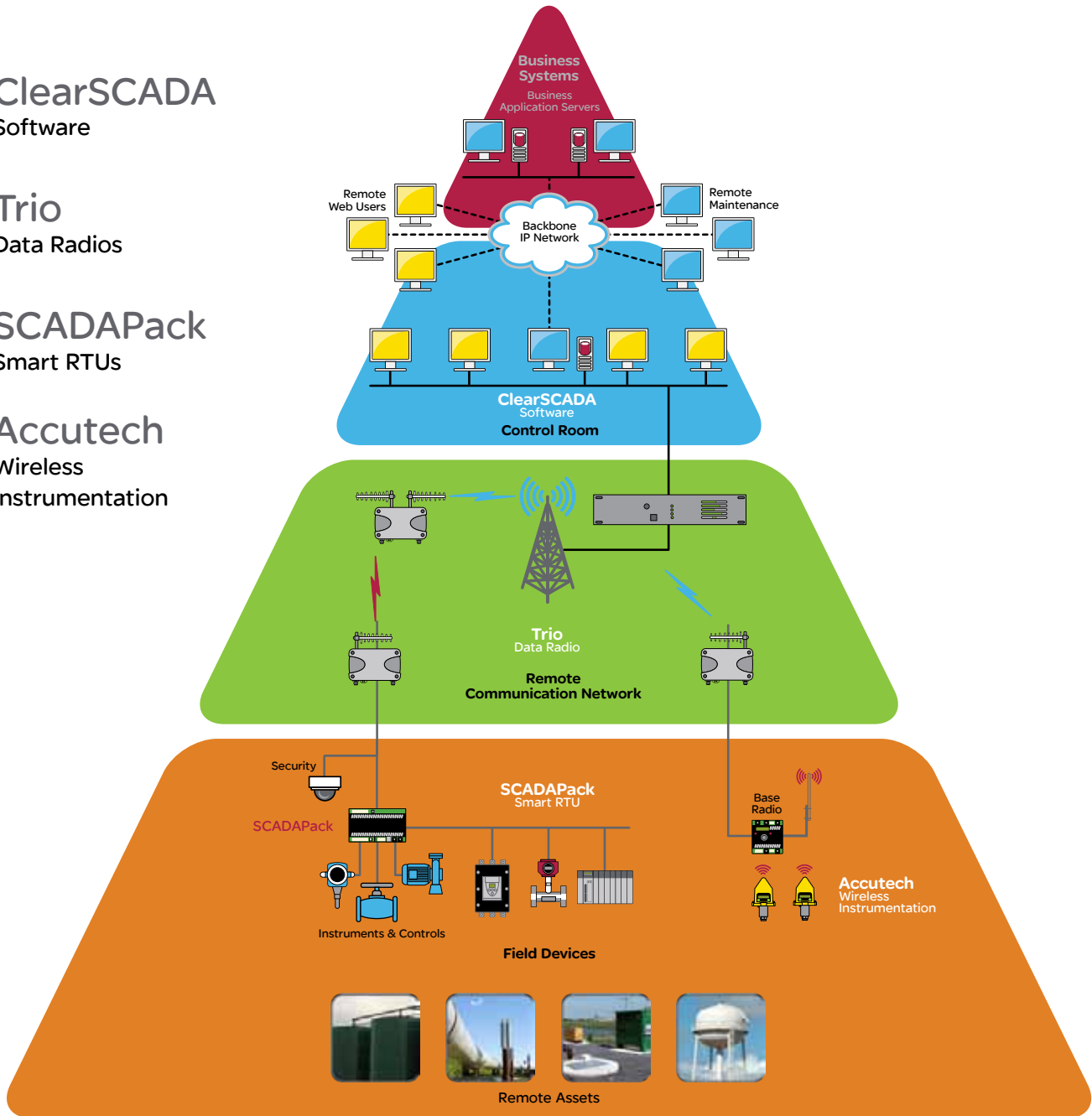
A complete integrated sensor to enterprise solution that will go beyond addressing the most challenging remote monitoring and control application and help you efficiently manage and operate a secure and reliable water infrastructure.

> **ClearSCADA**
Software

> **Trio**
Data Radios

> **SCADAPack**
Smart RTUs

> **Accutech**
Wireless
Instrumentation



www.controlmicrosystems.com

Telemetry & Remote SCADA Solutions



is part of the US Energy Policy Act of 2005. Within the Energy Policy Act of 2005, there is a section, which dictates that the NERC-CIP standard requires all power plants and electric utility facilities to develop new cyber security systems and procedures in accordance with a 3-year implementation plan. There are eight different CIP standards covering everything from Security Management Control and Critical Cyber Assets, to Incident Reporting and Recovery Plans. Each one of the eight standards defines a series of specific requirements. The standards are:

- CIP-002-1: Critical Cyber Asset Identification
- CIP-003-1: Security Management Controls
- CIP-004-1: Personnel and Training
- CIP-005-1: Electronic Security Perimeter
- CIP-006-1: Physical Security of Critical Cyber Assets
- CIP-007-1: Systems Security Management
- CIP-008-1: Incident Reporting and Response Planning
- CIP-009-1: Recovery Plans for Critical Cyber Assets

Now that we're seeing congressional action and government penalties for non-compliance, SCADA cyber security is being taken more seriously.⁷

Encryption and Authentication

In order to meet CIP-005-1 and CIP-007-1 standards, encryption and authentication are critical elements in a comprehensive cyber security solution. Typical SCADA security measures consist of physically securing the hardware and transmission media, and employing common cyber security defenses such as password protection and anti-virus utilities. Communication security measures are harder to enforce since modern day hackers can easily identify confidential phone numbers, decode proprietary protocols, and bypass firewalls and gateways. Encryption and authentication are highly effective methods to reduce some of these cyber threats to SCADA communications.

There are two open standards for SCADA communications available on the market today that were developed to provide security through encryption and authentication:

- IEEE6189 suite—Also known as AGA 12 incorporated in IEEE 1711, these standards secure SCADA equipment communication.

- IEC62351 suite—Secure Authentication for DNP3 communication is based on this standard.

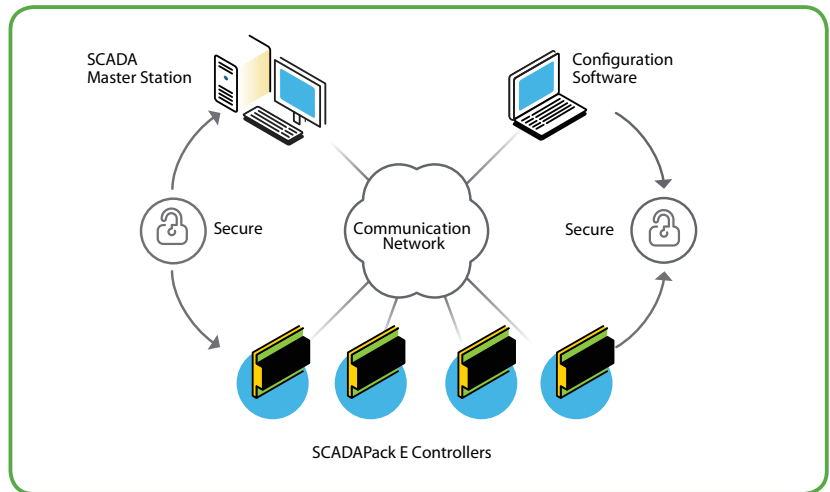
Encryption is the act of manipulating information until it appears almost meaningless to the casual observer. Decryption is the process that takes place to restore an encrypted message back to its previous readable state.

In a typical SCADA system, messages are sent using a given protocol format, such as MODBUS or DNP3. Anyone who can see the messages being transmitted can decode them and see what information is being transferred from device to device. On an encrypted SCADA communication system, messages are transformed into a seemingly garbled sequence of bytes. Short messages are stuffed with extra random data to make it difficult to estimate the size or type of the messages being transmitted. A casual observer can determine little more than the fact that a message has been sent from one device to another. Encryption makes spying on and tampering with SCADA networks much more difficult.

Like many forms of physical or electronic security, encryption uses a key. This type of key is a secret sequence of data that determines how the information being sent between devices is obscured (encrypted). Keeping this key secure is a fundamental part of SCADA security. It is therefore important to reiterate that employing a diverse range of security measures will always prove more effective. The other layers of security, like physical locks, operating procedures, and separately secured corporate and SCADA networks are necessary to protect encryption keys, and the system as a whole.

Authentication is the process by which one part of a SCADA system proves its identity to another. A SCADA device receiving a critical message, such as a command to perform controls or respond with data, can challenge the sending device's identity. The sending device must then provide the challenge response. If the receiving device is satisfied with the challenge response then it will act on the original command.

Like encryption, authentication requires the communicating SCADA devices to have a mutually know secret key. Whereas encryption uses its key to

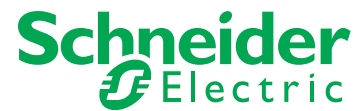


transform entire messages into an encrypted data stream, authentication challenges and challenge responses use their keys to create special digital signatures. The mathematics used in authentication is similar to that of encryption, but a smaller amount of data needs to be manipulated. This means that authentication is computationally far cheaper than encryption and typically uses the structure of the original SCADA protocol for better communication efficiency. Authentication prevents malicious parties from controlling a secured SCADA device, but it will not stop them from intercepting messages and reading their content.

Achieving Your Secure SCADA with Schneider Electric

As described above, government is mandating the deployment of security technology for SCADA systems in some utility sectors, while for the moment leaving others free to choose whether they deploy security or not. With the growing vulnerabilities of control systems and the potential for harm and civil disruption in a breached critical infrastructure system, SCADA users are advised to formulate and deploy a security plan that meets their individual and immediate needs. Even within a security mandate there is scope for choice about how to implement the security system: authentication or encryption, or both.

Schneider Electric's SCADAPack E controllers provide both IEEE6189 message encryption and DNP3 secure authentication. The E controllers now provide DNP3 communications to the latest DNP3-2009 standard as well. A new user-friendly security administrator is available for managing DNP3 secure authentication and AGA12 encryption



Telemetry & Remote SCADA Solutions

security and is multigroup aware so it can be used to manage security configurations for multiple controllers in a system.

The SCADAPack E Configurator software further enhances system security as it cooperates with the E controllers to authorize configuration software installation, authorize users, and prevent system manipulation. This technology addresses the vulnerable security gap that commonly exists between control devices and their management software.

This powerful line of programmable logic controllers with remote terminal unit functionality is designed specifically for telemetry and remote SCADA water and wastewater applications. With improving overall system visibility and security at its core, E controllers maintain no holes in data even when communication links go down and allow end users peace of mind in their system data's integrity for billable applications or critical operations.

In 2011, we will see utilities take a more proactive approach to protecting their SCADA infrastructure with the adoption of encryption and authentication technologies to meet compliance standards and avoid the monetary fines and reputational damage that a security breach can cause.

— by Metin Ozturk & Phil Aubin, Schneider Electric, Telemetry & Remote SCADA Solutions

⁵For control system security program information and incident reporting, visit Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) at www.ics-cert.org.

⁶The International Society of Automation, "ISA99, Industrial Automation and Control System Security", <http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821>.

⁷Philip Leggiere, "Infrastructure Security, Securing SCADA", *HSToday*, www.hstoday.us, September 2008.

Robust SCADA System at Sweetwater Springs Water District

In 2005, Sweetwater Spring Water District in Guerneville, CA installed a new SCADA system for water distribution. This is a tough application for radios, with hills, mountains, and dense redwood forests proving challenging for the radio system. The completed system has over time proven to be robust and reliable, requiring less maintenance and higher reliability than might have been anticipated. A good design, coupled with careful system integration, has helped achieve this high reliability.

The SCADA system provides for control and monitoring of 10 remote sites. Tank level data is sent to pump sites, and pump sites react to the tank level data by operation of the pumps to keep the tanks full. The SCADA system provides monitoring at the central office of equipment status, process data, alarm data, and data collection.

The SCADA system consists of 11 SCADAPack programmable logic controllers (PLC), monitoring approximately 13 remote sites. Teledesign Systems TS4000 radios at each PLC site provide licensed frequency communications at 467 MHz. This frequency is able to cut through the thick redwood forests that surround many sites. A SCADAPackVision10 operator interface provided locally at each PLC site provides local control and monitoring. Some PLC sites communicate via Bell 202 modem and buried cable to other nearby sites. The Front End Processor PLC and the SCADA computer are located at the central office. The SCADA computer is full-featured, and provides for monitoring and control, alarming, alarm dial-out, and remote access. The PLC's, radios, and operator interfaces were all provided though Sage Designs.

Control of the SCADA system is distributed throughout the SCADA system. This means that tank level control at a pumping site does not require the master site (District Office site) to be functional for the level control to be operational. The tank level control does not require even that a radio repeater be functional. This distribution of control provides for robustness by avoiding single points of failure. Radio communications control is distributed

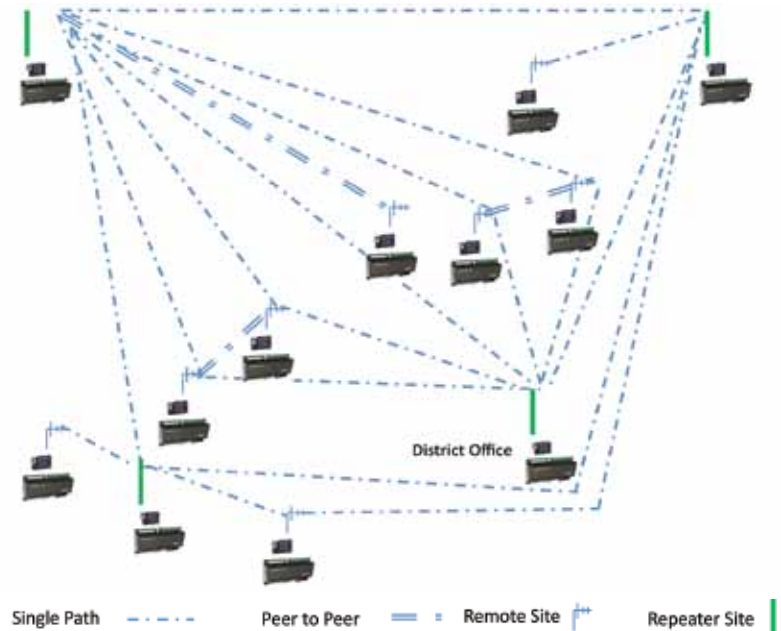
also. There is not one master radio site that provides for radio communications throughout the radio system. There is no single point of failure in the radio system. The details of this feature are in the following paragraphs.

The radio system consists of remote sites, repeater sites, combination remote and repeat sites, and one master site.

The pump sites generally have directional antennas pointing to their associated tank site. The tank sites have antenna (omni-directional or directional) that allow communications both with their associated pump site, as well as a relay site and/or the master site (central office site). There is also a main repeater site on Mount Jackson that is used by much of the radio system.

Quiescent telemetry was deployed on this project as specified. Quiescent telemetry is a method of SCADA communications in which the remote sites are not polled by a master site. With quiescent telemetry, each remote site transmits data to the master site on an as-needed basis, sending alarms and change-of-state information on an as-needed basis, and also sending analog data periodically as needed when a specified change of analog signal is detected by the PLC. This is sometimes called *report-by-exception*. Quiescent telemetry is more difficult to deploy than the typical polling system, but does offer significant advantages. The disadvantage to quiescent telemetry is that the logic for communications is spread over the SCADA system, and transmissions can originate from almost any remote site, making startup and troubleshooting less straightforward and possibly increasing the amount of time that startup requires.

This disadvantage of quiescent telemetry is mitigated by one valuable feature: The remote diagnostic feature available with the Teledesign Systems TS4000 radios allows "pinging" of each remote and relay site from the master site, which provides information on the communications



routing, signal strengths, and success and failure of the pinging. The remote diagnostic feature also allows tracing of radio packets received at any radio. With this radio diagnostic tool, from one central location the user may obtain a valuable picture of the health and performance of the entire radio system.

There are also some significant advantages to the use of quiescent telemetry. Because data is transmitted only on an as-needed basis by the remote sites, the radio frequency remains quiet (hence the name "quiescent telemetry"). This quiet of the radio system leaves room for multiple radio conversations over a single communications channel. The SCADA system design called for backup peer-to-peer radio communications. In other words, normally the remote tank site level signal is transmitted to the central , and the central site re-transmits this signal data to the remote sites (primarily pumping sites) that need this data for control of the process. The peer-to-peer mode works as follows: If a pump site has not received level data from the central office site in a specified period of time, the pump site's radio will transmit a

request for level signal data directly from it's associated tank site. If the District Office site (master site) fails, and the main repeater site fails at Mount Jackson, the pairs of tank and pump sites will then communicate with each other by peer-to-peer communications, providing for tank level control in a distributed fashion.

Reliability of the SCADA system is further enhanced by use of multiple repeaters. Some remote sites double as repeater sites. Many remote sites can communicate with the alternate repeater sites, so that in case of failure of the main repeater site at Mount Jackson, the alternate repeater sites seamlessly provide for an alternate communications route.

— By Douglas H Wirth, Sky Valley Engineering Services. Sky Valley Engineering Services has provided startup services and ongoing support to Sweetwater since 2006. Sky Valley specializes in SCADA system installation, upgrades, and maintenance for water districts and other industries in Central California since 2006. Sky Valley Engineering Services may be reached at dwirth.sves@sbcglobal.net.

Firetide Point-To-Point Bridges - Make Any Network Device Wireless Continued from page 4

quality, translating to better network performance and throughput.

Enhanced Radio Management

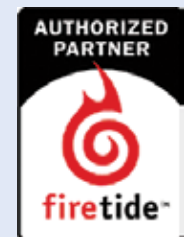
The FWB-205 enhances the Radio Management capabilities of the bridge by providing a second radio which will be dedicated for RF Monitoring purposes. This enables features such as spectrum analysis, channel load analysis, interference detection and mitigation.

Also since the radio is dedicated, this enables faster response to neighborhood RF changes.

Features Include:

- Wireless Video Transmission
- 150 Mbps of UDP throughput
- IEEE 802.11 a/b/g/n
- High power radio: 3X3 MIMO dual stream, 400 mW

- Supports the industry's highest level of security WPA2-PSK
- Unit powered via Power-over-Ethernet (PoE)
- Intuitive web-based interface
- Adjustable frequency ranges minimizing interference
- Easy installation



For more information, contact your Firetide Partner, Sage Designs.

SAGE DESIGNS, INC.

SCADA & Security Products

150 Shoreline Hwy., Suite #8A
Mill Valley, CA 94941-3634

STANDARD MAIL
US POSTAGE PAID
PERMIT 191
SANTA ROSA CA

 **SAVE A TREE**
Return Service Requested

The Sage Advisor

SCADA, SECURITY & AUTOMATION NEWSLETTER

Calendar of Events

March 5-8, 2012	ClearSCADA Training Course* , Indio, CA
April 4, 2012	CA-NV AWWA 2012 Spring Conference , Santa Clara, CA
April 18, 2012	CWEA AC 2012 Annual Conference , Sacramento, CA
May 1-3, 2012	SCADAPack - Telepace Studio Ladder Logic Training Course* , Mill Valley, CA. 
June 4-7, 2012	ClearSCADA Training Course* , Mill Valley, CA. 
June 10-14, 2012	AWWA ACE '12 Expo , Dallas, TX. Visit our manufacturers' exhibits.
June 20, 2012	Wine Country Water Works Trade Show & Symposium , Healdsburg, CA
September 12-14, 2012	CWEA Northern Regional Training , Redding, CA
September 25-27, 2012	Tri-State Seminar on the River , Primm, NV
Sept. 29 - Oct 3, 2012	WEFTEC.12 , New Orleans, LA. Visit our manufacturers' exhibits.
October 8-11, 2012	CA-NV AWWA 2012 Fall Conference , San Diego, CA
October 16-18, 2012	SCADAPack - Telepace Studio Ladder Logic Training Course* , Mill Valley, CA. 
October 22-25, 2012	ClearSCADA Training Course* , Mill Valley, CA. 
November 5-7, 2012	CASQA Annual Stormwater Conference , San Diego, CA

* Download the registration form from our website or call for more information.

SAGE DESIGNS, INC.

SCADA & Security Products

Schneider Electric
Telemetry & Remote SCADA Solutions



SCADA
ClearSCADA Enterprise Software
SCADAPack RTU/PLC Controllers
FlowStation Pump Controllers
WIN-911 Alarm Notification Software

WIN-911

firetide

TELEDESIGN

FREEWAVE

AXIS

VICON

PureTech SYSTEMS

MS4

MS4

WIRELESS
TRIO Spread Spectrum & Licensed Radios
Firetide Broad-Band Mesh Network
Teledesign Systems VHF & UHF Licensed
FreeWave Spread Spectrum Serial & Ethernet

SECURITY
Analog & IP Cameras, Video Surveillance
Hardware & Software
PureActiv Video Analytics
& Camera Management

MS4 PERMITTING SOFTWARE

CBI Systems, Ltd MS4 Permit Manager™
& MS4web™ software

1-888-ASK-SAGE • 1-888-FAX-SAGE
www.SageDesignsInc.com

Acknowledgements: SCADAPack™, FlowStation™, and ClearSCADA™ are trademarks of Control Microsystems Inc., (Schneider Electric Telemetry & Remote SCADA Solutions brand). Win-911® is a registered trademark of Specter Instruments. HotPort™, HotClient™, and HotView™ are trademarks of Firetide, Inc.. Firetide® is a registered trademark of Firetide, Inc.