The Sage Advisor

SCADA, SECURITY & AUTOMATION NEWSLETTER

Volume 20, Issue 2 • Fall/Winter 2010

A Publication of Sage Designs, Inc.

Control Microsystems is becoming Schneider Electric

Control Microsystems has recently been acquired by Schneider Electric, the global specialist in energy management. Under their Automation Portfolio, Schneider Electric serves machine builders, mining, mineral and metals, water/wastewater, oil and gas, and electrical energy markets. Control Microsystems' product portfolio complements and expands Schneider Electric's current application fields. Michel Crochon, Executive Vice-President of Schneider Electric's Industry business, commented in a press release dated April 13th, 2010: *"Schneider Electric acquires a global telemetry platform to address the needs of the attractive water, wastewater, and oil and gas industries for which remote monitoring and control are critical to their large and dispersed sites. The combination of technologies, channels, customer knowledge and complementary execution capabilities will put us in an excellent position to capture new opportunities in these fast growing markets."* Customers can expect a commitment to their core business with integrated solutions designed to provide safe, reliable and efficient energy.

Control Microsystems will become the global experts in remote SCADA and telemetry solutions for water/wastewater and oil and gas. As the transition to Schneider Electric occurs, the four leading product lines (Accutech, SCADAPack, Trio, and ClearSCADA) will continue to be sold through the established sales channels. Schneider Electric recognizes that existing Control Microsystems' representatives are highly skilled, specialized organizations that focus on providing best-in-class solutions to solve customer challenges.

Continued on page 6

Free November SCADA Seminars

SCADAWise

As the need for data increases in the modern world of SCADA, it seems natural that protocols for today's systems must advance to accommodate this thirst. Addionally, utilities managers want to be able to better manage their equipment in the field without ever leaving their office in order to save time and labor. Thankfully, the current trend towards DNP3 makes both of these goals achievable. Not only does DNP3 turn your remotes into data-loggers which don't miss an event just because it occurs between poll cycles, but the protocol allows for implementations which support the re-configuration of the remotes, version control of programs in them and diagnostics which watch the health of the controllers, their programs and their I/O.

If you are interested in these topics, you should attend one of our two upcoming free SCADA seminars. Presentations by experts at Control Microsystems explaining and demonstrating these capabilities which have been implemented in the E-series SCADAPacks and ClearSCADA SCADA host software will leave you with no doubt that the days of simple polled protocols such as Modbus and DF1 are soon to be behind us.

See the registration form in this newsletter or go on-line to www.scadawise.com to register.

SCADA Communication Security The "Onion" Perspective

As the profile of security for Supervisory Control and Data Acquisition networks has grown, experts have begun to talk more and more about this issue. It is a sign of the times that one of the first acts of President Obama was to instigate a comprehensive review of cyber security and he singled out SCADA systems as a key part of the review. Why? Because the increase in I.T. networking means that SCADA systems are being connected to the Internet, leaving them more open to attack.

Much literature has a focus on security technology in detail. This does not help those new to the technology. Nor does it help people to understand cyber security in the context of an overall security plan. For that, we need a reasonable model. This is where the "onion" comes in. As Shrek says *"Ogres are like onions. Onions have layers."* Well, security is like an onion, too. A good security plan involves many layers. One layer of security won't provide much of a deterrent, but add another 3 or 4 layers and you're starting to get somewhere. Different layers of security protect against different kinds of threats and will often complement one another.

There are many potential security layers, be they physical, electronic or procedural:

- Keeping SCADA networks isolated from corporate networks.
- Not advertising configurations (e.g. disable SSID on wireless networks).
- Installing field devices (e.g. RTU, PLC) inside locked enclosures.
- Creating audit logs that will reveal evidence of tampering.
- Encryption (hiding data as it moves across networks).
- Authentication (verifying that the person performing a critical operation is authorised).

It is encryption and authentication that will be the focus of this article. It's important to note that encryption and authentication are not mutually exclusive; they can both be used concurrently on the same system.

Encryption... and Decryption

Encryption is the act of manipulating information until it appears almost meaningless to the casual observer. Decryption is the act of restoring an encrypted message to its previous readable state.

In a typical SCADA system, all 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.

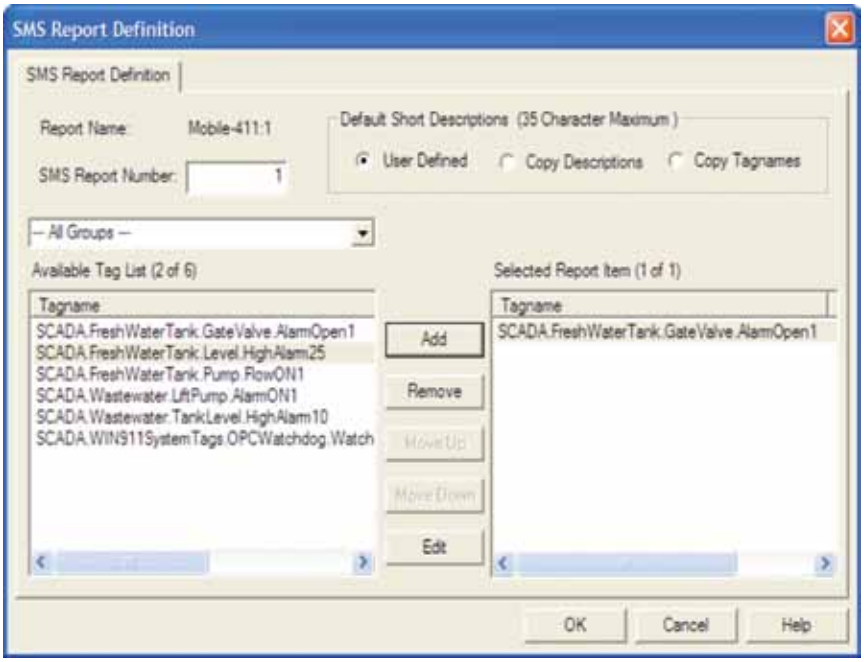
In an encrypted SCADA system, messages are transformed into a seemingly garbled sequence of bytes. Short messages are stuffed with extra random bytes to make it difficult to estimate the size of the messages being transmitted. A casual observer can

Continued on page 7

Inside This Issue

Get SMS Reports with Win-911

In addition to receiving alarms on any cell phone, users can now request text reports and get the current values of process variables using the 2-Way SMS capability available with all WIN-911/PRO systems. A user can request a report by texting Win-911 with a report number. These reports can contain several variables, each of which will come in as a separate message on your phone. Reports can be requested at any time, whether or not any alarms are active. Win-411 Reports is a valuable tool for field personnel and augments the powerful alarming capability of Win-411 2-way SMS. It supports all major wireless service providers and is included in the Win-911/PRO software package.



With Windows Smart Phones, you can run Mobile-411 which includes enhanced features such as a tabular layout for reports, plus a Refresh button for getting the latest values with a single stroke. Other features include the ability to receive and acknowledge individual alarms and get alarm status reports.

Configuring WIN-411 Text Reports is easy using the new 411 report module. Simply add data tags that have been imported into WIN-911 from your SCADA database, then add a short description for each.

Take WIN-911 SMS alarm notification to a whole new level using WIN-411 Text Reports and Mobile-911. Manage data and alarms more effectively and keep informed when it really counts.

Call Sage Designs for more information or visit the manufacturer's website: www.specterinstruments.com

SAGE DESIGNS, INC.
SCADA & Security Products

CONTROL MICROSYSTEMS

Control Microsystems is becoming Schneider Electric

Free SCADA Seminar

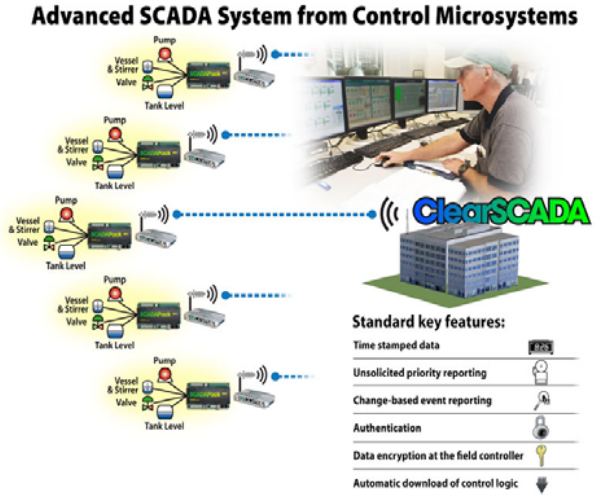
Integrated Water/Wastewater SCADA Solutions

November 3, 2010
8AM – Noon
Radisson Hotel Newport Beach
4545 MacArthur Blvd.
Newport Beach, CA 92660

November 4, 2010
8AM – Noon
Embassy Suites Walnut Creek
1345 Treat Blvd.
Walnut Creek, CA, 94597

Water utilities have been using Supervisory Control and Data Acquisition (SCADA) for many years, during which SCADA systems have evolved from simple tone telemetry to web-centric solutions. A SCADA system's primary function is to monitor and control the conditions of remote assets, such as pumps and lift stations, distribution networks, and treatment plants, while ensuring data integrity, overall system visibility, and security. If you are expanding, upgrading, or developing a new SCADA system, selecting the right hardware and software components can help you cope with ever changing demands in securing your infrastructure and improving data collection and reporting.

Join us to learn more about intelligent field controllers that can dramatically improve environmental compliance and reduce cost of deployment for water systems. Understand the benefits of event data logging and time-stamped data in the remote controller and how historical data backfill can help you meet regulatory requirements. Learn about secure and encrypted data transmission and innovative system architectures that can reduce your cost of operation.



Who should attend?

- SCADA Engineers, Managers and Technicians
- Water Systems Managers, Operators and Technicians
- SCADA Solution Providers

Featured Applications

- Pump/lift Station Controllers
- Water Quality Monitoring
- District Meter Zones
- Real-time and Historical Data Gathering
- Wireless Instrumentation & Measurement

Featured Products

- SCADAPack E-Series PLC/RTU
- ClearSCADA Integrated Enterprise Software
- Trio Long-range Industrial Wireless Radios

Featured Technologies

- Integrated Enterprise Software
- Historical Data Backfilling
- Wireless Ethernet Communications
- Data Encryption and SCADA Security

Continental breakfast included

Download the registration form at http:www.sagedesignsinc.com/events

Pre-registration Required

To Register: Email this form to info@sagedesignsinc.com **or fax to 1-888-329-7243.** A confirmation will be emailed to you. The registration form and hotel directions can be found on the Events Page of our website: http://www.sagedesignsinc.com/events. For more information, call 1-888-275-7243.

☐ **Register me for the free seminar in Newport Beach on Wednesday, November 3, 2010**

☐ **Register me for the free seminar in Walnut Creek on Thursday, November 4, 2010**

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

*** * * Registration Deadline: October 29, 2010 * * ***

There is no charge for this event, but we would appreciate notification if you must cancel your reservation.

SAGE DESIGNS, INC.
SCADA & Security Products

CONTROL MICROSYSTEMS

SCADAWise™ Training Classes

ClearSCADA

SCADAPack

ClearSCADA Training Course

December 13-16, 2010 - Corte Madera, CA
February 28 - March 3, 2011 - Mill Valley, CA

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 $1,800

SCADAPack TelePACE Studio Training Course

November 15-17, 2010 - Mill Valley, CA
February 15-17, 2011 - 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 Control Microsystems' 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 $1,275

* Optional SCADAPack 350 Training Kit – adds $990
* Optional SCADAPack 334 Training Kit – adds $990
* Optional SCADAPack 32 Training Kit – adds $1,060

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 Sannellla, Sage Designs, a Control Microsystems' Factory-Certified Instructor. The ClearSCADA Test Drives will be conducted by Ian Metcalfe, US ClearSCADA Sales, Control Microsystems.

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 of Win 2K or XP with 15mb free disk space, CD ROM, mouse with a scroll wheel, working serial, USB or Ethernet port, and 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

SAGE DESIGNS, INC.
SCADA & Security Products

ClearSCADA: ❑ **December 13-16, 2010 - Corte Madera, CA** ❑ **February 28 - March 3, 2011 - Mill Valley, CA**
SCADAPack TelePACE: ❑ **November 15-17, 2010 - Mill Valley, CA** ❑ **February 15-17, 2011 - 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.

150 Shoreline Hwy., Suite #8A • Mill Valley, CA 94941-3634 • 1-888-ASK-SAGE (1-888-275-7243) • 1-888-FAX-SAGE • www.SageDesignsInc.com

Integrator Spotlight: Sierra Control Systems

As the decade of the 60's came to a close, Sierra Control Systems, Inc. founder Allen Wilson recognized a need for accurate measurement of open channel water systems. In 1972, he incorporated Sierra Control Systems in Carson City, Nevada. Initially working from a garage with the help of family, the company developed highly accurate water level instruments, water control systems, and radio telemetry. Employing a soup-to-nuts approach, SCS engineered, designed the circuits and the circuit boards, and machined and fabricated much of the hardware in-house. They developed the programs and installed the finished product. SCS then followed through with support and training.

SCADA was a relatively new, emerging technology. One of the industries to make wide-use of the technology was hydroelectric power generation. Sierra Control Systems was contracted to engineer and provide equipment to monitor and control the critical processes involved at many of the hydro power plants in California. The expertise and reputation of the company grew along with the SCADA industry itself.

In addition to SCS's work with the power industry, municipal utilities and irrigation districts also wanted to monitor and control their facilities. To this end, the company developed tank top monitors with telemetry for water storage tanks, pump controllers, and gate controllers. These could report to a master telemetry unit in a central location. Again, the product was engineered and built down to the board level at the Sierra Control Systems facility. The company was quickly becoming known as a provider of reliable, quality equipment, much of which is still in service today.

As the 90's approached, open architecture in SCADA systems became an important consideration, as more vendors vied to provide products for the growing SCADA industry. It became essential that equipment from vendor "A" could integrate with equipment from vendor "B". Suddenly, everyone was speaking Modbus. Sierra Control Systems quickly embraced the changes. The new Control Microsystems' VS/3 RTU had been introduced. The convenient, single-board package began appearing in SCS controllers. The Control Microsystems' TeleSAFE 6000 RTU soon followed. SCS continued to develop products to expand the new controller's capabilities. These included multiplexers for enhanced I/O count and telemetry interfaces to existing SCS technology, among others. As the choice of OIT devices was limited at this time, Sierra Control Systems designed and built its own. These capabilities helped accelerate the company's entry into the System Integrator ranks, while setting the company apart.

Today, SCS remains at the forefront of modern SCADA system suppliers. Their Series 900 controller, which is based on a Control Microsystems' SCADAPack controller, has been deployed in hundreds of measurement and control applications throughout the West. The DNP3 protocol capabilities of these controllers can provide their customers with the latest in open architecture SCADA solutions, without the need to reengineer the products. Control Microsystems' ClearSCADA SCADA host software nicely ties these systems together, creating a system that can meet the needs of the most demanding of customers.

Sierra Control Systems works closely with engineers at the Irrigation Training and Research Center at California Polytechnic State University, San Luis Obispo. The ITRC has developed a vast knowledge of irrigation system practices and flow studies that it shares with irrigation districts throughout California. ITRC assists the districts with engineering aimed at maximizing the efficient use of valuable water resources through monitoring and automated control. Sierra Control Systems has provided, installed, and tested gate monitoring/control telemetry units for several California and Nevada Irrigation Districts.

Sierra Control Systems is located in a 15,600 sq. ft. facility at 940 Mallory Way in Carson City, Nevada. Currently, SCS is headed by company president Jerry Kelley. Mr. Kelley has been with the company since its inception and is a major influence in the product integrity and engineering practices employed. Day-to-day operations are overseen by general manager Joel Mc Menamy. SCS provides skilled jobs for 22 local Nevadans. With a full-time staff of 7 engineers and the support of fabrication, manufacturing, test, field, and administrative resources, the company has never been busier. SCS still uses state-of-the-art products from Control Microsystems in their "Series 900" controllers. Sierra Control Systems is an active Control Microsystems SCADAPartner Plus member and a major user of ClearSCADA. As new products come to market, SCS carefully evaluates their usefulness and reliability. The engineers continually update their knowledge of new software and hardware with manufactures training, including reporting options and advanced HMI development. Sierra Control Systems enjoys a long reputation for quality, reliability, and service.

With decades of experience as a manufacturer of telemetry and control systems, and a pioneer in the field of systems integration of SCADA systems, Sierra Control Systems enters the new century with optimism.

Sierra Control Systems, Inc. can be reached at (775) 883-0043 or their website: sierracontrols.com

SCADAWise

SAGE ADVICE

Tools of the Trade

Software programs used for path studies are an amazing tool. They allow you to estimate losses you will have in your radio system before you get to the field, so you know what is worth testing and what is not. Although there are programs for this that cost tens of thousands of dollars, there is one piece of freeware that does a pretty good job despite its minor flaws: Radio Mobile.

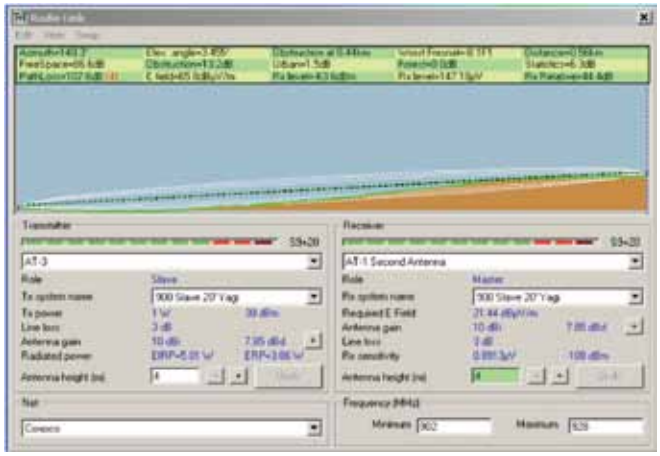
The program allows you to place radios anywhere on the earth and uses elevation data to generate a profile of the terrain between stations, which is how it calculates the path losses. It can use a variety of sources for the data, including the Shuttle Radar Topography Mission (SRTM) data from NASA.

You then input details about your radio frequency, sensitivity, antenna gain, cable losses and other information and it will generate details about the path.

Unfortunately, none of the programs for path studies take into account buildings, trees or other man-made obstructions, which can spell disaster for a radio path, and even the most careful practitioner cannot make up for this omission. On the up-side, this will tell you if there is hope for your system.

Now anyone can get a picture of what challenges they will face in building a radio network, whether it be for voice, video or data, without committing to an expensive field survey, but buyer beware. It's not that Radio Mobile doesn't accurately calculate the losses. I have compared the results to the expensive products and found that the results are pretty much identical. It's that no matter how well these programs work, they are no substitution for a real survey done in the field.

You can download a free copy of Radio Mobile at: www.cplus.org/rmw/english1.html, but please consider sending a donation to help pay the expenses of the programmer.



Navy Seals the Deal with SCADA Partner

North American Industry Tech, Inc. (NAIT), a control systems integrator in Southern California, was given the privilege of replacing an existing potable water treatment plant control system for the Naval Air Facility in El Centro, CA about three years ago. The primary reason we were invited to the site was the Navy's total dissatisfaction with the existing water treatment plant contract operators. The Navy wanted to replace the contract operators, but was fearful that a new contractor wouldn't be able to operate the existing system.

The existing water treatment plant control system was typical of most older systems, laced with many failing electrical subsystems and individual mechanical hardware components. It also seemed that it was being kept this way, perhaps in an effort to provide job security for the existing contract operators.

Prior to being awarded the project, we had some serious persuading to do. The Navy personnel were under the misguided notion that all of their hardware needed to be changed. They seemed to be focused on replacement of the filter units. After our preliminary survey, we found most of the existing hardware to be acceptable, with the only exception being the control system. The potable water filter units were, actually, the only things that seemed to be working well. All the sub-systems, however, were pretty much in shambles. For the Navy, they simply wanted a potable water treatment plant that was manageable, and worked well. This would allow them to change the contract operators, if they felt necessary, while maintaining a high quality water supply base-wide.

The potable water plant was composed of seven individual pump stations, with some operating on level controls, and some operating on pressure control. Several of these pump stations were part of the filter backwash batch routine, as well as the chemical controls. The plant's existing primary control, performed by a rotating cam-type actuator with contact blocks, was totally dysfunctional. This resulted in the operators performing manual backwash functions whenever they thought it was needed, which turned out to be about every 2 or 3 days.

During the award process for the project, we assessed the issues at hand: Problem #1: Political problems between the owner and the operation staff. Problem #2: Owner's belief that the whole plant had to be changed. Problem #3: A high level of skepticism by the client that our proposed solution would solve their problems. Ultimately, the client did finally commit to letting us help solve their problems.

Due consideration was taken to select the products because of the location of the plant (in the southern California Desert), having high desert temperatures, and exposed to a dusty environment. With its 158°F temperature rating and its resistance to the corrosive environment of salty, moist air found at the base, the Control Microsystems' SCADAPack controllers were the obvious choice. Further, the high temperature rating allowed us to forgo control panel air conditioners. The model 357 was selected as its I/O count pretty much matched the I/O requirement per site.

For the SCADA management software, Control Microsystems' ClearSCADA was considered and chosen because of several factors: its open architecture, open industry standard interfaces, such as OPC, ODBC, .NET for integration with business systems; an integrated event–based historian; and an integrated zero-configuration web server, making remote access easy.

As this was NAIT's first experience working with SCADAPack controllers, it gave us a chance to work with new products and protocols. During program development, we found the SCADAPack programming almost identical to the Modicon series of controllers. The programming software for the controllers was similar enough that using TelePACE was a major plus. In short, we discovered that the price of a SCADAPack 357 was close to that of a Modicon Compact (with limited I/O), but we got (almost) all the I/O we needed for this fairly large project, plus the PLC programming software enabled us to hit the ground running. Additionally (and here's the real icing on the cake), this controller has the same command set as the most expensive controllers you can buy, and it supports TCP/IP, USB, RS232, and RS485 right out of the box.

We ended up using a primary control panel located in the water plant control building next to the Motor Control Center, with one remote terminal unit (RTU) located next to the filter units. The two panels communicate using Modbus over RS485.

Implementing ClearSCADA was an entirely different situation. The learning curve initially seemed steep, since ClearSCADA is dramatically different from the other SCADA software we had been using for the last 20 years. We can actually say though, five implemented systems later, we have found that using ClearSCADA as a SCADA management software saves development time and allows many more options without the laborious necessity of using custom programming, as opposed to

configuration. We will never go back to the other HMI packages. The ease of connecting to end devices is one of the most important features of this software over all the others.

The control system implemented for the Navy has now been in operation for about 3 years. After the complete automation upgrade, the plant sits there most of the time making high quality potable water without operator intervention, as designed. It is worth mentioning that, since the upgrade, both filter units are rarely used; the plant almost always runs with only one of the two filters online, and backwashes automatically based on the water column within the filter unit. Our outdoor NEMA 4 RTU panel, which is located in an uncovered metallic enclosure regularly subjected to temperatures in excess of 115 degrees, has not experienced a single failure.

Since this level of automation was established at the plant, the Navy has cycled through three different contract operators until finding one they are happy with. They feel this would not have been possible without the plant running, and continuing to produce high quality potable water, on its own during the changeover and familiarity periods of the new operations staff.

At the conclusion of this project, we teamed with Control MicroSystems as an Authorized SCADA Partner, and consider their products to be our front line hardware and software.

— Kent Surratt
North American Industry Tech (NAIT)

Control Microsystems is becoming Schneider Electric

Continued from page 1

Control Microsystems' Evolution

Our evolution to Schneider Electric, the global specialist in energy management, re-affirms our commitment to provide you with innovative remote SCADA and telemetry solutions, best-in-class customer service, and exceptional quality in everything we do. We are proud to be your partner, and we are dedicated to helping you make the most of your energy.

About Schneider Electric:

As a global specialist in energy management with operations in more than 100 countries, Schneider Electric offers integrated solutions across multiple market segments, including leadership positions in energy and infrastructure, industrial processes, building automation, and data centres/networks, as well as a broad presence in residential applications. Focused on making energy safe, reliable, and efficient, the company's 100,000 plus employees achieved sales of 15.8 billion euros in 2009, through an active commitment to help individuals and organizations *"Make the most of their energy."*

www.schneider-electric.com

The "Onion" Perspective

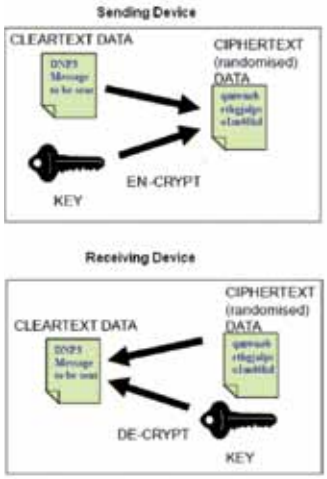
Continued from page 1

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.

The manner in which encryption is achieved is complex and requires the communicating devices to share secret knowledge. In general, this secret knowledge takes the form of a sequence of characters, known as a key. A good key has similar properties to a good internet password. It should be long and have random characters. Anyone who does not have the key cannot determine the meaning of the message without a great deal of effort.

How much effort? Like any form of physical or electronic security, encryption can be defeated, which is done by obtaining the key. There are different ways to obtain a key. A brute force approach involves testing random keys until the right key is found. This often requires a large sample of transaction data and lots of computer processing time. Some types of encryption might require hundreds of years of computer processing time to break in this way. The huge computational cost renders such an approach impractical.

It is much easier to obtain a key by tricking operators or infiltrating computer systems and accessing stored keys, or even by breaking into a site and stealing a field device. This is where the onion model comes in. The other layers of security, like physical locks, operating procedures and separate corporate networks, keep the encryption key safe.



There is a price to be paid for the security of encryption. Firstly, encrypting and decrypting involve numerous mathematical calculations. A SCADA device must be powerful enough to perform these calculations while still carrying out its traditional tasks of communication, monitoring and control.

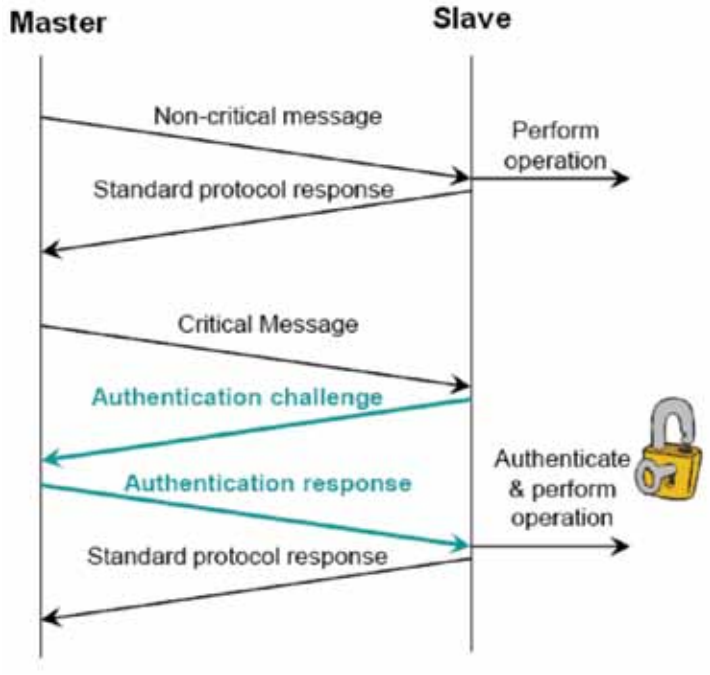
Secondly, encrypted communications take up more bandwidth. All encrypted messages have extra header information to help handle routing and encrypting. Short messages must be stuffed with extra random bytes, so that the message type is not made obvious by its size.

Lastly, the system's configuration becomes more complicated, as all devices on an encrypted network must be given security keys. This cost of inconvenience is true of any kind of security, and is not limited to encryption. It can be minimised by having a common key for the entire network, but this will make the network more vulnerable should that single key fall into the wrong hands. At the opposite end of the security spectrum, every single pair of devices could have a security key. While this system would be more complex to set up, a large number of keys would have to be discovered before the system was seriously compromised.

Authentication – Challenge & Response

Authentication is the process of one part of a SCADA system proving its identity to another. Whenever a SCADA device receives commands to perform controls or respond with data, it will challenge the sending device using a special message. 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. Think of this like a bouncer demanding to see ID before he lets you into a night club: Challenge and Response.

Like encryption, authentication requires two SCADA devices to have a mutually known secret key. Whereas encryption uses its key to transform entire messages into encrypted bytes, challenges and challenge responses are created by using the key to create a special digital signature. The mathematics is similar to that of encryption, but only a small amount of data needs to be manipulated. This means that authentication is computationally far cheaper than encryption. Authentication prevents malicious parties from controlling the SCADA device, but it will not stop them from intercepting and reading messages.



At this point, it may seem like authentication is a stripped down version of encryption, but this is not true. Authentication guarantees that the sender of the control has the authority to perform that control. With encryption, the message could be forwarded from a SCADA device that is encrypting a message on behalf of a sender who does not have the authority to issue such a control. For example, a misconfigured peer device or a malicious user may be the source of the control, but without the authentication key, any such requests will be denied.

Authentication is associated with users. A user can be a device on the SCADA network or an operator using a piece of interface software. There can be a single generic authentication user used by all staff and devices on a network. At the other extreme, there can be an authentication user for each SCADA device and individual who needs to perform protected operations.

Authentication comes with costs similar to that of encryption. The extra processor performance overhead is smaller than that of encryption, but is still present. Extra bandwidth is required for the header information and Challenge/Response messages. Keys must still be managed properly, lest they fall into the wrong hands.

Choosing the layers

The government mandates the deployment of security technology for some SCADA systems, while leaving others free to use it or leave it. We must remember that, even within a security mandate, there is scope for choice about how to implement the security system: authentication or encryption, or both.

Remember that encryption hides the messages on your SCADA network. If you have sensitive data being transmitted, you need to hide it. Authentication leaves the messages visible, but verifies the identity of the sender of the message. If you have critical controls, you need to guarantee they are legitimate.

Keys to Security

As previously mentioned, an encryption system can use a single key or a separate key for every communication link in the system, depending on the desired complexity. An authentication system can have a generic user or a user for every operator and SCADA device. More keys mean more security, as well as more overhead in keeping the keys up-to-date and secure. While it is difficult to generalize this decision, a straightforward choice is authentication keys for a few categories of users and encryption keys for several logical subgroups of the SCADA network.

Perhaps the wisest approach is to start with a very simple security setup and revise it upwards as the organisation becomes more familiar with a secure SCADA system.

It is beyond the scope of this article to discuss the many other aspects of security, but keep in mind that the other security layers will need to protect the keys of the encryption and authentication layers. Well secured physical sites, good log auditing and disciplined key distribution and update procedures all go a long way towards this end.

The ever expanding digital age means that cyber security issues are with us and are here to stay. It is in everyone's interest to be informed about SCADA security. Encryption and authentication are the newest layers in a comprehensive plan for a secure SCADA network. Layer upon layer upon layer, just like the onion.

— Metin Ozturk, Senior Engineering Specialist and SCADA Analyst, Control Microsystems, a Schneider Electric Company

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

September 9, 2010	**CWEA/Tri-Counties September Workshop & Exhibit,** San Luis Obispo, CA
September 14, 2010	**CWEA/San Diego Section & SDCWWG 3rd Annual Joint Vendor Fair,** Poway, CA
September 16, 2010	**CWEA Northern Regional Training Conference,** Modesto, CA
September 28-29, 2010	**Tri-State Seminar on the River,** Primm, NV
October 2-6, 2010	**WEFTEC '10 – 83rd Annual Technical Exhibition & Conference,** New Orleans, LA
October 5-8, 2010	**CA-NV AWWA 2010 Fall Conference,** Sacramento, CA
Oct 17-19, 2010	**Control Microsystems' 2010 SCADA & Wireless Instrumentation Symposium*,** San Antonio, TX.
October 26, 2010	**ISA/Orange County Section AutomationOC Expo & Oktoberfest,** Huntington Beach, CA
November 3, 2010	**Free SCADA Seminar*,** Newport Beach, CA
November 4, 2010	**Free SCADA Seminar*,** Walnut Creek, CA
November 15-17, 2010	**SCADAPack TelePACE Studio Training*,** Mill Valley, CA
December 13-16, 2010	**ClearSCADA Training Course*,** Corte Madera, CA
February 1-3, 2011	**DistribuTECH 2011 Conference & Exhibition,** San Diego, CA
February 15-17, 2011	**SCADAPack TelePACE Studio Training*,** Mill Valley, CA
February 28 – March 3, 2011	**ClearSCADA Training Course*,** Mill Valley, CA
April 13-14, 2011	**CWEA Annual Conference,** Ontario, CA

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