The Sage Advisor

SCADA, SECURITY & AUTOMATION NEWSLETTER

Volume 28, Issue 2 • Fall 2018

A Publication of Sage Designs, Inc.

Securing Your SCADA System

The Department of Homeland Security is on the hunt for groups, individuals, and their strategies to turn our systems against us. They know what we know, that Havex, Sandworm, and Stuxnet attacks against dozens of pieces of critical infrastructure have included dams and nuclear power among their targets. As our world becomes more efficient, it also becomes more complex, and so does securing against those that wish to harm others or make personal gains at the public's expense. Without updates to infrastructure technology it's only a matter of time before a critical breach slips past and stirs the public into outrage. Security is a battle of Cat and Mouse between automation professionals and those agencies and individuals who would damage or destroy the systems that support our quality of life.

Cybersecurity recommendations for Water and Wastewater SCADA can be found in Presidential Decision Directive 63 (PDD-63), which identifies water and wastewater industries as Critical Infrastructure whose destruction would have a debilitating effect on the United States. PDD-63 adds to and replaces PPD-21 issued by the Obama administration, which itself superseded Homeland Security Presidential Directive 7 (HSPD-7). These directives specifically list Water, Wastewater, and SCADA as at-risk and in need of updates to thwart attacks ranging in source from individuals to nation-states. These orders can be found summarized in Congressional reports, most recently Cybersecurity: Critical Infrastructure Authoritative Reports and Resources. Many of these documents refer to the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastucture Cybersecurity. The information in this article is provided as supplemental to those documents with specific recommendations for SCADA compliance.

The communications protocols used to control our SCADA systems have recently come under scrutiny by government and civilian oversight. While a large percentage of existing SCADA systems in our industry still employ Modbus and other extremely vulnerable protocols, we are beginning to see more and more systems moving towards secure protocols such as DNP3 with Secure Authentication (SA). Secure Authentication balances security and function by bringing a high level of protection against attacks targeting remote systems and, through purpose-driven construction of the protocol, creating only a minimal burden on the limited bandwidth found in typical SCADA media.

DNP3 SA protects against:

- Injection of unintended messages such as misleading data or illegitimate controls (Protocol attacks)
- Third party capture of old messages and retransmitting of control or other commands (Replay)
- Modification to the contents of messages (Data tampering)
- 3rd parties pretending to be one of the communication devices (Spoofing)
- Attempts to crack the "secret code" that protects keys (Encryption Attacks)
- Attempts to crack the "secret code' that proves data hasn't been changed (Signature)

We are seeing a greater number of SCADA systems using TCP/IP communications even in the narrow band licensed radio world, even here there is a need for SCADA and ID security. TCP/IP is not uniformly distributed to all end points in remote SCADA communications systems leaving islands of vulnerable devices. This is due to the use of many types of physical media such as dial-up, serial devices, older narrow band radios that don't support Ethernet connections and even where field devices are using TCP/IP but do not have the processing

Securing Your SCADA System, *Continued on Page 4*

DNP3 Protocol at a Glance

- Logic programming not required for most DNP applications
- Easily configured using Unity for SCADAPack, Telepace™, Workbench (IEC61131-3) and Realflo™ environments
- DNP Master and Slave modes supported
- Unsolicited messaging supported
- Change-of-State and Log-All event types supported
- Available through Ethernet and serial communicationports

Overview

Schneider Electric's complete family of SCADAPack™ Smart RTUs (Remote Terminal Units) and gas flow computers are available with DNP3 Protocol. Today's increasingly complex SCADA networks demand that data-transfer protocols be sufficiently flexible to meet communication challenges while remaining easy-to-configure. Our intelligent implementation of DNP3 protocol succeeds on both counts.

Enhanced Interoperability

DNP3, or Distributed Network Protocol, is a standards-based communication protocol developed to enhance interoperability among systems in the electric utility, oil & gas, water/waste water and security industries. It is a flexible, efficient, non-proprietary and layered protocol that offers higher data-transfer integrity than most conventional communication protocols.

DNP3 is suitable for implementation anywhere within a SCADA environment, including RTU to IED (Intelligent Electronic Device), master-to-remote, peer-to-peer and network communication applications.

The DNP3 User Group, (www.dnp.org), ensures continuous improvement of the protocol in the everchanging technological climate of industrial control.

Easily Configured

DNP3 is configured in TelePACE, Workbench and Realflo programming environments with an easy-to-use dialog. Application and data layers, master poll and mimic mode, address mapping, message routing and IO points are all configured on the same dialog. The majority of DNP3 applications can be configured using this dialog, thereby eliminating the need for additional logic programming.

Schneider Electric

TelePACE, Workbench, Realflo and Firmware Loader applications also support DNP connections to Smart RTUs. Firmware and applications can be downloaded to the Smart RTU and logic execution monitored on-line using a DNP connection.

Additional DNP Functions

Custom logic functions are available when additional DNP functionality is required. These functions allow the RTU logic application to trigger various DNP events, including class polls, clock synchronization and unsolicited response messages.

Another set of dedicated function blocks allows the RTU logic to access DNP diagnostic information including DNP connection status, event-count by point type and class, port communication statistics and station message statistics.

DNP3 Protocol, *Continued on Page 7*

Inside this issue:

City of Oceanside Successfully Launches 43-square mile Trio Radio Network

The City of Oceanside is located along California's golden coast. It is the third largest city in San Diego County. The City was incorporated on July 3rd 1888. Oceanside's Water Utilities Department purchases water from the San Diego County Water Authority and treats groundwater supplies and delivers potable water throughout the City. Water uses include domestic, commercial, irrigation and fire protection purposes. Serving a population of 176,000 with 44,000 water accounts across a 42 square mile area, Oceanside operates 450 miles of pipelines, two fresh water treatment plants with a total daily capacity of 40 MG, two waste water treatment plants with a daily capacity of 12-13 MG, 34 sewer lift stations and 31 water or distribution remote sites.

Oceanside's previous telemetry system was comprised of 42 phone lines and licensed radios. The ongoing monthly costs to operate the telephone network were an expensive nuisance, and their radios lacked Modbus TCP support. Management in the Water Department of Oceanside determined that an upgrade was necessary. The goals of the upgrade were:

- The need for a system free of leased or proprietary equipment,
- Elimination of monthly costs,
- Support for Modbus TCP
- Inclusion of redundancy.

Fiber was considered and eliminated as an option because of the expense involved to roll out to remote sites. Cellular was considered and eliminated as it would once again require monthly fees for each site. It was determined that radio would be the best option going forward. After consideration of different manufacturers, Oceanside standardized on the Schneider Electric Trio J-series radios in the unlicensed 900-mhz spread spectrum range.

The Schneider Electric Trio J-series 900-Mhz spread spectrum radios met all aspects of the City's project goals, being designed to work with many controllers and types of equipment, supporting Modbus-TCP, operating on frequencies free from fees, and has the ability to run as a redundant pair. The small form factor of the redundant pair was a particular and unanticipated benefit to Oceanside, as their previous MDS radios required a large rack and would take up too much space in the panels out in the field.

Utilizing Schneider Electric's support to overcome some initial difficulties, they were soon able to take advantage of more advanced features. Oceanside says they found the channel hopping feature of the Trio radios to be an elegant and sophisticated solution to mitigate some of the expected signal interference found in the unlicensed spectrum. Using radio filters and horizontal polarization, Oceanside was able to cut out interference from a nearby military base and secure clear signal to their outstations. While rolling out the radios to their entire system, Oceanside became fans of the built in packet test which can be used to ensure that two points talk successfully before unplugging the old connections. They also particularly appreciated the easy-to-use and intuitive web interface for the Trio-series radios. Thanks to this interface, if trouble shooting a radio is required, SCADA technicians only take a regular laptop out into the field to do so. No special software is required.

Even though Oceanside paid for (and highly recommends having) a professional radio path study done before starting the project, they ran into a few situations endemic to radio network construction, namely situations where the radio path study said two given points should communicate just fine, but in the real world did not.

Utilizing the Trio's ability to relay traffic they were able to overcome this by sending radio signals through alternative paths. This flexibility eliminated the need for other costly fixes midway through the project.

Overall the project has been a resounding success, the planning and implementation of the radio rollout was smooth thanks to the built in features of the Trio radios. The Trio radios exceeded expectations and Oceanside now has both better function and a much smaller operating cost for their network.

— **Chuck Reuck**, SCADA Consultant
City of Oceanside
CReuck@ci.oceanside.ca.us

Water network security here.
For the ultimate water fight here.

Life Is On | Schneider Electric

Whatever the size and complexity, ensuring safe, reliable and secure operation from field to enterprise

Flexible I/O configuration to handle expansions

Reduce engineering time with replicated object templates

SCADA Components:

- SCADA Expert ClearSCADA management software
- SCADAPack Smart RTUs & rPACs
- Accutech wireless instrumentation
- Trio data radios

For more information, live equipment demonstrations, a listing of contact-hour certified classes near you, or to schedule a consultation on solving your SCADA challenges, contact your local Schneider Electric | TRSS representative:

Sage Designs, Inc.
SCADA & Security Products

(888) 275-7243
www.sagedesignsinc.com
www.scadawise.com

SCADAWise
Training

SAGE DESIGNS, INC.
SCADA & Security Products

SCADAWise

Free SCADA Security Seminar

Next Gen SCADAPack with Unity-based Logic & DNP3 Secure Authentication

Registration Form

November 6, 2018
8:00am – Noon
Northern California – Larkspur Landing Hotel
5535 Johnson Dr.
Pleasanton, CA 94588

November 8, 2018
8:00am – Noon
Southern California – Invensys Complex
26561 Rancho Parkway South
Lake Forest, CA 92630

Schedule of Topics:

8:00 – 8:15 **Continental Breakfast & Introductions**

Speakers will include:
Asim Farooq, Cybersecurity and ClearSCADA Expert, Schneider Electric
Nick Smith, Senior Application Engineer-Telemetry & Hardware Specialist, Schneider Electric
Tony Sannella, Sage Designs Inc. Sales Engineer
Gregory Ochs, US Western Regional Sales Manager, Schneider Electric

8:15 – 9:15 **DNP3 Secure Authentication**

Features and basic functions of DNP3 Secure Authentication will be presented, including special emphasis on implementation for the newly released SCADAPack x70-series controllers.

9:15 – 10:15 **Secure Authentication in SCADA Master Station**

Implementation of Secure Authentication protocol in HMIs will be presented, with special emphasis on EcoStruxure GeoSCADA (ClearSCADA) SCADA Master Station and tight integration with SCADAPack controllers.

10:30 – 11:30 **Remote Connect / Unity Logic for SCADAPack x70-Series Controllers**

An introduction to the new Remote Connect programming utility for SCADAPack controllers, a powerful new tool based on Unity logic.

11:30 – 12:00 **SCADAPack x70-Series Hardware Review & Demonstration**

Presentation of the newly released SCADAPack 575 and a sneak peak at the upcoming SCADAPack 574.

12:00 –12:15 **Q&As and Open Forum**

Pre-registration Required

Registration Info: Please complete and return this form to indicate your attendance. Although there is no cost for this event, space is limited. Continental breakfast will be provided to all registered attendees.

☐ **Register me for Pleasanton on November 6, 2018 (NorCal)**

☐ **Register me for Lake Forest on November 8, 2018 (SoCal)**

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

Completed registration forms should be sent to orders@scadawise.com

Securing Your SCADA System, *continued from page 1*

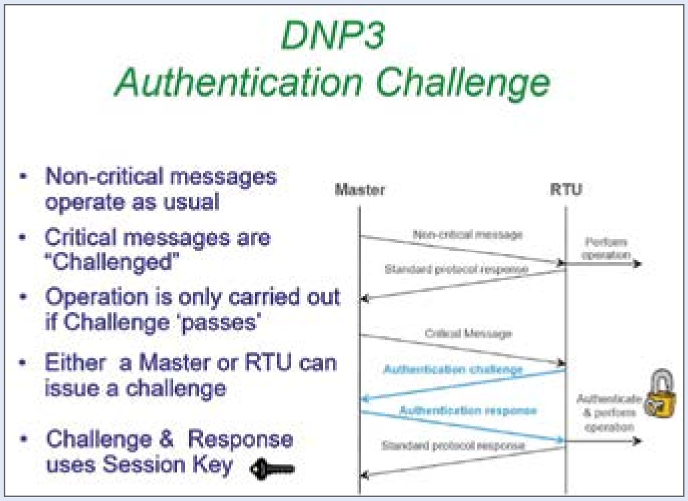
power to support high overhead IT security such as TLS. Where TCP/IP is in use, SCADA standards are now asking for both application security and protocol security layers.

The best security mechanisms to combat these threats in the SCADA environment are:

- Hiding the data content of messages (Encryption)
- Challenging senders of control messages to prove their identity and validate the message (Authentication)

As more SCADA users adopt security practices to combat these dangers an open standard for protection of SCADA communications has emerged. DNP3 Secure Authentication (SA) is based on this IEC62351 standard. The IEC62351 suite is a part of the wider IEC62334 suite previously known as ISA Secure.

DNP3 SA uses a dynamically changing key in a process called key rotation. The dynamic key is exchanged in DNP3 SA messages, encrypted so that the key can't be learned by eavesdropping. This dynamic key requires fixed 'secrets' (update keys) at both ends of the communications for deriving the dynamic key. DNP3 Secure Authentication uses cryptographic Signature and Encryption algorithms


DNP3
Authentication Challenge

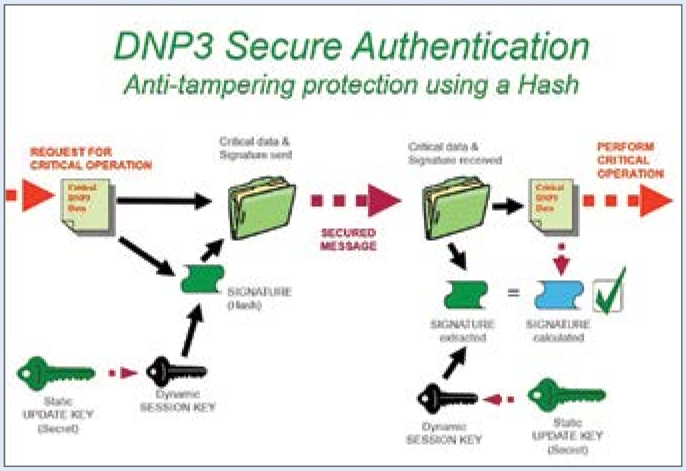
- Non-critical messages operate as usual
- Critical messages are "Challenged"
- Operation is only carried out if Challenge 'passes'
- Either a Master or RTU can issue a challenge
- Challenge & Response uses Session Key

The philosophy of DNP3 SA is based on an Authentication challenge in which the sender must prove who they are before a critical message is acted upon. These "critical" messages include such things as controls, set point writes, configuration changes, setting the time, firmware updates and application software updates. The data itself is not encrypted but the "signature" prevents tampering. Embedded cryptographic information in messages protects against "Replay" of messages but this method uses limited bandwidth and processing power making it viable in those SCADA systems with limited bandwidth and modestly powerful remote controllers. Schneider Electric has integrated these solutions into SCADAPack and ClearSCADA via a process where the best-practice of key management for the "Update Keys" is done from an independent security authority. The security authority is generally a software package running on a computer which is not connected to the SCADA system or other networks. (SCADAPacks offer a software package called Security Administrator to execute this function for DNP3 SA). The security administrator then generates a Master Key. The Master Key customizes the SCADAPack security configuration to specifically for an organization. The SCADAPack reads this information.

There are various security modes available within the Security Administrator program for securing access to the RTU when using DNP3 protocol:

- Default Key Mode, in which the configuration software and SCADAPack devices automatically communicate using the key provided out-of-the-box. This mode helps to protect against external attempts to access the protocol, but not against outside copies of the configuration software. The default key mode is provided for simplifying initial access to a SCADAPack device. It is strongly recommended that other key modes are used in field installations. This is the lowest security option.
- Common Key Mode, in which a new key is provided for each instance of the configuration software, disabling the default key and configuring one configuration tool key for the SCADAPack system. You deploy the same configuration security to each instance of the configuration software. The advantage of this mode is that you only have to maintain one key for all your configuration software installations. However, if a laptop with an instance of the configuration software is compromised, the configuration security files will need to be updated on each instance of the configuration software in your SCADA system, as well as each associated SCADAPack. This is a medium security option.
- Unique Key Mode, in which each instance of the configuration software has a unique key and each SCADAPack device is aware of the authorized configuration. Each instance of the configuration software is identified using a specific security configuration file, which is tied to a Machine ID to restrict operation of the software to authorized PCs only. If you add, edit or remove instances of the configuration software in the system, you will need to update each SCADAPack with the revised settings. The advantage of this mode is that if a laptop with an instance of the configuration software is compromised, there is no need to update the security configuration file for each instance of the configuration software. You can remove the compromised configuration in Security Administrator and generate new security configuration files to be deployed to the SCADAPack devices This is the highest security option.
- Aggressive Mode, in which DNP3 secure authentication communications are optimized to reduce the amount of protocol overhead. Overhead is reduced by including the action and the authentication information for an anticipated challenge inside one operation request message. The receiving device does not have to issue a challenge message, only a response to say the request has been executed. The first secure exchange between DNP3 devices uses full authentication transactions, but subsequent transactions can use aggressive mode, reducing the message transactions for critical operations from 4 exchanges to 2. There will again be a full exchange between devices when the Change Interval OR the Change Count has been reached.

DNP3 SA provides a layer of practical security by Securing Master-Station-to-Outstation Communications by challenging controls, configuration changes and Firmware changes. It secures Outstation to Outstation communications by authenticating Peer to Peer communications between devices. And it secures configuration tool to Outstation communication.


DNP3 Secure Authentication
Anti-tampering protection using a Hash

REQUEST FOR CRITICAL OPERATION
Critical DNP3 Data
Critical data & Signature send
SECURED MESSAGE
Critical data & Signature received
Critical DNP3 Data
PERFORM CRITICAL OPERATION
SIGNATURE (Hash)
SIGNATURE extracted
=
SIGNATURE calculated
Static UPDATE KEY (Secret)
Dynamic SESSION KEY
Dynamic SESSION KEY
Static UPDATE KEY (Secret)

In short, DNP3 SA allows your system to operate in confidence that only your team can send control messages and manage your remote RTUs; and that critical messages cannot be replayed by third parties; all with only a minimal amount of communications overhead. If you are interested in a secure and reliable SCADA system, please call Sage Designs for more information.

SAGE DESIGNS, INC.
SCADA & Security Products

Earn Contact Hours

Schneider Electric

SCADAWise™ Training Classes

ClearSCADA

ClearSCADA Level 1 Training Course

October 15-18, 2018 — Mill Valley, CA
March 11-14, 2019 — Mill Valley, CA
May 20-23, 2019 — Buena Park, 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	$2,200

Sage Designs' ClearSCADA Level 1 Course has been certified by (a) the California Department of Public Health as courses qualifying for contact hour credit for Water Operator Certification for Drinking Water Treatment or Distribution in the State of California and (b) the State of Nevada Department of Environmental Protection, Bureau of Drinking Water for contact hours towards the Nevada Drinking Water Operator Certification Program.

(28 Contact Hours)

ClearSCADA Level 2 Training Course

2019 Dates TBD

Day 1 (8AM - 4PM)	Installation, Understanding the Architecture of ClearSCADA, Application Design Considerations, Server Automation Interface, ClearSCADA Logic Engine, Using ODBC and SQL.
Day 2 (8AM - 4PM)	Advanced Mimic Design and Techniques, Data Grids and Data Tables.
Day 3 (8AM - 1PM)	Accessing Historical Data, Ad Hoc trends, Archiving

Prerequisite: ClearSCADA Level 1 Training Course

Cost: ClearSCADA Level 2 Training Course	$1,650

SCADAPack

Telepace Studio Training Course

October 2-3, 2018 — Mill Valley, CA
March 5-6, 2019 — Mill Valley, CA
May 14-15, 2019 — Buena Park, CA

Day 1 (8AM - 5PM)	SCADAPack controller operation, Series 5000 I/O, Telepace Studio introduction
Day 2 (8AM - 5PM)	Telepace Studio advanced programming techniques and advanced functions
Cost: SCADAPack Telepace Studio Course	$1,650*

* You must have a licensed copy of Telepace Studio installed on your computer for this course. If you do not have a licensed copy, you may purchase one with the class at a special course price. Course price for Telepace Studio: $510 + applicable CA sales taxes

Sage Designs' Telepace Studio Course has been certified by (a) the California Department of Public Health as courses qualifying for contact hour credit for Water Operator Certification for Drinking Water Treatment or Distribution in the State of California and (b) the State of Nevada Department of Environmental Protection, Bureau of Drinking Water for contact hours towards the Nevada Drinking Water Operator Certification Program.

(14 Contact Hours)

Instructors: ClearSCADA Level 1 & Telepace classes will be taught by Tony Sannellla, Sage Designs, a Factory-Certified Instructor. SCADA Level 2 classes will be taught by a SEUSA-certified training 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.

*You must have a licensed copy of Telepace Studio to take the Telepace course. We offer a course price for a license or you may purchase through your local Schneider Electric TRSS representative.

What is provided? Course manual, daily continental breakfast, lunch & beverages.

Free Hands-On Test Drive

Call to Schedule a Test Drive
Call 1-888-ASK-SAGE
email: info@scadawise.com

SAGE DESIGNS, INC.
SCADA & Security Products

Download the Registration form at: http://www.SCADAWise.com

*** * * Registration Deadline: 4 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.

DNP3 Protocol at a Glance, *continued from page 1*

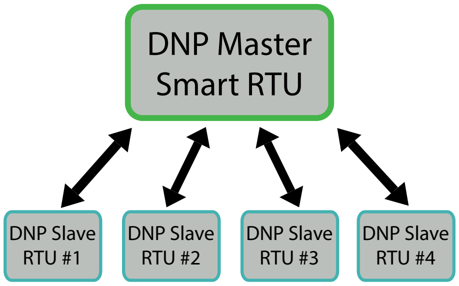
DNP3 enables tight integration between SCADAPack E RTUs and ClearSCADA™ enterprise software with features that include automatic/manual downloading of firmware, configuration and application from ClearSCADA to the RTU, trend reading, alarm time profile and security configuration downloading.

Features

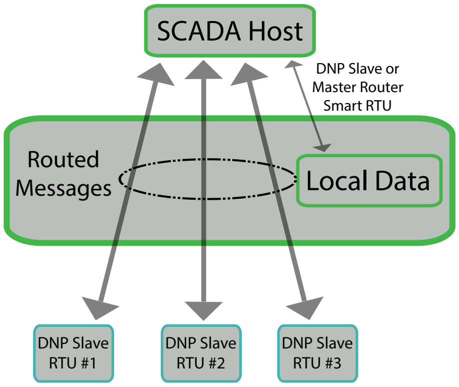
Master Mode

SCADAPack 32 and SCADAPack 300 Smart RTUs support DNP3 master functionality. A DNP master can initiate polls for static data (Class 0) and event data (Class 1, 2, 3) and accept unsolicited event data from slave RTUs.

A typical DNP application consists of a DNP master Smart RTU, routinely polling a number of DNP slave Smart RTUs as shown below.



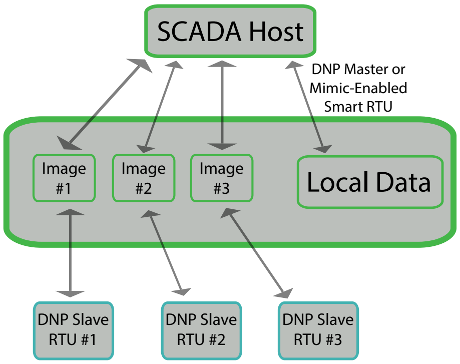
In many applications the DNP master RTU or DNP slave RTU is simply required to route messages to/from a SCADA host as shown below.



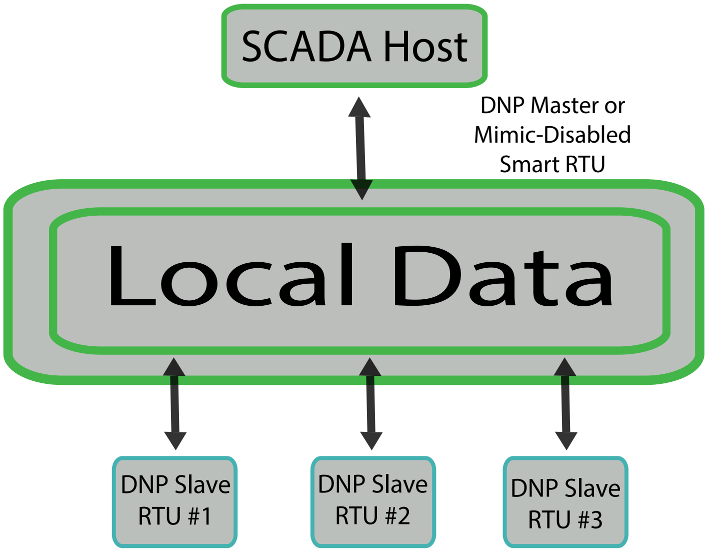
In addition to message routing, master functionality also includes data concentration, using mimic and mapping modes.

In mimic mode the master maintains ‘images’ of remote site data for upload by the SCADA host (or other master). This is recommended in applications where the slave RTUs are on low speed or non-continuous links (eg. Dial-up).

This allows the master to respond to SCADA host requests for remote slave data from its buffered images as shown on the right. A typical DNP application consists of a DNP master Smart RTU, routinely polling a number of DNP slave Smart RTUs as shown below.



In applications where data concentration is required, the master is able to map remote data to its own local registers. This is accomplished using the mastermapping mode as shown below.



Slave Mode

All SCADAPack Smart RTUs and gas flow computers support DNP3 slave functionality. When configured as a DNP3 slave, the RTU can be polled for static data (Class 0), or event data (Class 1, 2, 3) by a DNP master. The RTU is also able to send unsolicited messages containing event data to a DNP master and route messages to/from other DNP RTUs and DNP devices.

Unsolicited Messages

An important feature of DNP3 is the ability for the RTU to generate unsolicited messages sent to the master RTU/host based upon a local RTU event. An application layer menu allows event-reporting rules for each object class (1-3) to be defined.

Reporting Rules – These are defined for each object class and include:

- Enable/Disable – Turns unsolicited reporting On/Off
- Hold Time – period seconds
- Hold Count – number of unread events in the RTU history

Object Classes

Data object classes allow for the management of message content and message triggering based upon user-determined priority of the data. The data classes are assigned independently of the data priority.

Supported DNP object classes could be configured with the following priority structure:

- Class 1 – highest priority
- Class 2 – medium priority
- Class 3 – lowest priority

Class 0 is always a reference used by a master to read all DNP data objects. These are instantaneous/lastread values. The master/host polls for Class 0 data objects, on an infrequent basis and after each restart of the master or slave.

Ethernet and Serial Communication

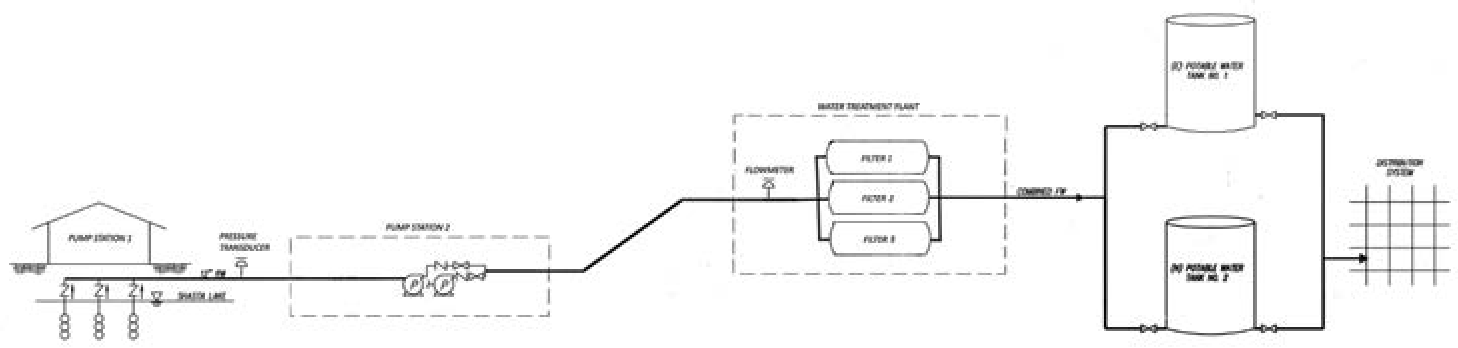
DNP3 is fully supported on all Smart RTU controller communication ports, including the serial RS-232 and RS-485 ports as well as the Ethernet TCP/IP port of the SCADAPack 32 and SCADAPack 300* Smart RTUs.

*Footnote: * Ethernet port is not available on the SCADAPack 312E, 313E, 314 and 314E RTUs.*

For more information contact your Sage Designs representative.

Innovative Control Solution from Pace Engineering

Integrating a recent project proved challenging when it came to Implementing process control with telemetry over radio links. Polling delays, occasional timeouts and varying polling cycle times all contributed to the challenge of controlling pump speed at a remote pump station. I was unexperienced with implementing DNP and didn't have the time or budget to jump into it for this project, so I was stuck with using Modbus and had to find a way to adjust the remote station pump speed with a signal that isn't local at the pump station. Unable to use a PID loop for process control, I was able to find success by using an iterative method that takes a little longer for the process to settle, but is well within acceptable operation. I was able to "get away" with my solution because of a few specific behaviors of the system described below, but the secondary lesson learned here is that proper implementation of DNP could have been a more straightforward solution (minus the complexities of DNP, that is).



The Problem

The project was specifically a WTP with two remote pump stations. Pump Station 1 (PS1) draws water from the bottom of the lake and pressurizes a manifold. The pressurized manifold provides water to the suction side of Pump Station 2 (PS2). PS2 then pushes the water up several hundred feet to the Water Treatment Plant (WTP). One can surmise that PS2 needs as constant a supply of water as possible, as any change in suction side pressure will affect the discharge side flow.

PS1 pump speeds are controlled by a PID loop that maintains an operator adjustable pressure setpoint, typically around 30 PSI. This loop was easy to implement, as the Process Value signal came from a pressure transducer that is located at PS1.

PS2 pump speeds are adjusted to maintain an operator adjustable flow setpoint, which varies based on the flow demands of the WTP; this number changes based on how many filters are called to run (each filter train has its own flow setpoint) or if one of the filters is backwashing. Unfortunately, the flowmeter used for the Process Value is located at the WTP, not at PS2. The problem here is that the flow is only updated at PS2 when it is polled by the radio.

Polling sites one at a time inherently introduces lag time for the polling cycle, which means data read from and written to remote sites can be delayed for a significant amount of time. This project has several remote locations and every site will obviously increase the polly cycle time. Even with strong radio signals, the time it takes to poll a site can vary and occasional timeouts can significantly change the duration of polling all remote sites. Thus with Modbus, the update of data coming from and going to remote sites cannot be reliably predicted. The implementation of the DNP protocol for communications can mitigate the polling cycle delay by proper use of data classes, but DNP is more complicated to properly implement. The increased complexity of DNP makes training and experience very valuable, if not essential, for proper implementation. In my situation I simply didn't have the time or budget to realistically learn and get experienced, so I felt I had no choice but to still with Modbus this time.

The Solution

Initially I did try a PID loop with a slow cycle time, but not surprisingly found it inadequate. With the PV showing up at unpredictable times coupled with the unreasonably slow cycle time, I never got even close to a stable system and instead had pump speeds swinging back and forth. One experiment was to increase the polling of PS2; instead of polling it once per cycle, I would poll it between every site. This didn't really pan out either, because the PV data was still inconsistent in its changing and it increased polling times for the rest of the system tremendously.

I realized that there were a few things I could use to my advantage when trying to find a usable solution to my issue. First, the operation of the plant was discussed with the lead operator and the civil engineer who designed the hydraulic aspect of the system. We realized that the plant would only be operated in a somewhat narrow range of flows; the filters have a "goldilocks" range of where they tend to prefer to operate and too little flow is undesired. Additionally, the filters have a maximum flow rate cutoff based on their size.

Another aspect taken into account was how PS1 reacts to changing lake levels. Obviously if the lake levels are high, the pump doesn't have to work as hard to maintain its pressure setpoint and conversely, as the lake level drops the pump has to work harder.

Looking at the pump curves and drawing out realistic filter flow requirements and limitations (and taking into account seasonal changes), we were able to define a somewhat narrow range of speeds that the pump at PS2 would realistically operate at. Doing this allowed me to not have to worry about getting the process stable at such a wide range, which simplified things dramatically.

The first step of getting the solution to work was realizing that the PS2 pump would never run below about 90%; anything slower wasn't adequate for moving the volumes of water the WTP needs. The start process was simplified and instead of relying on the control loop to ramp the PS2 pump speeds all the way to 90% before water was even flowing, the PS2 pump is instead called to run at an initial speed of 90% until flow is seen at the WTP. A pump speed of 90% straight out of the gate means that my control loop only needs to adjust 10% of total pump speed, not 100%. Once flow is established at the WTP, PS2 then employs a watchdog that energizes a one shot every time a new flow value is received. If the flow is too low, the pump speed is increased one-half percent until the flow is within 1% of flow demand. If flow is too high, then pump speed is reduced one-half percent. If flow is within 1% of demand, then no adjustment is made. It takes several polling cycles for the flow to get up to the setpoint, but the timing is not critical to the process and the operator prefers things to come up gently to avoid water hammer. We also avoid overshooting and once the setpoint is reached, the system is very stable and flow stays well within deadband.

Conclusion

It is typical that an integrator's involvement with a project begins towards the tail end of construction, long past when design decisions cannot be changed and a significant control challenge is presented. When this happens, it is up to the integrator to provide a solution under less than ideal conditions. A competent integrator should have both the ability to find solutions within the programming capabilities of the PLC they are programming, but also to be competent in solutions that may involve alternate methods of communications (Modbus vs DNP, in this case). In the future, I will definitely be looking at DNP as an alternative for critical, time based comms versus Modbus.

— **Phil Gowan**, Staff Engineer
Pace Engineering, Redding California
pgowan@paceengineering.us

PACE
ENGINEERING
REDDING, CALIFORNIA

SAGE DESIGNS, INC.
SCADA & Security Products

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

Return Service Requested

SAVE A TREE

The Sage Advisor

SCADA, SECURITY & AUTOMATION NEWSLETTER

Calendar of Events

September 24-17, 2018	**Tri-State Seminar on the River,** Las Vegas, NV
October 2-3, 2018	**TelePACE Training Class,** Mill Valley CA
October 15-18, 2018	**ClearSCADA Level 1 Training Class,** Mill Valley CA
October 22-25, 2018	**CA/NV AWWA Conference,** Rancho Mirage CA
November 6, 2018	**Sage SCADA Security Seminar,** Pleasanton, CA
November 8, 2018	**Sage SCADA Security Seminar,** Lake Forest, CA
December 12-14, 2018	**Colorado River Water Users Conference,** Las Vegas CA
January 23-25, 2019	**US Bureau of Reclamation Mid-Pacific Region Conference,** Reno NV
February 4-5, 2019	**Calif. Irrigation Institute Conference,** Sacramento CA
March 5-6, 2019	**TelePACE Training Class,** Mill Valley CA
March 11-14, 2019	**ClearSCADA Training Class,** Mill Valley CA
March 25-26, 2019	**CA/NV AWWA Spring Conference,** Sacramento CA
April 9-12, 2019	**CWEA Annual Conference,** Palm Springs CA
May 7-10, 2019	**ACWA Spring Conference,** Monterey CA
May 14-15, 2019	**TelePACE Training Class,** Buena Park CA
May 20-23, 2019	**ClearSCADA Level 1 Training Class,** Buena Park CA

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

Acknowledgements: SCADAPack™, Trio™, Realflo™, Telepace™ and ClearSCADA™ are trademarks of Schneider Electric.