Integrating Modern Substation Automation Systems With Enterprise-Level Management

Mark Nakao
Los Angeles Department of Water and Power

Simon Loo and Lee Melville
Schweitzer Engineering Laboratories, Inc.

This paper was presented at the 68th Annual Conference for Protective Relay Engineers and can be accessed at: http://dx.doi.org/10.1109/CPRE.2015.7102194.

For the complete history of this paper, refer to the next page.

Published in
Sensible Cybersecurity for Power Systems: A Collection of Technical Papers Representing Modern Solutions, 2018

Originally presented at the
68th Annual Conference for Protective Relay Engineers, March 2015

Integrating Modern Substation Automation Systems With Enterprise-Level Management

Mark Nakao, *Los Angeles Department of Water and Power*
Simon Loo and Lee Melville, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—To maintain compliance with cybersecurity requirements for power systems, the Los Angeles Department of Water and Power (LADWP) implemented a substation automation system managed by an enterprise system that supports the security, operation, testing, and maintenance of the automation components. This paper addresses the method by which the enterprise and substation components are integrated at LADWP to provide a secure and manageable system.**

Secure configuration management and centralized syslog monitoring solutions were implemented to ensure the integrity of substation equipment. Intelligent electronic device (IED) passwords are automatically changed regularly with conformance to complexity rules. IED event information is archived to a centralized server for ease of event analysis across the entire system.

An enterprise approach to compliance was incorporated through synchrophasor protocol (IEEE C37.118) to satisfy a portion of NERC CIP PRC-002-2 requirements for dynamic disturbance recording.

I. Introduction

The Los Angeles Department of Water and Power (LADWP) is responsible for the operation and maintenance of approximately 200 substations. Some of the substations have equipment that is no longer supported by manufacturers and in need of replacement. Substation equipment from different manufacturers lacks cohesion on applications, and extensive work is required to integrate the obsolete equipment into the LADWP system.

To comply with North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) PRC-002-2 requirements and create a more robust substation automation system (SAS), LADWP integrated their SAS with their enterprise system.

The primary responsibility of the enterprise system is to form a coherent collection of functions needed to support the security, operation, testing, and maintenance of the SAS. The enterprise system also collects, organizes, screens, and publishes the wealth of information produced by the SAS for use by authorized enterprise users. Secure configuration management and centralized syslog monitoring solutions were implemented to ensure the integrity of substation equipment.

II. Centralized Security

Given the number of substations, there are many locations with devices that require secure authentication for operation. A distributed approach would be difficult to manage, so a centralized approach was designed using a domain created for the LADWP supervisory control and data acquisition (SCADA) wide-area network (WAN). For ease of management, a domain controller and an active directory were set up within this domain. The reliability of the domain controller was increased using virtual machine and hardware techniques, but a second controller was added at a physically separate location to mitigate the risks associated with physical damage to the server location.

Security groups are defined within the active directory configuration that are representative of the roles and responsibilities for personnel at LADWP. This simplifies personnel changes by removing the need for individual user account configurations. Automation devices that are Lightweight Directory Access Protocol-compatible (LDAP-compatible) within the SAS architecture can take advantage of these security groups by referencing them in their own security settings. This streamlines the approach to security by tying all devices to a centralized reference.

Modern substations use substation-based human-machine interfaces (HMIs) to operate breakers, review relay settings, and allow many other actions that can shorten outage times or prevent outages caused by hackers. Access to the substation HMI is accomplished using LDAP authentication as part of the centralized approach. If a person with operational access to the HMI is moved out of the operational group, the security group is modified centrally and that person is no longer able to access the HMI at any substation.

Additional security is implemented at LADWP using a group policy to lock down all Microsoft® Windows® client machines within the SAS architecture. Group policy defined at the domain controller is used in conjunction with a well-defined hierarchy of layers. Multiple layers of reliable security control are part of a complete best-practice security approach.

As shown in Fig. 1, the first layer of security is an access gateway, the second layer is a real-time controller (RTC), and the last layer is intelligent electronic devices (IEDs) controlling substation equipment. This multilayer approach to substation equipment protection deters hackers and provides time for power operators or security software to counteract cyberattacks.

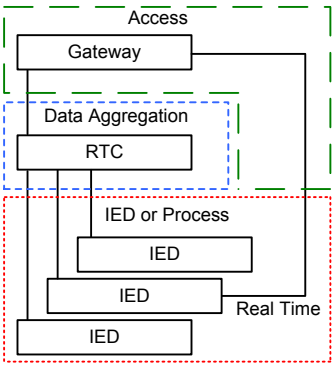

Fig. 1. Multilayer substation security approach

III. Scalable Architecture

Existing standards for LADWP server hardware were incorporated into the SAS enterprise hardware design. This approach takes advantage of the existing knowledge of LADWP staff, reducing the effort to understand the new system. It also simplifies the maintenance and operation of the new hardware.

Two sets of servers were implemented at physically separate locations to support redundant domain controllers. Also, the administrative and operational functions of the enterprise system were divided between separate servers in each location.

Redundancy was built into one of the hardware specifications by the use of dual servers, two storage area network (SAN) switches, and redundant array of independent disk (RAID) controllers and technology. Fig. 2 shows the basic architecture used to support this high-availability setup.

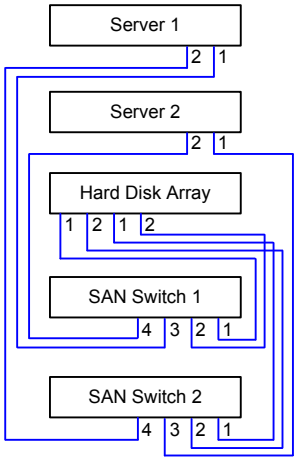

Fig. 2. Enterprise hardware redundant architecture

For a second set of servers, a scaled-down approach to redundancy was used. This included the use of a virtual storage appliance, taking a software-based approach to managing the hard disk array.

The use of disk arrays allows for the addition of hard drives with very little effort, allowing for future expansion. Additional scalability is realized with a virtual machine architecture, which supports multiple virtual servers on each physical server provided. If additional servers are required, they can be added into the virtual environment, providing simple scalability.

In each substation, both the new SAS equipment and the network need to be rugged to endure the harsh environment, robust to support multiple applications simultaneously, and flexible to accommodate user logic for advanced calculations. The microprocessor-based relays that were implemented in the SAS project support various protection elements, multiple protocols, and different communications interfaces. The preferred protocols for the project were protocols that offer traditional SCADA application features, such as freezing counters, event buffers, unsolicited reporting, and variation for bandwidth control that may be critical as the SAS is scaled. A secondary protocol offers engineering access and event collection and acts as an alternative SCADA protocol. Using more than one SCADA protocol allows LADWP to quickly adjust for a zero-day vulnerability of the primary protocol or shorten outage time during hardware maintenance processes.

Existing microprocessor-based relays were configured to use two serial ports to communicate in DNP3 and a command line protocol. The serial ports were connected to two RTCs, which were dedicated for each protocol to simplify troubleshooting, improve firewall setup, and prevent a single point of failure. The new microprocessor-based relays use dual fiber Ethernet ports to implement a daisy-chain network, connecting to two separate managed switches (see Fig. 3). This provides a ring redundancy configuration.

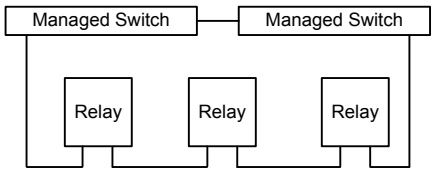

Fig. 3. Ethernet ring redundancy setup

Each RTC is a user access gateway and data concentrator with the following features that complement the enterprise approach to substation automation:

- Web-based HMI that offers easy access for cross-department collaboration and quick data access for sectionalized troubleshooting.
- Windows-based software with a graphical user interface (GUI) that supports multiple protocols and backup SCADA, creation and import of preconfigured templates, extensible markup language (XML) file programming, and mapping and buffering for multiple servers.
- Advanced logic for custom applications and the centralized collection of various alarms, which both assist with NERC CIP compliance efforts.

Because LADWP is an organization with a large number of substations to maintain, its operation and maintenance groups are commonly broken into multiple divisions. Hence, a team effort approach is required to manage substation equipment. An ideal data concentrator needs to be easy to access through a USB or Ethernet connection and authenticate with an LDAP server for centralized management of user role authentication. Network management and substation maintenance tasks can be distributed between two different entities in the organization. As shown in Fig. 4, substation engineering access has primary and backup ports to accommodate on-site serial and Ethernet connections for both older and modern test equipment.

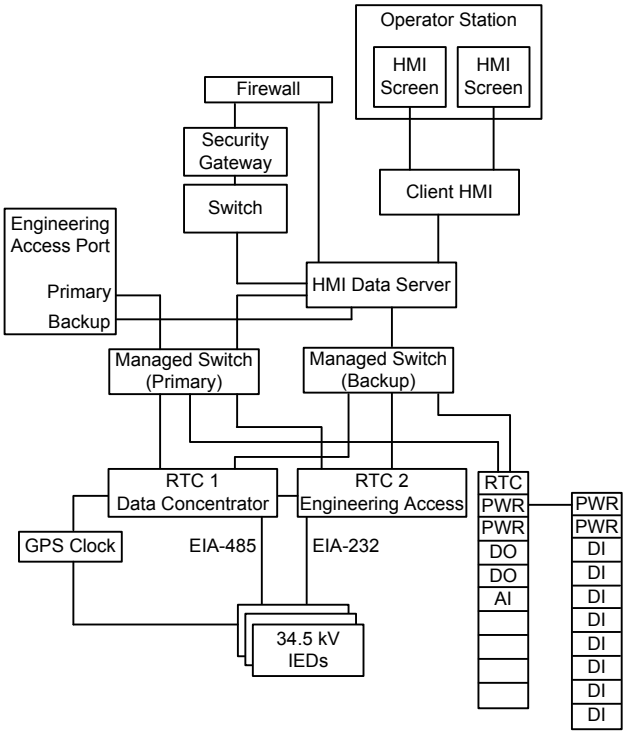

Fig. 4. SAS substation equipment connection diagram

The web-based HMI allows personnel to safely operate and manage all of the substations remotely. Likewise, personnel can remotely access the data concentrator to review aggregated substation events from relays that support fault event oscillography and sequence of events (SOE) archiving and transfers. If the SCADA system is not receiving updates of analog values, troubleshooting personnel can perform preliminary checks to isolate the problem to between the substation and the SCADA master or inside the substation, allowing them to quickly determine the correct dispatch crews to resolve the problem.

In the LADWP SAS project, two RTCs were used. As shown in Fig. 4, one was dedicated as a data concentrator, and the other was for user gateway access and to back up the data concentrator. Settings for each RTC for relay communication can be configured as a template and duplicated quickly for use in the same or different substation projects. Advanced users can export the project file as XML and modify it using a script for quick deployment among other substations. As the number of data servers increase, the data concentrator provides an easy interface to accommodate multiple servers with minimal programming and automatic failover among those servers.

The NERC CIP standard is rapidly changing to address the increasing threats from cyberattacks. The LADWP RTC has IEC 61131 logic to allow customized alarm logging, automatic email notifications, support for automatic failover schemes between primary and backup RTCs, and other advanced applications. The RTCs have the ability to centralize all the alarms from all non-relay equipment, including weather stations, battery charging stations, and various hardware contacts. Substation protection applications, such as direct transfer trip, require operation in milliseconds. The RTCs support EtherCAT protocol and communicate through expandable I/O modules that collect data points and execute controls in milliseconds [1]. Each network cycle, the EtherCAT client (master) sends out a frame, which includes all input and output information. Each I/O module has custom hardware that is configured at network initialization to know which frame locations are associated with its data. Therefore, when the EtherCAT frame arrives at a module, the module does not evaluate the entire frame, but it simply reads and writes needed data elements and forwards the message with almost no delay. As shown in Fig. 4, those expandable modules have redundant power supplies to provide the same reliability as the network.

IV. Device Management

With approximately 200 substations, taking a manual approach to device management is not practical. The security gateway used in the SAS project provides automated password management and proxy access to IEDs connected through the RTC. Initially, the IED hierarchy and existing passwords for the IEDs and RTC were programmed into the relay settings database. The database was imported into the security gateway along with a schedule for complex password changes and LDAP group or personnel access permissions for each IED. Every update cycle, the security gateway generates a series of new complex passwords for each access level of each IED. Through advanced IEC 61131 logic, the RTC receives those passwords and assigns them to the client IEDs. The RTC verifies the communications and provides alarms to dispatch for any unsuccessful password changes.

Fig. 5 shows the scheduled password change flow diagram.

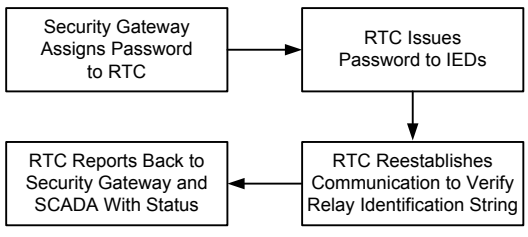

Fig. 5. Password change flow diagram

Users are required to enter their LDAP username and password for access through the security gateway for any IED access, but they are not required to know the IED password. The security gateway enters the complex IED password on

behalf of the user and archives all the changes or keystrokes performed by the user. If the user attempts to change the password of the IED to inhibit the communication to the RTC, the user command will be logged as "blacklist," ejected from the active terminal section, and discarded.

Fig. 6 shows the flow diagram for proxy remote access of IEDs.

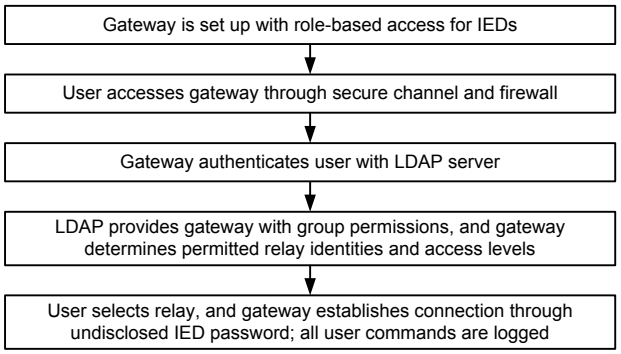

Fig. 6. Proxy remote access flow diagram

V. Continuous Monitoring

Monitoring of the LADWP enterprise system was achieved using a combination of a configuration management system and a log center. These two systems work together to identify changes or events on the SAS that may represent compliance or security issues.

Rules set up in the configuration management system provide a set of integrity checks that compare device configurations against a known baseline. One such check is to search for any changes to local firewalls that do not correspond to the accepted baseline configuration. All ports and services that are required for each server or client machine on the SCADA WAN are defined and included in the integrity checking.

The log center relies on syslog messages originating from server or client machines on the network as well as SAS devices capable of producing syslog messages. For example, the SAS device that manages passwords for the IEDs of each substation will produce syslog messages for information, such as user login to the IEDs. Once the log center receives these messages, it interacts with the configuration management system to apply logic to groups of syslog messages. A group, or sequence, of syslog messages better identifies issues as compared with single isolated messages.

Due to the large volume of messages and events that are integrated with the monitoring systems, dashboards that provide high-level views of the monitored data were implemented. Administrators can drill down as necessary to view issues in need of attention. Separate dashboards for NERC CIP compliance-related issues were created based on NERC CIP rules defined within the configuration management system.

VI. Maintenance and Compliance

NERC CIP-007-R3 compliance requires Windows machines to receive regular updates, per the Microsoft release program, 30 days after patch evaluation. A Windows Server Update Services (WSUS) server was set up within the enterprise system for the purpose of distributing Windows updates to all machines, as shown in Fig. 7 [2] [3]. Groups were defined within the WSUS server so that updates could be applied to certain types of machines at different times. Part of the reasoning for this is that there are different conditions that need to be met for the distribution of updates, depending on the machine type.

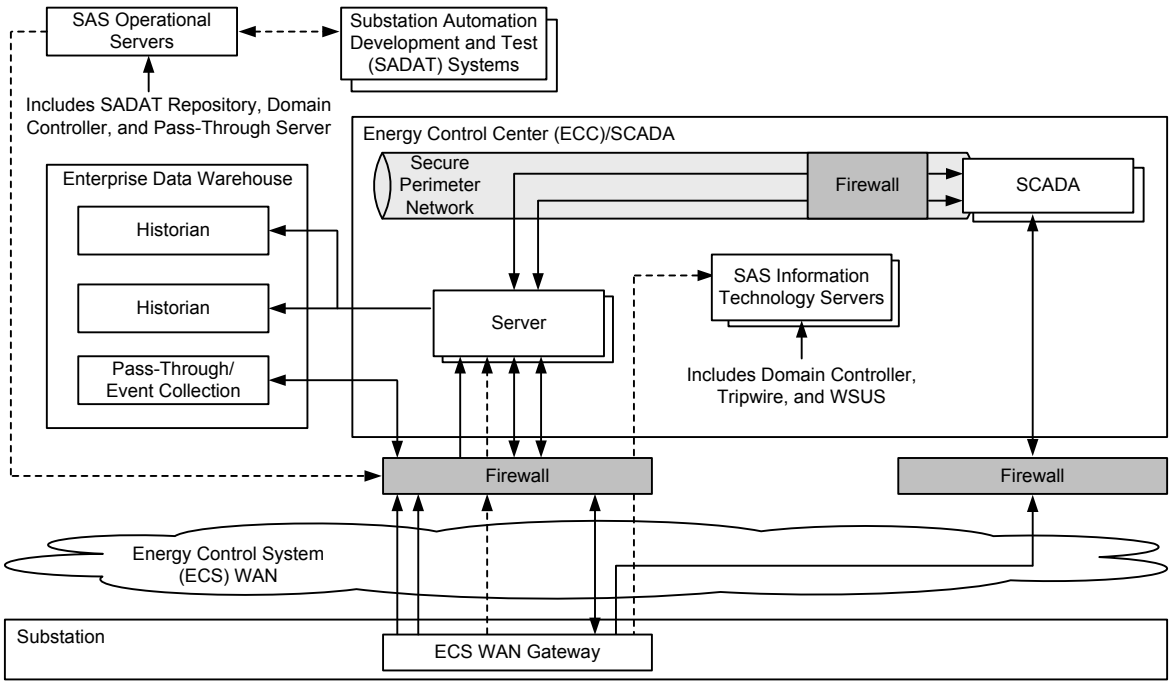

Fig. 7. SAS WAN and enterprise data flow diagram

Before a Windows update is distributed to substation machines, it is tested to make sure that there is no conflict with other software used on the substation client machines.

A substation automation development and test (SADAT) system that included all components of the substation automation system, including IEDs, was provided. The implemented SADAT system is loaded with Windows updates and tested appropriately before the updates are approved by the WSUS for distribution to all machines [3]. This approach provides for a centralized method of keeping Windows machines updated and reduces their vulnerability to known issues.

Antivirus protection is also managed centrally with a server set up specifically for antivirus management. Antivirus patches are tested on the SADAT system prior to approval for distribution to all machines. At LADWP, groups were set up on the antivirus server so that different types of patches could be distributed appropriately.

Maintenance of the HMI software is also managed using a centralized approach. A repository server was set up to hold all HMI configuration data for each substation, with a single common repository for settings that are consistent across all substations. If a common setting is changed, the update can be made in one place (the repository server) and then distributed to all substations. As such, the repository server is defined as the master version of all substation HMI configurations. Changes that are specific to any one substation are also made at the repository server, which is tightly integrated with the SADAT, so that changes can be tested prior to distribution. Once a change is tested and approved, it is then distributed to the substation for operational use. Redundant middleware servers were implemented to help manage this transfer as well as manage data archival, as described in the following section.

VII. Data Visibility

Because a large amount of data is available through the IED event database archiving and security gateway alarm collection, sophisticated event collection software is used to collect all of the event files and execute any scheduled base command line that could archive and reset monthly meter values or reset targets after an event is analyzed. The software used in the SAS project is able to access all of the event files of all IEDs through the equipment database connection and automatically collect event files as operations are generated in the substations. The reports for generated passwords, keystrokes of proxy access, and the managed equipment list that reside in the security gateway are also collected in a timely manner through the WAN.

As mentioned previously, users can also connect to the RTC HMI feature to download the same event files for quick event analysis and shorter outage time. However, the RTC has a limited amount of memory, and it is not designed for long-term event storage. The RTC in the LADWP project can only store 512 oscillography events with a first-in-first-out algorithm to manage the memory space. Hence, automated event collection software plays an important role for long-term data collection, auditing efforts, and power system review operations because a heavyweight disk array system stores all critical data permanently.

Most modern relays offer a synchrophasor phasor measurement unit (PMU) capability built into the relay that can provide three-phase current, three-phase voltage, frequency, and other significant data at 60 samples per second for high-resolution data archiving. LADWP archives PMU data as dynamic disturbance recordings. Event files generated by IEDs and from SOE data are collected through the network architecture for NERC CIP PRC-002-2 compliance without additional hardware or significant cost [4]. LADWP can use the available high-resolution synchrophasor data to monitor power system stability, observe load type to plan future substation growth, or install capacitor banks for improved power quality based on studies of the recorded power quality data. LADWP is planning to capitalize on the synchrophasor feature in the future through real-time power system data monitoring and archiving and a high-speed RTC algorithm to ensure power system stability.

The archiving of substation alarm data is an important feature of the enterprise system. This provides a central location, using a data historian database, where alarms across the network can be viewed and analyzed. It also provides a backup of alarm data in case something happens to the HMI system at the substation.

Substation HMIs periodically sample and collect local time-series and alarm/event data and forward them to a data historian interface on the middleware servers. The data historian interface writes the received data to the corporate data historian and acknowledges the receipt of each successfully written data packet to the sending HMI sampler. The data historian interface takes advantage of the data historian application programming interface (API) built-in buffering feature to avoid the loss of data between the middleware servers and the data historian server.

VIII. Lessons Learned

Through the SAS project, valuable experience was gained for future use. As proven in the completion of upgrades on a handful of substations, the flexibility of Ethernet connections simplifies the upgrade process and maximizes the processing power of the RTC. We were restricted to 33 physical serial connections on each RTC, and additional serial-to-Ethernet port servers were needed for some substations. In the first substation, the substation operators had difficulty with the GUI of the new scheme, which was hindering the user experience. We reviewed the previous LADWP HMI screens and mimicked the operating experience as closely as possible. The standardization of project templates took many hours

prior to the actual substation upgrade. We incorporated the LADWP naming scheme for relays, point lists, I/O labels, and logic implementation to ensure that the script generated an accurate RTC project file for the majority of the substations. This greatly reduced the hours required to modify or customize a project file and shortened the troubleshooting time for LADWP maintenance crews because there is similarity among all of the substations.

IX. Conclusion

As utilities continue to commission more substations, taking a scalable approach to the integration of substation automation systems with enterprise systems can reduce the time required to deploy, learn, and maintain the system. Integrating modern substation automation systems with enterprise-level management enables an organization to gain complete visibility of all of their system assets and physical equipment.

With integrated systems, power grid operators can respond to power outages quicker, envision areas in need of infrastructure expansion, maximize the capacity or applications of their existing substation equipment, and counteract any physical or cybersecurity threat to the power system. Through the analysis of available data and the use of more intelligent power system applications, power generation and power delivery can be made safer and more reliable for the end users and the power provider.

X. References

[1] EtherCAT Technology Group. Available: http://www.ethercat.org/.

[2] NERC Standard CIP-007-5 – Cyber Security – Systems Security Management. Available: http://www.nerc.com/files/CIP-007-5.pdf.

[3] Microsoft, "Windows Server Update Services," *Windows Server*. Available: http://technet.microsoft.com/en-us/windowsserver/bb332157.

[4] NERC Standard PRC-002-NPCC-01 – Disturbance Monitoring. Available: http://www.nerc.com/files/PRC-002-NPCC-01.pdf.

XI. Biographies

Mark Nakao is a SCADA integration and control engineer for the Los Angeles Department of Water and Power (LADWP). Mark received his B.S. in electrical engineering from California State University, Los Angeles, and his M.S. in electrical engineering from the University of Southern California. In addition, Mark received an M.B.A. from the University of Southern California. Mark has worked with remote SCADA equipment for over 28 years, beginning with traditional RTUs and progressing to substation automation systems. Mark provides technical support to utility design engineers on integrating IEDs and DCS systems with LADWP's substation automation system. As a key member of LADWP's Cyber Security team, Mark maintains LADWP's substation automation systems in CIP compliance. Mark has presented technical papers on substation automation at DistribuTECH conferences and at the Southern California Public Power Authority (SCPPA) conference.

Simon Loo is a communications application engineer at Schweitzer Engineering Laboratories, Inc. (SEL). Simon received his B.S. in electrical engineering from the University of Arizona with minors in math and computer engineering. He joined SEL in 2011 as an integration application engineer. Prior to joining SEL, he was with Southwest Transmission Cooperative, Inc. as a field engineer and Freeport McMoran Copper & Gold Inc. as an electrical engineer. He is a member of IEEE and was vice-chair of his IEEE student branch in 2008. Currently, he is pursuing his master's degree in business administration with an emphasis in international business development at the University of California, Irvine.

Lee Melville is an automation engineer at Schweitzer Engineering Laboratories, Inc. (SEL). He has 15 years of experience in the electrical utility industry, working with substation automation and smart grid development. Lee holds a B.E. in electrical engineering and an M.E. in engineering management from the University of Canterbury. He joined SEL in 2012 as an automation engineer. Prior to joining SEL, he was with Black & Veatch as a project engineer and Convergent Group as a system engineer.

Previously presented at the 2015 Texas A&M Conference for Protective Relay Engineers.

20150217 • TP6690-01