How Would We Know?

Edmund O. Schweitzer III, David Whitehead, Allen Risley, and Rhett Smith
Schweitzer Engineering Laboratories, Inc.

This paper was presented at the 64th Annual Conference for Protective Relay Engineers and can be accessed at: http://dx.doi.org/10.1109/CPRE.2011.6035632.

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

Presented at the
64th Annual Conference for Protective Relay Engineers
College Station, Texas
April 11–14, 2011

Originally presented at the
37th Annual Western Protective Relay Conference, October 2010

How Would We Know?

Edmund O. Schweitzer III, David Whitehead, Allen Risley, and Rhett Smith
Schweitzer Engineering Laboratories, Inc.

***Abstract*—Modern power system monitoring, protection, automation, and control rely on communications and computing technology. Along with the benefits of these technologies come some risks of electronic or cyber attack. There are legitimate concerns about how inadequate information security (cyber security) is affecting electric power systems and other critical infrastructure. As a result of cyber security threats, both governments and industry are putting forth significant effort to improve critical infrastructure security. In the United States, for example, electric power utilities must now follow a set of cyber security standards. Security practices are evolving and improving, and new products and architectures are being developed and applied to counter the ever-increasing sophistication of attacker exploits that attempt to access, inspect, manipulate, and control critical infrastructure control systems.**

A fundamental question is "How would we know if our assets are being explored and exploited?" An attack strategy would likely include a number of initial probes, data collection, tests, and other activities as the adversary develops intelligence and capabilities against a target. To counter this strategy, asset owners need to detect the activities of the intruder.

In part, this paper takes the perspective of an engineer investigating a FICTITIOUS incident, using the records and "fingerprints" an attacker would likely leave behind, which we can use to identify when our systems have been compromised. The paper explains how to answer the question using the many tools readily available in devices and systems in service today. These tools include access logs and syslogs, event reports, sequential events reports, information at adjacent stations, alarms, and precision timing. We also investigate some system design choices that make the process of answering the question easier. Finally, we make some recommendations that not only help answer the question "How would we know?" but also make an adversary's job much more difficult.

I. Introduction

When one of the authors was participating in a meeting about cyber security and the electric power industry, a security expert asked, "How would you know if your system was being cyber attacked?" The answer given was based on using the information in digital relays and integration equipment to determine if the system was being explored or attacked.

Our objective in this paper is to carefully answer the question by exploring ways to determine if and when unauthorized communications, probes, settings changes, or control actions are attempted or achieved.

Addressing the question leads to greater security and even automatic real-time reporting of attempted penetrations, as we will demonstrate. We examine the wealth of information that protective relays, automation equipment, PCs, and network equipment capture and maintain. We evaluate how event reports, metering functions, sequential events reports (SERs), and other information can reveal various kinds of attacks. We show how to combine the physical nature of the power system with measurement consistencies to aid in revealing efforts of an attacker to "cover his tracks." Finally, we explain how using these data can identify when an attack attempt is happening, so operators can take action before an attack is successful.

It is, of course, good to know if an attack occurs, but it is even better to avoid being attacked. So, the authors point out many straightforward steps to increase system security using digital equipment already in service.

II. Background

Modern control systems consist of discrete processing elements that communicate to accomplish a specific task. Corporate networks must securely support many different activities, such as email, business system programs, configuration control, and engineering documentation. But, control systems generally perform one or two primary functions, such as power system monitoring and control. Due to the critical functions that control systems perform, great care must be taken to ensure they are not compromised by intentional or unintentional activities.

Further complicating the job of ensuring control system integrity is the mixture of technologies. Today's power control systems consist of both electromechanical and microprocessor-based devices, the latter providing a high degree of automation through communications. Communications technologies within these systems range from 1200 baud modems to OC-48 SONET and gigabit Ethernet, which represent unique and different security challenges.

Security was addressed from the beginning, during the design of the first microprocessor relay. Cyber security began with simple yet strong security features, such as alarm contacts, event reports, lockouts, and complex password access controls. Utilities have also added a layer of security by using SCADA control points to enable modems before allowing engineering access [1].

III. The Incident

To illustrate "How would we know?" consider a fictitious outage on a modern control system architecture from the point of a utility engineer. To remind the reader that this is a fictitious event used to illustrate these concepts, we'll identify the fictitious events with the marker **[F]**.

[F] As the engineer responsible for evaluating unintended power outages, I need to determine why two breakers opened, isolating a transmission line. On that day, the weather was cool and clear, and the lineman reported that there was no known

physical damage to the transmission lines. With no readily apparent reason for this operation, it is my job to determine what caused this unexpected event. I begin the investigation by asking the following questions.

- Are the circuit breakers faulty? *I'll check maintenance records to see if we have noted any problems with them in the past.*
- Did the relays malfunction? *If they did, I should take them out of service and send them back to the vendor to have them checked out. Before I do that I'll make sure to download all the SERs, event records, and settings, just in case I need them later.*
- Was an engineer or maintenance person logged into either relay? Were settings changed or did a user issue commands to the relay? *I'll check the SERs in the relays for any events or settings changes.*
- Did the relay receive a SCADA command to open the breaker? *I will check the SCADA HMI server logs to see if an open command was sent.*
- Is something else going on? Could this be a cyber attack? *If it is, how would I know?*

IV. Reviewing the Control System Connections

[F] The fictitious control system has a protected connection to the corporate network. I asked our information technology (IT) personnel to investigate the corporate side, so I could concentrate on the control network.

[F] My next step was to develop a clear picture of the control system equipment and communications networks. I located and reviewed the control system network and business network diagrams.

[F] Fig. 1 depicts the affected control system components. The system incorporates both serial and TCP/IP wide-area network (WAN) connections that provide SCADA operators, technicians, and engineers with remote access to Intelligent Electronic Devices (IEDs) in Substations 1 and 2. SCADA masters and front-end processors on the control center energy management system (EMS) send information and operator-initiated commands between control system personnel and remote SCADA data concentrators, protective relays, and other IEDs. In addition, engineering communications links allow system engineers to remotely view and modify configuration settings in IEDs or download event reports and SERs for analysis after system events.

[F] Substation 1 is connected to the control center with a serial SCADA link and a serial engineering access link. Substation 2 connects to the control center by a TCP/IP link.

[F] A Synchronous Optical Networking (SONET) infrastructure connects the two substations. This network is used for protection and real-time control. Also connecting Substations 1 and 2 are 900 MHz ISM band radios used in a pilot protection scheme.

[F] Finally, there are several TCP/IP connections between the control center EMS network and Internet-connected support networks.

[F] After reviewing the system topology, I investigated what data sources were available to help my investigation.

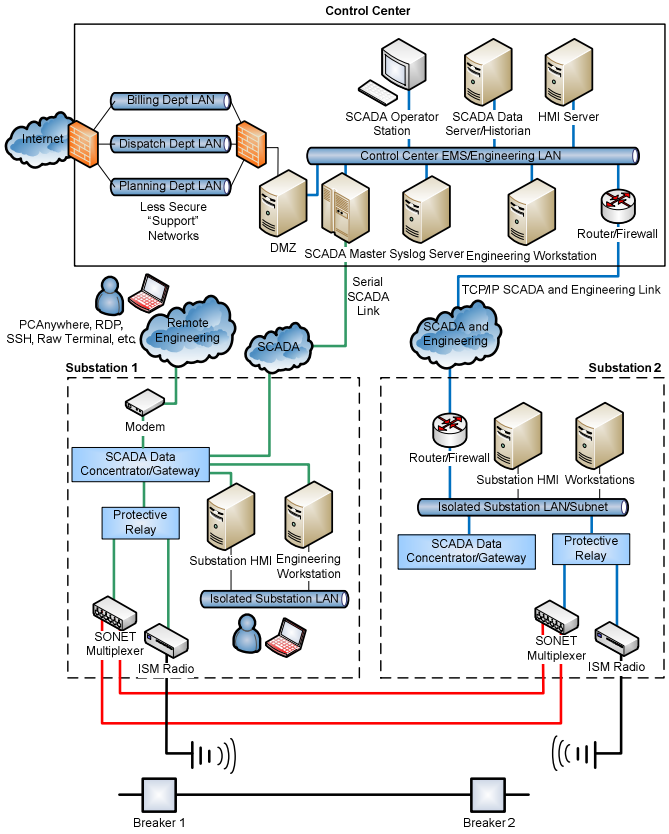

Fig. 1. Control System Network Diagram

V. Information Gathering

Each IED, network appliance, and EMS/SCADA software application collects data that can be used to investigate cyber events.

A. IED Cyber Monitoring

1) Alarm Contacts

Alarm contacts indicate when self-check or security-related events occur. Many IEDs use an alarm contact to indicate unauthorized access. For example, if a password is entered incorrectly or a certain access level is entered, the alarm contact will pulse for one second. When the alarm contacts are connected to a separate monitoring device, such as SCADA, the connection provides an independent communications channel back to SCADA operators. If an intruder is attempting to compromise the serial or Ethernet communications channels, we can use the IED's alarm contact as an independent means to signal other monitoring devices that there is a problem. Thus, while the attacker is attempting to compromise the IED via one communications channel, the IED has signaled a second device, via a second communications channel. This method ensures a successful warning even if the attacker is suppressing alarms coming from the IED via the first communications channel. In Fig. 1, an attack from the engineering access communications to Substation 1, causing the alarm to close, will alert the operators via SCADA's independent communications.

2) Sequential Events Reports

SERs provide a time-stamped record of binary change-of-state events such as trip commands, SCADA commands, and when the IED is powered on or off. Many events are automatically recorded; however, many additional monitoring points may be added to the SER too, with security in mind. Useful points to monitor include breaker status, contact input and output status, and protection and SCADA control points. For example, consider the contact output used to trip a breaker. Under normal operation, the output should only assert via a relay trip condition, SCADA command, or local operation. When the breaker opens, we would expect the SER to include the trip output assertion, and either the trip, SCADA command, or local assertion. Under normal operation, the output should only assert via a trip condition, SCADA command, or local pushbutton operation. When the breaker opens, we would expect the SER to include the output assertion and either the trip, SCADA command, or pushbutton assertion. If the SER does not include two points related to the breaker opening, then this would require further investigation. SERs are stored locally on the IED in a nonvolatile buffer. After the buffer fills, the oldest record is deleted to make room for the newest. Good design practice requires that SERs cannot be written to the relay by a user. Therefore, an attacker cannot insert a false SER to cover his tracks. Although the attacker could clear SERs from memory, this can be monitored and detected.

3) Event Reports

Event reports provide analog and digital measurements, time-stamped to the millisecond. Some event reports also include the IED settings at the time the event report was triggered. Event report lengths can vary from 30 cycles to many seconds. The primary purpose is to show the voltages, currents, and digital points during a fault. However, they can also assist in determining if abnormal power system conditions existed during suspected cyber intrusions. For example, if the relay commanded the circuit breaker to open but there were not any faults on the power system, this would be suspicious enough for more investigation. Like SERs, event reports are stored in nonvolatile memory. When the maximum number of events is reached, the oldest event is deleted to make room for the newest. As with SERs, event reports cannot be written to the relay by a user. Therefore, an attacker cannot insert a false event report to cover his tracks.

4) Metering and Monitoring Functions

Many measurements are available to operators, technicians, and engineers, including fundamental, harmonic, and RMS metering, and breaker-wear monitoring. These measurements can be used to check other measurements within the IED. For example, fundamental and RMS current measurements should be similar, assuming insignificant harmonic content. A large difference indicates either harmonics or that one of the reported values is not correct. An incorrect value can be caused by either an IED error or outside data manipulation between the IED and an observation point.

Breaker-wear monitoring data are stored in nonvolatile memory. These reports include the monitored quantity and the time that the monitored function's change-of-state occurred. We can use these reports to validate other reports. For example, if there is a breaker operation, then there should be an SER and an event report along with a corresponding breaker-wear report. Should the SER and event report be deleted, a time-stamped breaker-wear report would still remain.

5) Communications Channel Reports

Communications channel reports document the health of communications channels. Information includes channel availability, reasons for channel unavailability, and date and length of unavailability. Unexpected communications loss can be a sign of data tapping, data injection, or other malicious activity. Communications channel reports are stored in nonvolatile memory. These reports can be cleared from memory, but the reports include the date and time the report is reset. So, clearing reports generates a new report!

6) Programmable Security Points

Programmable security status points, configured in IEDs, provide an independent communications alarm similar to the standard alarm contact. This feature provides the opportunity to implement a tailored security alarm. For example, by mapping inputs, outputs, and settings group changes to the security points, the security alarm will notify an operator or IED of status changes.

7) Unsolicited SER

Using the processing points, an operator can program the IED to send an unsolicited SER security message based on the change of state of selected processing points. The disadvantage to this system is that since the attacker is using the communications channel, they might be able to suppress the unsolicited SER message. This is overcome when the messages are transmitted out more than one path.

B. Network Appliances

Network appliances within Substations 1 and 2 include Ethernet switches/routers/firewalls, multiplexers, modems, radios, and encryption equipment. All of these collect data that can assist with deciphering electronic events.

1) Network Traffic Monitoring

TCP/IP routers and firewalls, like the ones installed at the network perimeters of Substation 2 and the control center EMS network, can provide a very detailed view of all network traffic received and processed by the device. Logging capabilities include device reboot, configuration changes, and allowed and denied TCP/IP connections. We can use these capabilities to track and monitor network activity. For example, a series of logs detailing dropped connection attempts to blocked service ports can indicate that an attacker has probed the network perimeter, attempting to locate vulnerable services.

2) Communications Alarms

Many network devices produce communications alarms. For example, SONET multiplexers produce an alarm for a loss of the primary communications path, and Ethernet switches and radios signal for a loss-of-link.

C. Computer Operating Systems

SCADA HMI servers, data historians, process data servers, and SCADA masters are often implemented using standard PC hardware and operating systems. PC operating systems include extensive logging capabilities that enable system administrators to monitor system activity, including local logins, program execution, and remote accesses.

D. SCADA and EMS

SCADA and EMS provide an overview of the power system by gathering data from various locations.

1) Logging Capabilities

Power system software packages, including HMI servers, process data historians, and SCADA masters, support detailed logging functionality. This functionality includes operator actions, HMI project modifications, software errors, user logins, and database access.

2) Alarm Reporting

EMS software packages allow you to map security-related system state changes to event triggers. These triggers notify operators of suspicious activity in real time. For example, changes in security-related status points, such as engineering access connection attempts, IED settings change events, or device failures can notify operators via the HMI or an alarm panel.

3) Measurement Consistency

SCADA and EMS monitor and record the power system status across a network, allowing them to observe and detect inconsistent measurements between connected substations. For example, Substations 1 and 2, which are connected by a transmission line, should have some similar measurements. Inconsistencies in any of these measurements provide clues for diagnosing potential data manipulation. The following are a few consistency checks.

- Voltage magnitudes and angles should be similar. Synchrophasor technology in substation IEDs can easily measure this.
- Current measured at the ends of relatively short lines should be about equal.
- Breaker states should be consistent with power flow measurements.
- Each substation should have net power and current flows that are near zero, i.e., the amount of power and current entering the substation should equal the power leaving the substation.
- State estimator programs automatically check for data consistency and can detect disagreement between breaker status and current flow.
- New devices, such as the Synchronous Vector Processor, can automatically check data for consistency within the substation.
- When adjacent station communications are available, such as the SONET network shown in Fig. 1, station-to-station checks are easily made and are independent of the SCADA master communications.

4) Communications Monitoring

The SCADA and EMS software packages also monitor communications statistics, such as the response times from the IEDs. These systems tolerate communications channel problems, such as dropped packets and missed polls; however, excessive missed polls, prolonged communications outages, or nonrandom missed polls (e.g., IED 1 misses polls for one minute, then IED 2 misses polls for one minute, then IED 3, etc.) may indicate communications channel tampering.

E. Central Log Consolidation in Syslog Servers

Syslog is a protocol that allows a device to send event notification messages across IP networks to event message collectors known as syslog servers. Most network appliances support the syslog protocol, which allows system administrators to collect and review network activity logs from a central location. Log entries detailing network activity are sent to a centrally located syslog server where they can be conveniently analyzed by network security personnel.

VI. Potential Points of Exploit

Identifying possible points of exploitation is important to maintaining a secure power system. The U.S. Department of Homeland Security Control Systems Security Program website contains many resources to assist with identifying system vulnerabilities [2]. The appendix to this paper contains additional sources of information.

The red arrows in Fig. 2 show potential remote electronic attack entry points in our fictitious system. The letters correspond with the attack types described in this section.

A. External Network Access

An attacker may have gained entry to the EMS network through indirect connections to less secure "support" networks. These connections are becoming more common as networking technologies make it easier to provide almost real-time access to system status data collected by the critical EMS infrastructure. Oftentimes, these support networks are also connected to the Internet, creating an indirect bridge between attackers on the Internet and critical control system assets. Similarly, an attacker may use an unsecure SCADA or engineering WAN connection to mount an electronic attack against assets in the connected substation. Dial-up modems, unsecured wireless links, or physically accessible communications cabinets—all may provide an attacker an exploitable attack avenue.

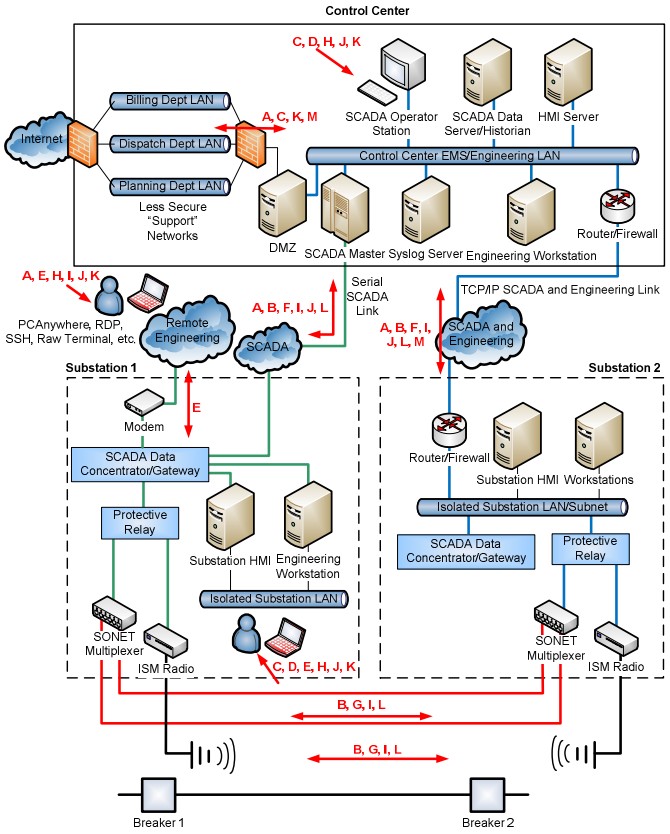

Fig. 2. Potential Remote Electronic Attack Entry Points

B. Man-in-the-Middle

Man-in-the-middle attacks consist of intercepting or subverting communications to a client. For example, an attacker could have accessed the SCADA system and sent an "open" command to one of the protective relays to open a circuit breaker. Similarly, an attacker could generate a false breaker status and send that message to the SCADA system. An attacker could also modify replies to the HMI, presenting the operator with false system status.

C. Malware

Malware is software that is designed to infiltrate a computer system without the owner's informed consent. An attacker who has gained access to a network at any point can install malware in the form of viruses, worms, and Trojans. Malware is installed through unsecure communications services or removable media. Once malware infects a control system, it can cause the system to stop operating, allow nonauthorized users access, and send information to nonauthorized users.

D. USB Stick Access [3]

USB memory sticks are frequently used for software upgrades, manual retrieval of data, etc. They are one of the most dangerous network access devices because popular operating systems do not perform security checks until after the malicious code has infected the host system. They are very effective in transporting malware, for example.

E. Engineering Communications Access

Access ports, used to monitor and configure devices, are also targeted points of entry. These communications ports are not in continuous service but are only used on an as-needed basis. As a result, they may not be monitored. Exploitation of these communications links could result in breaker misoperation, settings changes, clearing of logs, etc.

F. SCADA Communications Access

SCADA communications channels are used to monitor and control power system equipment. Tampering with these communications links could result in breaker misoperation, false data reported to the SCADA system, and loss of communications.

G. Real-Time Control Communications Access

Real-time communications links are used for power system control, e.g., SONET multiplexers and ISM radios are used for line-current differential and pilot wire protection. Subversions of these communications links could result in breaker misoperation.

H. Insider or Direct Access

During an insider or direct attack, authorized personnel deliberately manipulate power system devices to produce an unauthorized condition, e.g., open a circuit breaker or load malware onto an IED. This is one of the most difficult attacks to prevent because the attacker is a trusted user.

I. Denial of Service

Denial of service (DoS) attacks block legitimate information from reaching the intended recipient. Examples of DoS attacks include radio jamming and high IP network traffic.

J. Malicious Data Injection

Malicious data injection consists of attacks such as buffer overflow exploits. These attacks result in memory being corrupted. The corruption could cause the device to shut down or, if the attack is sophisticated, load and execute an authorized program.

K. Software Upgrade Exploits

These exploits consist of loading unauthorized code into a device or modifying the upgrade process in such a way as to stop the device from functioning. In the case of the unauthorized code scenario, an attacker modifies IED firmware in such a way as to cause undesired operations or to allow unauthorized user access.

L. Data Playback

During a data playback attack, the attacker records communications channel data and retransmits at a later time. For example, SCADA metering data may be recorded under nominal conditions. An adversary will then send the recorded information to the SCADA EMS in an attempt to hide their actions.

M. Database Manipulation

IED database services, like process data historians, communications processors, or HMI servers, may also be vulnerable to unauthorized access. If an attacker gained access, they could manipulate the data to perform malicious actions on the control system.

VII. Reviewing the Fictitious Incident Data

[F] Many devices within our power system measure and record information that I can use to determine if the system is being probed or attacked. Combining the information from multiple devices provides a means to validate and cross-check data across the power system.

[F] Syslog is a feature found in modern TCP/IP-based equipment that forwards event data to a central storage device. This capability is important because most IEDs that generate logs store them locally in a finite-sized circular buffer (e.g., nonvolatile memory or hard drive file). When the buffer gets full, the IED deletes the older log entries to make room for new entries. An attacker can flood the target device with network traffic to generate useless events in the log buffer, eventually causing the uninformative log entries to overwrite the entries of interest in the circular buffer. I can verify information stored in local IED circular buffers using data from IEDs that support the syslog remote log concentration service. Rather than storing the log entries locally, our syslog-enabled IEDs transmit all logs to the centralized syslog server in the control center via TCP/IP network links.

[F] I sent a technician to gather data at three locations: the control center, Substation 1, and Substation 2. At the control center, the technician queried the syslog server to retrieve logs generated by syslog-enabled PCs and IEDs that may have observed suspicious system activity. In order to get a view of any pre-attack probing activity, we gathered logs from the seven days before, and including the day of, the incident. The syslog queries included logs from the firewalls and routers in the control center and at the perimeter of Substation 2. We also included logs from all servers and user workstations in the control center and Substation 2, so we could analyze user and software application activity on the network. We were also able to retrieve logs from the syslog-enabled SCADA data concentrator in Substation 2.

[F] In addition to the syslog entries described above, the technician manually extracted all available information from nonsyslog-enabled IEDs and PCs in the three locations of interest. This included application-specific logs and alarms from the HMI server, SCADA master, process data server/historian, and the SCADA operator workstations in order to detect any suspicious manipulation of the control center EMS infrastructure. The technician also gathered all SERs, event records, and IED self-check reports from the protective relays at Substations 1 and 2.

[F] Substation 1 is not TCP/IP-connected, so logs cannot be sent to the syslog server on the control center LAN. Because of this, the technician manually collected log entries from the engineering workstation, substation HMI, and SCADA concentrator in Substation 1 in order to detect any suspicious activity on this isolated network segment. After reviewing this information, I took another look at my original questions.

A. Are either of the circuit breakers faulty?

[F] The technician had investigated the circuit breakers to see if there was a malfunction. Maintenance records for the breakers indicated no apparent problems and verified that they were within normal operating parameters.

B. Did the relays malfunction?

[F] Both of the relays that control the two affected breakers (labeled Breaker 1 and Breaker 2 in Fig. 1) were enabled and operational. I had the technician check the internal self-check reports for both relays, and all measurements were within normal operating parameters.

[F] The technician reported that at Substation 1, Relay 1, which controls Breaker 1, was enabled, and the TRIP LED was lit, indicating that a protective trip had occurred.

[F] In Substation 2, Relay 2, which controls Breaker 2, was enabled, but no target LEDs were lit, indicating that the trip was not caused by a protective element pickup.

Both relays for Breakers 1 and 2 appeared to be functioning normally.

C. Was an engineer or maintenance person logged into either relay? Were settings changed or did a user issue commands to the relay?

1) Substation 1 Logs

[F] I examined the SERs and event reports from Relay 1 at the time of the trip and found no SERs. This is suspicious because normal substation and power system activities generate SERs. There should have been some SERs. I asked the technician if he had cleared the SERs, but he had not. The lack of SERs could be the result of someone erasing the logs to cover their tracks. Attackers will do this to hide the methods they use to gain access. There was, however, an event record in the relay that corresponded to the trip event. The measurement data in the event report showed normal system conditions and no discernable evidence of a fault on the transmission line.

[F] The Relay 1 TRIP LED indicates that the breaker tripped due to a protection element asserting. I compared the settings shown in the relay with the approved settings for the relay and found that the overcurrent element setting was lowered from 15 amperes to 3 amperes, which caused the relay to trip on load current. But who changed this and why?

[F] From the SERs saved in the local Substation 1 engineering workstation, I identified an event generated by assertion of the Relay 1 alarm contact, indicating a successful login using the proper username and password. Another alarm contact assertion event occurred just before Breaker 1 tripped. There were no other alarm contact assertions in the one-week time frame that we analyzed. Because of this, the second alarm contact assertion must also correspond to the change of overcurrent protection settings. This suggests that the Relay 1 settings change caused the relay to trip the breaker.

[F] From log entries manually gathered from the SCADA data concentrator/gateway at the perimeter of Substation 1, I

also identified a successful user login shortly before the incident. An operator's credentials were used to remotely access the gateway and log into Relay 1.

2) Substation 2 Logs

[F] Next, I reviewed the activity of the alarm contact bit from Relay 2 in the archived power system status and measurements contained in the process data historian in the control center. The trend graph showed a large number of state changes over the two days prior to the incident. This could indicate multiple failed login attempts.

[F] In addition, router and firewall logs at the control center and Substation 2 perimeters recorded several engineering access sessions between an engineering workstation in the control center and Relay 2. This activity indicates that the engineering workstation may have been the source of the failed login attempts indicated by the alarm bit state transitions recorded in the SCADA log.

[F] Checking the Relay 2 SER logs, I noted that a SCADA control message had been received by the relay, causing Breaker 2 to open.

3) Control Center Logs

[F] The syslog events generated by workstations on the control center EMS and engineering LAN indicated that the same operator, who had remotely logged into the SCADA data concentrator in Substation 1, was also logged into an engineering workstation in the control center at the time of the incident.

D. Did the relay receive a SCADA command to open the breaker?

[F] The syslog entries from the routers and firewalls between the control center and Substation 2 contained evidence of abnormal SCADA protocol sessions between Relay 2 and the same engineering workstation that was the source of the engineering activity mentioned above. Any SCADA protocol activity initiated from any device other than the SCADA master is highly suspicious. A session was active at the time of the event, indicating that the engineering workstation may have been the source of the commanded trip received by Relay 2.

E. Could this be a cyber attack?

[F] I identified warning signs indicating unauthorized electronic system access: multiple failed login attempts on Relay 2, SCADA sessions initiated from an engineering workstation, and an unauthorized settings change in Relay 1.

[F] Further investigation revealed additional evidence that allowed me to piece together how the attack occurred. Examining the logs of the control center LAN's firewalls, routers, and HMI server showed large data transfers from the HMI server to the control center engineering workstation on at least four occasions over the past few months. The tag names and HMI project files that were downloaded from the HMI server contained all the information needed to piece together a power system one-line diagram and the communications addresses of targetable breakers. All of these attack indications make it clear that a deliberate electronic attack was initiated from the engineering workstation. Now, I have to determine how someone gained access to this workstation and eventually to the substation IEDs that allowed the unauthorized breaker operations.

[F] The corporate IT staff identified evidence of multiple intrusions into the corporate network from the Internet, including a compromised Internet-facing web server. Our IT staff also identified additional compromised machines on the corporate network that proxied attack traffic between the corporate network and the connected control center EMS LAN. We reported the incident to the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) that assists critical asset owners with the analysis of control system-related incidents, and they responded by sending an Incident Response Team in two days to help with the investigation.

[F] A detailed forensic analysis of the engineering workstation revealed that malware had allowed the attacker to access the workstation from the corporate network. The attack traffic was disguised as a database access service that was allowed through the firewall that separates the corporate network and the EMS network. In addition, the engineering workstation also provided access to Relay 1. In a deleted email folder was a recent email from another operator in which they exchanged the username and password of Relay 1. This email enabled the attacker to successfully access Relay 1 and change the overcurrent settings that caused Breaker 1 to trip.

[F] In summary, multiple vulnerabilities allowed an external attacker to change settings in a relay and inject SCADA control commands, which resulted in the isolation of a transmission line.

VIII. Improved Intrusion Detection

In the previous sections, we described a fictitious scenario in which an electric power system engineer performed a forensic analysis of system activity after a suspicious event. The best incident response is a well known and practiced plan that is supported with a good alert and logging infrastructure. The faster the operators identify an intrusion attempt, the better the chance of swift containment and recovery. We have outlined many IED logging capabilities that are common in electric power system networks. These network activity logs are a valuable tool for detecting suspicious activity before an intruder has a chance to perform damaging actions. Most electronic attacks are preceded by detectable network reconnaissance activity. A way to identify when reconnaissance happens is to know the normal traffic patterns on the system. Normal network traffic patterns include data frames associated with SCADA service connections between a control center EMS infrastructure or periodic engineering access connections between authorized remote users and substation IEDs. Once this normal traffic pattern is understood, deviations are easier to identify. The following are signs of malicious reconnaissance traffic associated with attack activities.

- TCP/IP scans to identify available services and accessible routes through perimeter defenses.

- Unauthorized database queries to a control center EMS SCADA data historian/server or HMI server to analyze system architecture and find accessible breakers in order to map the system.
- Scripted login attempts designed to guess authentication passwords that protect remote engineering access services.
- Unauthorized, outgoing TCP/IP connection attempts initiated from a workstation. This is a sign that attackers have compromised a PC that is attempting to "call home."

In order to detect these attack precursors, network designers connect critical network segments with routers and firewalls to filter and provide activity logs. It is important to ensure that these critical devices are configured to provide optimal logging capabilities. Routers and firewalls should be configured to create time-stamped log entries every time a TCP/IP connection is routed through the device or is denied by the device's configured access control list (ACL) rules. These log entries identify suspicious traffic patterns. For example, a series of logs detailing dropped connection attempts to blocked service ports can indicate that an attacker has probed the network perimeter in an attempt to locate accessible services. As another example, a security administrator who has detected a highly suspicious configuration change in a critical protective relay can trace the allowed engineering access connection through intermediate routers to locate the source of the connection.

Similarly, serial network connections can be monitored by extracting log entries from the devices receiving the serial traffic. Many dial-up modems have onboard event logs that document the time of each incoming or outgoing connection. Modem connection logs can be used to detect suspicious activity, like repeated unauthorized, after-hours connections to critical dial-up engineering access ports. IEDs to which the serial connection is being made will also contain important log entries documenting activities conducted during the serial connection.

The communications diagnostics we have in place for SCADA are powerful tools to identify cyber attacks. Missed polls could be a sign that someone was using the channel for malicious behavior, such as performing a man-in-the-middle attack, denial-of-service attack, or an exploited engineering access connection.

Many malware or program installations need a reboot to complete the installation process. Any reboot of a device used in a control system is a problem. Determining root cause of the reboots is important to ensure the reboot was not caused by a malware, data injection, or software upgrade attack.

In many cases, an attacker will gain access to a device and then patch the system in order to keep other attackers out. If the computer is updated to the latest release or has the latest security updates enabled and you did not authorize these updates, this is a clear sign of malicious activity [4], [5].

Latency changes in the network may indicate an electronic attack. If latency increases, attackers could be using the communications bandwidth for malicious purposes. As we discussed earlier, knowing your normal traffic patterns and loads is key to identifying when this is taking place. Traffic load spikes are a clear indication that you either have a device malfunction or an attack in progress.

Ethernet networks provide information on all the communications paths established. These logs detail source and destination for each conversation. In many cases, the firewalls at the critical segmentation points show the allowed and dropped traffic. Dropped traffic is important to note because it shows the methods a potential attacker is using to gain network access. By studying these logs, you can determine if you need additional countermeasures or new firewall rules. Switches fill in the rest of the network picture with valuable insight into what is happening with peer-to-peer communications and changes in traffic patterns. Switches show when new hosts join and leave the network. This combined information assists in identification of malicious behavior and spotlights any unauthorized external network access, denial-of-service attack, unauthorized insider activity, or malware infection.

IX. Prevention

Combining security features of IEDs, network appliances, and software using a layered approach provides a very robust cyber security solution. The following list provides tools that, when implemented, create a robust solution to detect and deter cyber attacks.

A. Build on the Security Tools and Information in Your IEDs [6], [7]

- Connect alarm contacts to other system equipment to create a secondary notification channel.
- Use all available time-stamped reports to correlate system events.
- Create a custom alarm point that includes inputs, outputs, communications channel failures, and settings group changes.
- Map the custom alarm output to SCADA.
- Use a spare contact output, and map the custom alarm output to a SCADA gateway or RTU to create a secondary communications path.

B. Analyze Redundant and Related Power System Measurements

- State estimators purge "bad data;" the purge can tip off an attack.
- Synchrophasors and vector processing, at the substation and over wide areas, can also uncover "bad data." For example, consider using the voltages and currents at one substation to determine the voltage at the next substation, and compare the voltage measured with the calculated one. Disagreement could be measurement or sensor problems, or a cyber attack.
- Even simple metering checks are useful, especially on shorter lines. The current and power measured on "my" end should be close to those on "your" end when the breakers are closed.

C. Implement Best IT Cyber Security Practices [8], [9], [10], [11]

- Use bump-in-the-wire cryptography to protect serial connections and VPNs to protect Ethernet connections [12], as was done in the Department of Energy Lemnos and Hallmark projects [13], [14].
- Architect networks with clear segments connected by firewalls, and filter both incoming and outgoing communications [15].
- Isolate critical control system networks from less regulated networks, using demilitarized zones (DMZs) [16].
- Use static network routes to guarantee fixed communications paths.
- Program router logs to capture undesired traffic patterns.
- Configure an IDS to log unauthorized traffic patterns and respond when logs are received [17].
- Implement a patch management system that includes how vendors will communicate patch releases.
- Develop an antivirus strategy tailored to your system configuration making sure to understand the implications and any potential adverse effects.
- Establish a test bed to verify patches and antivirus before deployment.
- Baseline your IED settings to document system configuration. Then routinely compare the baseline with the current device states, and investigate and correct any unauthorized changes discovered.

D. Examine Logs for Abnormal or Suspicious Activity

- Set logs to automatically elevate critical events for immediate attention.
- Program IEDs to alarm when settings or firmware are changed.
- Archive logs for post investigation.

E. Develop an Incident Response Plan

Use an incident response plan to repair and restore any potential damage caused as a result of a cyber attack. Guidance documents for developing an incident response plan are listed in Section D of the appendix.

F. Create Security Awareness and Audit Programs

- Provide regular training to employees, and add simple security reminders throughout the work place. Ideas include computer login banners or posters similar to the WWII slogan, "Lose Lips Sink Ships."
- Notify employees immediately of discovered threats along with appropriate mitigations.
- Conduct regular security audits to verify that security rules are being followed.

X. Conclusion

Every cyber security intrusion or attack will leave fingerprints. Using the existing features in IEDs, network equipment, and EMS/SCADA monitoring systems is an effective way to detect and deter cyber intrusions.

We have examined the wealth of information that protective relays, automation equipment, PCs, and network equipment capture and maintain. We have evaluated how event reports, metering functions, SERs, and other information can reveal intrusions. We have shown how to combine the physical nature of the power system with consistency checks to aid in revealing efforts of an attacker to "cover his tracks." And, we have explained how using the various features within the monitoring and control system can identify when an attack attempt is happening, so operators can take action before an attack is successful.

We have included a cyber security-related reference section in the appendix as an additional resource.

Implementing the concepts shown in this paper is not difficult, does not require extensive capital [18], and answers the question "How would we know?"

XI. Appendix – Resources to Implement Computer Security

A. WARNING NOTICE

Do not attempt to implement any of the settings presented here without first testing them in a nonoperational environment.

Many of these documents are only guides containing recommended security settings; they are not meant to replace well-structured policy or sound judgment. Furthermore, these guides do not address site-specific configuration issues. Care must be taken when implementing these guides to address local operational and policy concerns.

SEL assumes no responsibility whatsoever for its use by other parties and makes no guarantees, expressed or implied, about its quality, reliability, or any other characteristic.

This is not a comprehensive list, but it highlights a few of the many resources on computer security.

B. General IT Security – Broad Range of Security Subjects

- National Security Agency Security Configuration Guides (covers operating systems, database servers, routers, switches, web servers, and wireless access): http://www.nsa.gov/ia/guidance/security_configuration_guides/index.shtml
- NIST Special Publication 800-68 "Guide to Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist": http://csrc.nist.gov/itsec/SP800-68r1.pdf
- Microsoft Windows XP Security Baseline: http://technet.microsoft.com/en-us/library/cc163061.aspx

- Microsoft Windows XP Professional Product Documentation – Predefined Security Templates: http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sag_scedefaultpols.mspx?mfr=true
- Microsoft Windows Server 2003 Security Baseline: http://technet.microsoft.com/en-us/library/cc163140.aspx
- Microsoft Windows Vista Security Guide: http://technet.microsoft.com/en-us/library/cc507874.aspx
- Various **nix* Security Guidelines: http://www.auscert.org.au/5816 http://www.redhat.com/solutions/security/ http://www.redhat.com/apps/support/errata/ http://www.debian.org/security/ http://www.slackware.com/security/ http://www.suse.com/us/private/support/security/
- Apple Mac OS X Security Configuration Guides: http://www.apple.com/support/security/guides/
- NIST Special Publication 800-123 "Guide to General Server Security": http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf
- NIST Special Publication 800-44 "Guidelines on Securing Public Web Servers": http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf
- "Preventing Incidents With a Hardened Web Browser": http://www.sans.org/reading_room/whitepapers/bestprac/preventing-incidents-hardened-web-browser_33244
- NIST Special Publication 800-46 "Guide to Enterprise Telework and Remote Access Security": http://csrc.nist.gov/publications/nistpubs/800-46-rev1/sp800-46r1.pdf
- NIST Special Publication 800-97 "Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i": http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf
- NIST Special Publication 800-48 "Guide to Securing Legacy IEEE 802.11 Wireless Networks": http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf

C. Control System Security

- Improving Industrial Control Systems Cyber Security With Defense-In-Depth Strategies: http://www.us-cert.gov/control_systems/csdocuments.html
- U.S. Department of Energy "21 Steps to Improve Cyber Security of SCADA Networks": http://www.oe.energy.gov/DocumentsandMedia/21_Steps_-_SCADA.pdf
- "Engineering Defense-in-Depth Cybersecurity for the Modern Substation": http://www.selmeters.org/WorkArea/DownloadAsset.aspx?id=7402
- "Cybersecurity as Part of Modern Substations": http://www.selmeters.org/WorkArea/DownloadAsset.aspx?id=3530
- "NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks": http://www.cpni.gov.uk/docs/re-20050223-00157.pdf
- "Implementing Firewalls for Modern Substation Cybersecurity": http://www.selmeters.org/WorkArea/DownloadAsset.aspx?id=7386
- "Implementing SCADA Security Policies Via Security-Enhanced Linux": https://www.selinc.com/WorkArea/DownloadAsset.aspx?id=3531
- "Low- or No-Cost Cybersecurity Solutions for Defending the Electric Power System Against Electronic Intrusions": http://www.selmeters.org/WorkArea/DownloadAsset.aspx?id=3182
- Bandolier: http://www.digitalbond.com/index.php/research/bandolier/
- U.S. Department of Homeland Security "Cyber Security Procurement Language for Control Systems": http://www.us-cert.gov/control_systems/pdf/FINAL-Procurement_Language_Rev4_100809.pdf

D. Maintenance – Security Concerns During the Maintenance Phase of the Life Cycle

- Recommended Practice for Patch Management of Control Systems: http://www.us-cert.gov/control_systems/csdocuments.html
- NIST Special Publication 800-40 "Creating a Patch and Vulnerability Management Program": http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf
- Securing the Microsoft Desktop Environment Using Patch Management: http://www.microsoft.com/downloads/details.aspx?FamilyID=1b93a1cd-06cd-42b9-a077-75663133832d&displayLang=en

E. Incident Response – How to Detect, Respond to, and Limit Consequences of a Cyber Intrusion

- NIST Special Publication 800-86 "Guide to Integrating Forensic Techniques Into Incident Response": http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf
- Developing an Industrial Control Systems Cyber Security Incident Response Capability: http://www.us-cert.gov/control_systems/csdocuments.html
- U.S. Department of Homeland Security "Incident Handling: Preparing for Incident Analysis": http://www.us-cert.gov/control_systems/pdf/Incident Handling Brochure-1.pdf
- Creating Cyber Forensics Plans for Control Systems: http://www.uscert.gov/control_systems/csdocuments.html
- NIST Special Publication 800-94 "Guide to Intrusion Detection and Prevention Systems (IDPS)": http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf
- NIST Special Publication 800-61 "Computer Security Incident Handling Guide": http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

- Computer Forensics, Cybercrime and Steganography Resources: http://www.forensics.nl/links/
- NIST Special Publication 800-83 "Guide to Malware Incident Prevention and Handling": http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf
- Forensics Information From CERT: http://www.cert.org/forensics/
- Computer Forensics World: http://www.computerforensicsworld.com/index.php
- Cornell University Law School – Federal Rules of Evidence: http://www.law.cornell.edu/rules/fre/overview.html

F. Security for Managers – Explaining the Security Threat to Your Management

- "Information Security Governance to Enhance Corporate Value": http://www.sans.org/security-resources/information-security-governance.pdf
- US-CERT Control Systems Security Center "Backdoors and Holes in Network Perimeters: A Case Study for Improving Your Control System Security": http://www.us-cert.gov/control_systems/pdf/backdoor0503.pdf
- US-CERT Control Systems Security Center "An Undirected Attack Against Critical Infrastructure: A Case Study for Improving Your Control System Security": http://www.us-cert.gov/control_systems/pdf/undirected_attack0905.pdf
- "Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia": http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf
- Attack Methodology Analysis: SQL Injection Attacks: http://www.us-cert.gov/control_systems/practices/documents/SQL Abstract.pdf
- Internet Storm Center: http://isc.sans.edu/index.html
- CWE/SANS Top 25 Most Dangerous Software Errors: http://www.sans.org/top25-software-errors/
- "Battle for the Internet: The War Is On!": http://www.sans.org/reading_room/whitepapers/testing/battle-internet-war-on_1075
- Numerous other computer security publications at the NIST Computer Security Resource Center: http://csrc.nist.gov/publications/PubsTC.html
- Searching the SANS Information Security Reading Room could provide papers addressing your specific needs: http://www.sans.org/reading_room/

XII. REFERENCES

[1] C. Ewing, "Engineering Defense-in-Depth Cybersecurity for the Modern Substation," proceedings of the 12th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2010.

[2] U.S. Department of Homeland Security Control Systems Security Program. Available: http://www.us-cert.gov/control_systems/csvuls.html.

[3] Industrial Control Systems Cyber Emergency Response Team, "ICS-CERT – Control Systems Analysis Report: USB Drives Commonly Used as an Attack Vector Against Critical Infrastructure," April 2010. Available: http://www.us-cert.gov/control_systems/pdf/ICS-CERT CSAR-USB USAGE.pdf.

[4] R. Bradetich and P. Oman, "Implementing SCADA Security Policies Via Security-Enhanced Linux," proceedings of the 10th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2008.

[5] D. Anderson, "Securing Modern Substations With an Open Standard Network Security Solution," proceedings of the 11th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2009.

[6] P. W. Oman, J. Roberts, and E. O. Schweitzer, III, "Tools for Protecting Electric Power Systems From Electronic Intrusions," proceedings of the 4th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2002.

[7] P. W. Oman, A. D. Risley, J. Roberts, and E. O. Schweitzer, III, "Attack and Defend Tools for Remotely Accessible Control and Protection Equipment in Electric Power Systems," proceedings of the 55th Annual Conference for Protective Relay Engineers, College Station, TX, April 2002.

[8] S. Hurd, R. Smith, and G. Leischner, "Tutorial: Security in Electric Utility Control Systems," proceedings of the 34th Annual Western Protective Relay Conference, Spokane, WA, October 2007.

[9] D. Anderson and G. Leischner, "Cybersecurity as Part of Modern Substations," proceedings of the 7th Annual Power Systems Conference, Clemson, SC, March 2008.

[10] A. Risley, J. Roberts, and P. LaDow, "Electronic Security of Real-Time Protection and SCADA Communications," proceedings of the 5th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2003.

[11] T. Tibbals and D. Dolezilek, "Communications Technologies and Practices to Satisfy NERC Critical Infrastructure Protection (CIP)," proceedings of the 5th Annual Power Systems Conference, Clemson, SC, March 2006.

[12] G. Leischner and C. Tews, "Security Through VLAN Segmentation: Isolating and Securing Critical Assets Without Loss of Usability," proceedings of the 9th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2007.

[13] U.S. Department of Energy, "Lemnos Interoperable Security." Available: http://www.oe.energy.gov/DocumentsandMedia/Lemnos_Interoperable_Security.pdf.

[14] U.S. Department of Energy, "Hallmark Cryptographic Serial Communication." Available: http://www.oe.energy.gov/Documentsand Media/Hallmark_Cryptographic_Serial_Communication.pdf.

[15] D. Anderson and N. Kipp, "Implementing Firewalls for Modern Substation Cybersecurity," proceedings of the 12th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2010.

[16] R. Bradetich and P. Oman, "Connecting SCADA Systems to Corporate IT Networks Using Security-Enhanced Linux," proceedings of the 34th Annual Western Protective Relay Conference, Spokane, WA, October 2007.

[17] U.S. Department of Homeland Security and Idaho National Laboratory, "Control Systems Cyber Security: Defense in Depth Strategies," May 2006. Available: http://www.us-cert.gov/control_systems/practices/documents/Defense in Depth Strategies.pdf.

[18] A. Risley and K. Carson, "Low- or No-Cost Cybersecurity Solutions for Defending the Electric Power System Against Electronic Intrusions." Available: http://www.selinc.com.

XIII. BIOGRAPHIES

Dr. Edmund O. Schweitzer, III is recognized as a pioneer in digital protection and holds the grade of Fellow of the IEEE, a title bestowed on less than one percent of IEEE members. In 2002, he was elected a member of the National Academy of Engineering. He is the recipient of the Graduate Alumni Achievement Award from Washington State University and the Purdue University Outstanding Electrical and Computer Engineer Award. In September 2005, he was awarded an honorary doctorate from Universidad Autónoma de Nuevo León in Monterrey, Mexico, for his contribution to the development of electric power systems worldwide. He has written dozens of technical papers in the areas of digital relay design and reliability and holds more than 30 patents pertaining to electric power system protection, metering, monitoring, and control. Dr. Schweitzer received his Bachelor's and Master's degrees in electrical engineering from Purdue University, and his PhD from Washington State University. He served on the electrical engineering faculties of Ohio University and Washington State University, and in 1982 he founded Schweitzer Engineering Laboratories, Inc. to develop and manufacture digital protective relays and related products and services. Today SEL is an employee-owned company, which serves the electric power industry worldwide and is certified to the international quality standard ISO-9001. SEL equipment is in service at voltages from 5 kV through 500 kV, to protect feeders, motors, transformers, capacitor banks, transmission lines, and other power apparatus.

David Whitehead, P.E. is the vice president of Research and Development at Schweitzer Engineering Laboratories, Inc. Prior to joining SEL, he worked for General Dynamics, Electric Boat Division as a combat systems engineer. He received his BSEE from Washington State University in 1989, his MSEE from Rensselaer Polytechnic Institute in 1994, and is pursuing his PhD at the University of Idaho. He is a registered professional engineer in Washington and Maryland and a Senior Member of the IEEE. Mr. Whitehead holds nine patents with several others pending. He has worked at SEL since 1994 as a hardware engineer, research engineer, and chief engineer/assistant director, and has been responsible for the design of advanced hardware, embedded firmware, and PC software.

Allen D. Risley is a senior research engineer for Schweitzer Engineering Laboratories, Inc. in Pullman, Washington. Mr. Risley is responsible for leading electronic security research efforts aimed at defending critical infrastructure communications networks. His work has been presented at several electric power industry conferences including the Western Power Delivery Automation Conference, DistribuTECH, and the Texas A&M Conference for Protective Relay Engineers. He has worked for Advanced Hardware Architectures as a senior research engineer specializing in information theory, channel modeling, and advanced digital communication techniques. His work on wireless channel modeling and optimized, iterative forward error correction techniques has been presented at the 1998 Conference on Information Sciences and Systems, as well as the 2001 International Symposium on Communications Theory and Applications, and has been published in the Proceedings of the International Symposium on Information Theory and the IEEE Transactions on Communications. He earned his M.S.E.E. from Washington State University.

Rhett Smith is a development manager for the security solutions group at Schweitzer Engineering Laboratories, Inc. In 2000, he received his B.S. degree in electronics engineering technology, graduating with honors. Rhett is working on five U.S. Department of Energy control system cyber security cooperative agreements. He is the project director for the Hallmark project, Watchdog Project, Padlock Project and is a principal investigators on the Lemnos project and Whitelist A/V Project. Rhett has his GSEC, GIAC Security Essentials Certification, and is a Certified Information Systems Security Professional (CISSP).

Previously presented at the 2011 Texas A&M
Conference for Protective Relay Engineers.

20110217 • TP6464-01