Requirements or Recommendations? Sorting Out NERC CIP, NIST, and DOE Cybersecurity

David Dolezilek and Laura Hussey
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.2011.6035634.

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

Originally presented at the
12th Annual Western Power Delivery Automation Conference, April 2010

Requirements or Recommendations? Sorting Out NERC CIP, NIST, and DOE Cybersecurity

David Dolezilek and Laura Hussey, *Schweitzer Engineering Laboratories, Inc.*

Abstract—**Oil and gas, water and electric power—all of these essential services rely on SCADA (supervisory control and data acquisition), protection, and monitoring systems that use communications networks. The use of communications networks makes these systems potentially vulnerable to cyberattack. Over the past decade, faced with an increase in computer hacking and the recognition of the importance of these services to health and welfare, economic stability, and national security, the United States federal government has been increasingly involved in efforts to assist utilities in improving their security posture.**

Smart grid has become synonymous with asynchronous, nonmission-critical information exchange applications. Smart grid infrastructure describes the existing, yet largely unrecognized, mission-critical control applications that enable generation and delivery of power. Smart grid infrastructure applications require deterministic and synchronous message exchange, including automation and teleprotection.

Today, utilities are faced with a confusing array of cybersecurity guidance, standards, and regulatory requirements. Electric utilities operating bulk power system assets must comply with eight NERC (North American Electric Reliability Corporation) CIP (Critical Infrastructure Protection) standards that are in the process of being revised. Federal entities are required by the FISMA (Federal Information Security Management Act of 2002) to comply with NIST (National Institute of Standards and Technology) standards. Under the Energy Independence and Security Act of 2007, Congress gave NIST the task of developing a framework of interoperability and cybersecurity for smart grid applications. To date, the framework has been primarily focused on smart grid information exchange applications that use asynchronous data flow, including metering, demand response, and the near real-time elements of substation and distribution automation. These automation elements and other smart grid infrastructure applications that require deterministic synchronous data exchange, including teleprotection and synchrophasor state measurement, remain a future endeavor.

This paper discusses various cybersecurity requirements and presents a clear picture of work being done by NIST to explain what is required and recommended and what utilities should expect to see in the near future as NERC and NIST work continues.

I. Introduction

Several different United States laws impose cybersecurity-related requirements on utilities, but each law covers a different set of entities. Some entities, such as federal power marketing administrations, are required to comply with more than one law when implementing cybersecurity.

The cybersecurity requirements imposed by these laws sometimes take the form of standards, as in the case of the NERC (North American Electric Reliability Corporation) CIP (Critical Infrastructure Protection) standards. However, the word *standard* is also used to identify cybersecurity guidance and strategic documents (e.g., NIST [National Institute of Standards and Technology] standards, such as SP 800-82) and consensus technical standards (e.g., ISO 27001), as well as regulatory mandates. Standards describe uniform engineering or technical criteria, methods, processes, and practices and may actually be a regulatory requirement. It may not be clear that requirements that apply to one set of entities may not apply to another set of entities, although they may provide useful guidance to the latter.

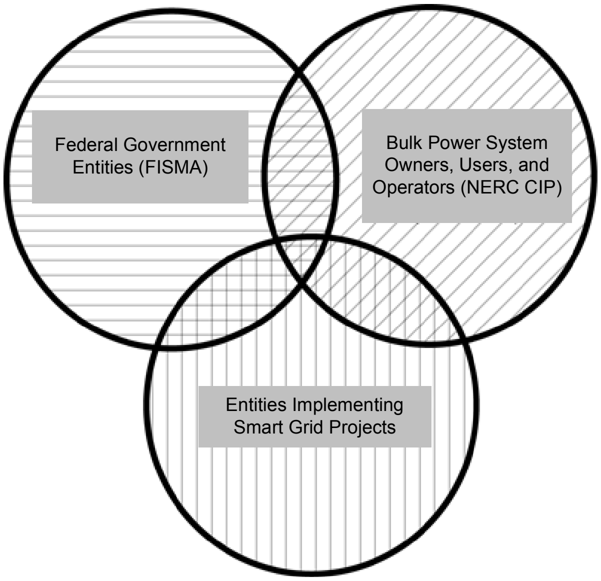
Federal Government Entities (FISMA)
Bulk Power System Owners, Users, and Operators (NERC CIP)
Entities Implementing Smart Grid Projects

Fig. 1. Applicability of Cybersecurity Laws

The confusing proliferation of standards and guidance for electric power system cybersecurity has understandably made it more difficult for individual utilities to quickly determine what is required of them and has certainly posed a challenge for those who would like to review or provide input to the many parallel efforts.

This paper provides some clarity by comparing the purpose, scope, and approach of various NERC and NIST cybersecurity documents with applicability to electric power systems.

II. FERC, the Federal Power Act, and Mandatory Cybersecurity Standards

The U.S. Federal Energy Regulatory Commission (FERC) derives its authority to regulate cybersecurity from the Federal Power Act. In 2005, the Energy Policy Act of 2005 (EPAct 2005) amended the Federal Power Act, creating a new

Section 215 that gave FERC authority over the reliability of the bulk electric power system (and the owners, users, and operators of bulk power system assets). EPAct 2005 explicitly defines the term *reliability standard* to include cybersecurity protection [1].

Section 215 sets out a framework for developing reliability standards, including cybersecurity standards, with input from industry technical experts. Industry-developed standards must be approved by FERC and, once approved, are enforced by an Electric Reliability Organization (ERO) approved by FERC. In 2006, NERC officially became the ERO when FERC approved its application.

This model is referred to as a self-regulatory model, because the industry develops the standards that regulate it, although FERC may send the industry back to the drawing board if it determines that a standard is not enforceable or is overly permissive, or for other reasons. Standards are developed by drafting teams made up of volunteers selected for appropriate technical expertise. The draft standards are then vetted by the broader industry through a balloting process. Once approved through the balloting process, the standards are filed with FERC for approval [2].

Although it is not required to do so, FERC has conducted formal rulemaking proceedings for standards filings it has received to date. Rulemaking provides utilities and other interested parties an opportunity to comment on FERC proposed actions before a final rule is issued. In a final rule on standards filed, FERC can take one of three actions: approve as filed, approve but require changes, or remand the standards back to the ERO for further work.

In January 2008, acting under its Federal Power Act Section 215 authority, FERC issued Order 706, approving the first set of eight cybersecurity standards and an implementation schedule requiring all utilities that own, use, or operate assets that are part of the United States bulk electric power system to be fully compliant with the standards in 2010. Order 706 also requires that NERC make numerous revisions to strengthen the eight standards, NERC CIP-002 through CIP-009, which are collectively referred to as the NERC CIP standards [3].

Activities to implement the directives in Order 706 are in progress, and a final set of NERC CIP standards incorporating FERC directives will probably be finalized in 2011. While it is too early in the process to predict how the standards will look, preliminary indications from drafts provided by the CIP Standards Order 706 Drafting Team suggest that a major overhaul is underway [4].

III. NIST and the Federal Information Security Management Act of 2002

A second United States law imposing requirements that affect some entities in the electric power industry is the Federal Security Management Act of 2002, commonly referred to as FISMA [5]. FISMA codifies a comprehensive framework of requirements to secure federal computer systems with oversight by the U.S. Office of Management and Budget. Under FISMA, NIST is charged with developing standards for the security of federal computer systems. In addition to complying with NERC CIP standards as owners, users, and operators of assets that are part of the bulk electric power system, United States federal entities that own and operate electric power systems must comply with FISMA for both their control and office systems.

The NIST Computer Security Division carries out NIST and FISMA information and computer system security activities. There are many NIST work products that may be useful in the context of securing electric power systems; several of them are discussed later in this paper. The NIST process for developing information and computer system security standards and guidance for federal agencies is substantially different from NERC processes. NIST is not required, as NERC is, to use consensus-based processes for developing standards. Instead, as a federal agency, NIST is generally required to provide the public with notice of its activities and may seek input but is not obligated to respond to the input in the same way as NERC and FERC. Although NIST processes are not consensus-based, NIST staff have sought extensive input from interested parties [6].

In the NIST realm, there are two types of documents that are sometimes referred to as NIST standards. One is a Federal Information Processing Standard (FIPS) that is approved by the Secretary of Commerce and with which federal agencies must comply as part of FISMA. An example of this type of standard is FIPS-200, which describes minimum security standards for federal information systems. The second type is the NIST Special Publication series (the 800 series applies to computer system security). The Special Publication series documents, such as NIST SP 800-53, are closer to a framework written to guide entities required to comply with FISMA with implementing those requirements in ways that are appropriate to their particular function and circumstances.

According to NIST, the FIPS and Special Publications documents are designed to be used together to provide a strong foundation for an entity to use in developing a comprehensive cybersecurity risk management framework [7]. Nongovernmental organizations may also use both types of documents to assist them in their cybersecurity efforts.

Owners and operators of federally owned industrial control systems are subject to FISMA compliance and must comply with the FIPS developed by NIST in securing their control systems. For all other entities, including nonfederal electric utilities, there is no requirement to comply with FIPS. These entities can consider the NIST standards and companion Special Publications as guidance.

As explained in the NIST risk management framework, the general approach to applying NIST standards for information system security is to:

- Identify and categorize systems requiring security according to their impact on the mission of an organization and the need for confidentiality, integrity, and availability of information in the system.
- Select an appropriate set of security measures or controls [7].

Two FIPSs correspond to these two steps. First, FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, sets out requirements for the identification and classification of systems according to their impact on the mission of an organization and the need for confidentiality, integrity, and availability of information in the system. Next, FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, identifies 17 areas of security that must be addressed [8].

For electric power systems, NIST Special Publication 800-53 (SP 800-53) and Special Publication 800-82 (SP 800-82) provide guidance that can be used to assist entities in selecting the right set of security controls to address each of the 17 areas, as well as an eighteenth area, program management. Table I lists the 18 areas, along with an identifier (code) that is used in SP 800-53 and SP 800-82 for each of the 18 areas, or families, of security controls.

TABLE I
FAMILIES OF SECURITY CONTROLS

Identifier	Family	Class
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational
PM	Program Management	Management

SP 800-53 provides extensive guidance on selecting an appropriate and cost-effective set of security measures (controls) for any information system. Because SP 800-53 was written to be broadly applicable to all types of information systems used by federal agencies and departments, it provides general guidance that must be applied by each entity in the context of the entity mission, the purpose of an individual system, and other considerations. It was not specifically written to address utility or industrial control systems, such as SCADA (supervisory control and data acquisition).

IV. Operations and Information Technology Require Different Performance and Standards

Cybersecurity of electric power systems is a reliability matter, and appropriate cybersecurity measures must not compromise reliability. When selecting security measures, it may be helpful to differentiate two types of networks: operations technology (OT) networks and information technology (IT) networks. OT refers to the devices and methods, such as networks of intelligent electronic devices (IEDs), used to automatically control and manually operate an industrial process [9]. In electric power systems, OT networks are specialized IED networks that include protection, control, and monitoring (PCM) IEDs and associated PCM applications. These PCM OT networks automatically control and allow manual operation of the apparatuses that generate, transmit, distribute, and consume energy. The IEDs in these networks also generate, transmit, distribute, and consume information associated with the automatic control and manual operation processes.

PCM OT networks are local networks that support a substation and may also cover its neighboring distribution circuits or wide-area networks connecting several substations. For example, Fig. 2 shows several local OT networks communicating mission-critical information over a wide-area OT network.

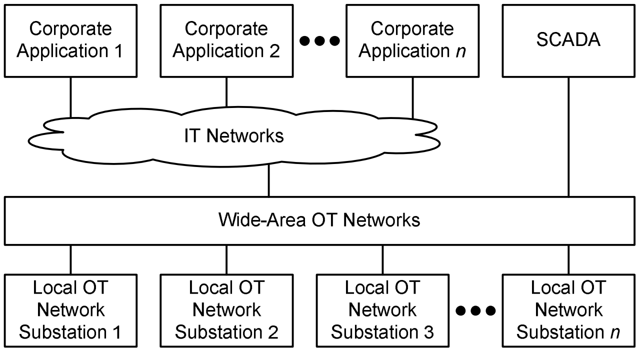
Corporate Application 1
Corporate Application 2
Corporate Application *n*
SCADA
IT Networks
Wide-Area OT Networks
Local OT Network Substation 1
Local OT Network Substation 2
Local OT Network Substation 3
Local OT Network Substation *n*

Fig. 2. Local OT Networks Communicate Mission-Critical Information Over Wide-Area OT Networks

This information, including the synchronous exchange of teleprotection signals, synchrophasors, remedial action schemes, arming data, contingency alarms, and mitigation control, as well as asynchronous SCADA data and engineering access, is traditionally transported via OT network methods. Successful wide-area OT methods, such as time-division multiplexing, provide the deterministic and high-availability characteristics necessary for synchronous mission-critical electric power system applications.

IT refers to the devices and methods used to transport information among people and processes. IT networks are not the source of information but rather the conduit to move information from the source to a remote person, process, or network. In the Fig. 2 example, IT networks provide information for corporate applications, such as planning, asset management, and billing. OT networks are the information sources for these applications. Fig. 2 shows that IT networks connect to OT networks to collect and distribute decision-making information. IT networks are represented as a cloud because their structure and behavior are variable, adaptable, and nondeterministic. These characteristics are acceptable for IT purposes, where convenience and flexibility are desirable to move smart grid information for nonmission-critical business processes and some asynchronous electric power system applications.

Present day activities focused on smart metering and other peripheral smart grid applications are being designed using bandwidth-sharing IP (Internet protocol) methods. Many activities already underway are promoting more adoption of IT technologies in local-area and wide-area PCM OT networks. However, real-time PCM applications and mission-critical communication do not exist in other industrial OT networks where IT methods have been adopted. PCM OT networks must be designed based on a clear understanding of their expected behavior. These PCM OT networks perform "smart grid infrastructure applications," the activities that automate the generation, delivery, and consumption of electric energy.

As an example, consider the very different OT and IT approaches to two important PCM OT network design criteria: secure and dependable exchange of information. In this context, security is not referring to cybersecurity attributes of confidentiality, integrity, and authentication.

- *Security of communications-aided protection and control* requires deterministic latency of each message delivery. For example, security of a mission-critical control means "to refrain from tripping a breaker when not required to trip." A secure OT network is designed to guarantee deterministic, on-time delivery of each blocking or interlocking message. OT security means every message is delivered with predetermined maximum latency. IT networks are instead designed to buffer and redirect traffic to increase the likelihood that the message will eventually be delivered. IT networks optimize network throughput, meaning that the network makes a best effort to deliver each message, regardless of how long it takes. Message propagation delays of IT networks may cause protection and control problems.
- *Dependability of communications-aided protection and control* requires delivery of each message. For example, dependability of a mission-critical control means "to perform tripping when a breaker is required to trip." A dependable OT network is designed to guarantee deterministic, on-time delivery of each tripping or control message once and only once. OT network dependability means reducing lost messages to near zero. A dependable IT network is instead designed to send and resend messages to increase the likelihood that one eventually makes it through. IT dependability means the network detects and resends lost messages. Resent buffered messages of IT networks may cause protection and control problems.

V. Balancing Communications, Cybersecurity, Performance Security, and Dependability in the Smart Grid

To address security in the context of the unique performance requirements of control systems, NIST incorporated an appendix in revision two of SP 800-53 that contains guidance for tailoring and supplementing SP 800-53 for control systems.

This document addresses the needs of asynchronous control system applications, but this and most other efforts have not yet addressed the underlying mission-critical synchronous data exchange requirements. Synchronous and asynchronous control systems alike differ from traditional corporate IT systems in a number of ways. In many traditional IT systems, the most significant consequences of the temporary loss of availability may be inconvenience and lost productivity. In contrast, real-time control systems, such as SCADA and distributed automation used in electric power systems, tend to have high reliability requirements with potential adverse impacts on the safety and health of power system personnel and the public resulting from failure or misoperation. High reliability requirements, combined with a very different set of assets than those found in a typical corporate network, require that certain security practices common in corporate IT systems be modified to suit the control system environment without causing other adverse impacts.

Evaluation of the two smart grid application categories reveals differences that mirror the differences between OT and IT networks. Smart grid infrastructure describes the existing, yet largely unrecognized, mission-critical control applications requiring deterministic and synchronous message exchange via OT networks that will not function on bandwidth-sharing IT networks. These include substation and distribution automation teleprotection, which enables power generation and delivery, as well as future synchrophasor applications. Smart grid has become synonymous with asynchronous, nonmission-critical information exchange applications. These applications work over either OT or IT networks because of the less stringent data flow performance requirements.

NIST prepared SP 800-82 to provide expanded guidance on securing industrial control systems. SP 800-82 includes a comprehensive overview of industrial control system architecture and techniques for managing risk without negatively affecting control system operations. One potential use of SP 800-82 is as a tool to facilitate communication about security requirements between owners and operators of industrial control systems and the manufacturers of those systems. SP 800-82 does not duplicate but instead significantly expands on the guidance found in Appendix I of SP 800-53.

Efforts are underway to help the Smart Grid Interoperability Panel, which is responsible for identifying and recommending communications standards, recognize that the synchronous data exchange within the power system and smart grid infrastructure applications is not yet addressed by an applicable standard. Once complete, appropriate cybersecurity measures can be addressed.

VI. NIST, FERC, AND THE ENERGY INDEPENDENCE AND SECURITY ACT OF 2007

Title XIII of the Energy Independence and Security Act of 2007 (EISA), the Smart Grid title, creates additional cybersecurity responsibilities for NIST, FERC, and the U.S. Department of Energy. Several sections of Title XIII are relevant to understanding which responsibilities fall to each agency and ultimately how electric utilities may be affected.

Section 1302 lists ten characteristics that, in combination, make up a smart grid. The first two are noteworthy from a cybersecurity perspective:

- Increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid.
- Dynamic optimization of grid operations and resources, with full cybersecurity [10].

Section 1306 lists eight smart grid functions, along with a ninth function that allows the Secretary of Energy to add to the list at a future time. Fifth on the list is: “the ability to detect, prevent, communicate with regard to, respond to, or recover from system security threats, including cyber-security threats and terrorism, using digital information, media, and devices.” [10]

Section 1305 concerns the development of an Interoperability Framework for Smart Grid. NIST is responsible for overseeing and facilitating appropriate input into the development of this document. NIST has undertaken an extensive effort to develop a report that provides guidance on cybersecurity for smart grid projects. The NIST Smart Grid Interoperability Panel Cybersecurity Working Group (formerly called the Cybersecurity Coordination Task Group, or CSCTG) is helping to develop this document with NIST staff.

The group work product is NIST Interagency Report 7628: *Smart Grid Cyber Security Requirements* (NISTIR 7628). When NISTIR 7628 is finalized in the summer of 2010, it will reflect input from two rounds of public comments and provide high-level guidance to assist entities involved in implementing smart grid projects with securing those projects. The NISTIR does this in part by applying existing work, such as the *Catalog of Control Systems Security: Recommendations for Standards Developers* [11] published by the Department of Homeland Security, NERC CIP standards, and the standards and guidance produced by the NIST Computer Security Division, particularly those mentioned in this paper.

NIST does not have authority to require compliance with NISTIR 7628, and indeed, the document was not written to facilitate compliance enforcement. Instead, NISTIR suggests a methodical approach to developing an appropriate set of security controls for a smart grid project. The tasks were followed at a macro level by the working group, but an individual utility may apply the macro approach to a particular project at the micro level.

Briefly, the approach taken to create NISTIR involved the following tasks:

1. Identify use cases for the purpose of defining cybersecurity requirements.
2. Perform risk assessment, identifying vulnerabilities, threats, and impacts or consequences.
3. Identify security requirements.
4. Develop security architecture.
5. Assess gaps to be addressed and recommend actions to address gaps.

Applying this macro approach to securing an individual utility project would approximately translate into the following tasks:

1. Review NISTIR use cases and interface categories to identify those that fit most closely with the utility project.
2. Perform risk assessment.
3. Identify security requirements using the high-level requirements from NISTIR as a guideline but taking into account the modes of communications, as well as the impact assessment from Step 2.
4. Develop and implement a project security architecture, including identification of mitigating controls to address gaps.
5. Develop and implement a security management plan.

One significant difference between the NIST work products mentioned previously and NISTIR is that NISTIR focuses on securing interfaces or the communications links between systems or devices rather than on securing systems. The interface approach has strengths and weaknesses. A strength of the approach is focusing on the very thing that makes the grid smarter—that is, the increased use of data for monitoring and real-time control of the system. These data flow over the interfaces, and the nature and uses of these data drive the need for confidentiality, integrity, and availability. A system-oriented approach might drive overall security requirements higher than the interface-oriented approach does and at greater cost, without commensurate risk reduction.

On the other hand, the interface approach is difficult to apply in certain situations. Consider, for example, the use of mobile computers in maintaining device settings. The interface approach is concerned with securing data travelling over the communications medium between the mobile computer and the intelligent device. While this is necessary, it is not sufficient. The security of the mobile computer, and particularly the integrity of the data stored on the mobile computer before being transmitted over the interface, is important as well.

Another difference is that NISTIR focuses both on current applications of technology and future applications that are either not mature or have not yet been developed. In addition, it is inevitable that new vulnerabilities and perhaps threats will be identified, requiring utilities and smart grid manufacturers to proactively review risk assessments and adapt their security posture.

The evolving nature of smart grid technologies and security suggests that the approach embodied in NISTIR should guide but not be considered as the definitive source of security requirements for smart grid projects, but instead as one resource in a utility's toolkit. Effective and cost-effective security is best achieved by carefully and realistically assessing risk and then thoughtfully applying documented security principles to mitigate those risks.

Cybersecurity regulatory requirements will continue to evolve as well. EISA Section 1305 (d) is the important part for understanding how the NIST framework may translate to future cybersecurity requirements for electric utilities:

> At any time after [NIST's] work has led to sufficient consensus in the [FERC's] judgment, the [FERC] shall institute a rulemaking proceeding to adopt such standards and protocols as may be necessary to insure smart-grid functionality and interoperability in interstate transmission of electric power, and regional and wholesale electricity markets [11].

According to Section 1302 and 1306, smart grid functionality includes cybersecurity. It is unclear at this time how FERC will proceed, but the rulemaking process will provide an opportunity for electric utilities to comment on a proposed rule before a final order is issued. In addition, before conducting a rulemaking, FERC has the option of seeking public input through a technical conference or notice of inquiry, which it has done in other complex matters. The entire process, from the determination of sufficient consensus through proposed rulemaking, comment, and issuance of a final order, as well as the inevitable requests for rehearing or clarification of the order, is likely to take a year or longer and not likely to be initiated before middle to late 2010.

VII. Conclusions

Much the same way that industrial and power system OT networks differ from IT networks, smart grid infrastructure applications differ from visible smart grid data exchange applications. Most people equate metering, demand response, and other visible data exchange applications with smart grid. As an industry, we must make the infrastructure applications visible, because they are essential to the actual operation of the grid. We must also design appropriate security for them as well.

Effective and cost-effective cybersecurity for electric power systems requires a realistic risk assessment coupled with a thoughtful, commonsense application of security principles. Compliance with regulatory requirements does not guarantee effective security, nor does blindly following a single guidance approach. The documents discussed in this paper and those referenced within them are a rich source of information, but ultimately, each utility is in the best position to identify and implement a collection of security measures that together provide effective security for its systems [12].

VIII. References

[1] Energy Policy Act of 2005, Pub. L. No 109-58, Title XII, Subtitle A, 119 Stat. 594, 941 (2005).

[2] NERC Rules of Procedure. Available: http://www.nerc.com/page.php?cid=1|8|169.

[3] Mandatory Reliability Standards for Critical Infrastructure Protection, Federal Energy Regulatory Commission, Order No. 706, 73 FR 7368 (Feb. 7, 2008), 122 FERC 61,040, 123 FERC 61,174 (2008).

[4] NERC Project 2008-06, Cyber Security Order 706. Available: http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html.

[5] E-Government Act of 2002, Pub. L. 107-347, Title III, 116 Stat. 2899 (2002).

[6] "Guide to NIST Information Security Documents." Available: http://csrc.nist.gov/publications/CSD_DocsGuide.pdf.

[7] "Risk Management Framework," National Institute of Standards and Technology (2002). Available: http://csrc.nist.gov/groups/SMA/fisma/framework.html.

[8] "Minimum Security Requirements for Federal Information and Information Systems," FIPS Publication 200, National Institute of Standards and Technology. Available: http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.

[9] D. Dolezilek, "Case Study Examples of Interoperable Ethernet Communications Within Distribution, Transmission, and Wide-Area Control Systems," proceedings of Grid-Interop, Denver, CO, November 2009.

[10] Energy Independence and Security Act of 2007, Pub. L. 110-140 (2007).

[11] "Catalog of Control Systems Security: Recommendations for Standards Developers," U.S. Department of Homeland Security, U.S. Computer Emergency Readiness Team, September 2009. Available: http://www.us-cert.gov/control_systems/pdf/Catalog_of_Control_Systems_Security_Recommendations.pdf.

[12] E. O. Schweitzer, III, "Ten Tips for Improving the Security of Your Assets." Available: http://www.selinc.com.

IX. Biographies

David Dolezilek received his BSEE from Montana State University and is the technology director of Schweitzer Engineering Laboratories, Inc. He has experience in electric power protection, integration, automation, communications, control, SCADA, and EMS. He has authored numerous technical papers and continues to research innovative technology affecting our industry. David is a patented inventor and participates in numerous working groups and technical committees. He is a member of IEEE, the IEEE Reliability Society, CIGRE working groups, and two International Electrotechnical Commission (IEC) technical committees tasked with global standardization and security of communications networks and systems in substations.

Laura Hussey joined Schweitzer Engineering Laboratories, Inc. (SEL) in June 2009 as director of cybersecurity policy. Before joining SEL, Laura was employed by Edison Electric Institute (EEI) for almost nine years, most recently as manager of security, infrastructure, and operations. In that role, she served as staff to the EEI Security Committee and Business Continuity Working Group. She has extensive experience working on cybersecurity matters with electric utilities, NERC, and government agencies (including FERC, the Departments of Energy, Homeland Security, and Defense, and the National Institute of Standards and Technology). Laura has a BS in information science from the University of Pittsburgh. Before joining EEI, she spent 15 years as an IT trainer and consultant for a variety of clients in the manufacturing, health care, financial, legal, and higher education sectors.

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

20110217 • TP6434-01