# Smart Grid Cyber Security and Substation Network Security

J. Farquharson, A. Wang, J. Howard

***Abstract*—**
A successful Smart Grid system requires purpose-built security architecture which is explicitly designed to protect customer data confidentiality. In addition to the investment on electric power infrastructure for protecting the privacy of Smart Grid-related data, entities need to actively participate in the NIST interoperability framework process; establish policies and oversight structure for the enforcement of cyber security controls of the data through adoption of security best practices, personnel training, cyber vulnerability assessments, and consumer privacy audits.

***Index Terms*—**
Advanced Metering Infrastructure (AMI)
Advanced Security Acceleration Project for the Smart Grid (ASP-SG)
Automated Data Exchange (ADE)
Consumer Privacy
Data Minimization
Data Security
Demand Response and Smart Grid Coalition (DRSG)
Home Area Network (HAN)
IP Security (IPSec)
ZigBee Smart Energy

## I. Introduction

A recent report from Pike Research, "*Smart Grid Cyber Security*" has found if smart grids can realize their full potential, consumers, utilities, nations, and even the earth itself will benefit. As with nearly any new technology, the industry focus has been on getting smart grids up and running, often with little consideration for cyber security issues. However, the report found that investment in securing the grid from malicious attacks, natural disasters, and other accidents is picking up pace. The cleantech market intelligence firm expects that smart grid cyber security spending will increase 62% between 2010 and 2011, and by 2015 the annual worldwide market spending in this critical sector will reach $1.3 billion.[1]

Additionally, steps to transform the nation's aging electric power grid into an advanced decentralized, digital infrastructure with two-way capabilities for communicating information, controlling equipment, and distributing energy will take place over many years. In concert with these developments and the underpinning public and private investments, key enabling activities also must be accomplished. Primary among them is devising effective strategies for securing the computing and communication networks that will be central to the performance and availability of the envisioned electric power infrastructure and for protecting the privacy of Smart Grid-related data. While integrating information technologies is essential to building the Smart Grid and realizing its benefits, the same networked technologies add complexity and also introduce new interdependencies and vulnerabilities. Approaches to secure these technologies and to protect privacy must be designed and implemented early in the transition to the Smart Grid.[2]

The first step is to adopt appropriate privacy policies defining what data may be collected and their permissible uses, disclosing those practices clearly and conspicuously, and obtaining consents where required. Since Smart Grid data differ qualitatively from what utilities collected in the past, they will likely need new and stronger privacy and security policies. Consumers are interested primarily in controlling what information is collected, who has access to it, and how it may be used. These interests are often described in fair information privacy practices or core principles, such as the OECD's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.

Once a utility establishes the permissible uses of Smart Grid data, it is in its interest to assure that unauthorized uses do not occur. The *Security Profile for Wide-Area Monitoring, Protection, and Control* (WAMPAC) prepared by The Advanced Security Acceleration Project[3] for the Smart Grid (ASAP-SG) defines a reference architecture, a set of use cases to define system functionality, and a set of security controls for systems and components that implement the use cases, leveraging synchrophasor technology. Every utility will want to avoid regulatory sanctions for violating express or implied privacy policies as well as damages claims based on compromised customer data or facilities.  Thus the utility's second step is to establish systems for enforcement of sound cyber security controls of the data through adoption of security

[1] Report on Smart Grid Cyber Security, May 2011, Paul Budde, Managing Director of Paul Budde Communication, http://www.circleid.com/posts/20110503_report_on_smart_grid_cyber_security/

[2] Introduction to NISTR 7628 Guidelines for Smart Grid Cyber Security: The Smart Grid Interoperability Panel Cyber Security Working group, September 2010.

[3] Security Profile for Wide-Area Monitoring, Protection, and Control. Prepared for: The UCAlug SG Security Working Group; Prepared by: The Advanced Security Acceleration Project for the Smart Grid (ASP-SG); Managed by: EnerNex Corporation, Version 0.08, May 16, 2011.

978-1-4577-2159-5/12/$31.00 ©2011 IEEE

practices, training, cyber vulnerability assessments, and consumer privacy audits.

As P. A. Subrahmanyam, *et al.*, recognized early, in *Network Security Architecture for Demand Response/Sensor Networks,* the Smart Grid architecture will determine the points of security vulnerability. Wireless sensor networks, for example, are subject to the general security problems of computer networks, ordinary wireless networks, and ad-hoc networks. The limited resources of common sensor nodes – slow CPUs and small memories – hinder the use of cryptography defenses. Packet jamming and insertion may occur over any network or link layer in the communication infrastructure. Adversaries may use simulated nodes, out-of-band channels, and modified or self-generated data to facilitate sinkhole attacks, acknowledgement spoofing, rushing attacks, HELLO floods, or blended attacks. These may result in denial of service to customers or utilities (e.g., access to billing information or energy usage), payment avoidance, system overload, reduced quality of service, and violation of power control protocols. Attacks may come from inside the network via disgruntled, negligent or untrained employees or an outsider's access to a compromised node or IP server. Indeed, Smart Grid security weaknesses could enable penetration of presently secure systems. As LeMay, *et al.* has shown in *Unified Architecture for Large-Scale Attested Metering*, robust security is achievable, and imperative.

The upshot is that customer interest in having effective security to protect privacy interests converges with the utility's need to protect its economic interests in the data and to secure its systems against malicious attacks. By recognizing that utility and consumer have convergent interests, the tension between Smart Grid implementation and privacy interests fades.

**Legal Considerations**

Privacy and security laws vary widely from place to place. In the European Union, for example, the *Privacy Directive* 95/46 EC establishes a presumption that personally identifiable information belongs to the data subject. Such information may be processed only for specified, legitimate, and limited purposes where there is either valid consent from the data subject or a legitimate need of the data processor that outweighs the data subject's general privacy interests. This general privacy right will extend to personally identifiable Smart Grid data. In the United States, privacy and security rules arise out of a large number of federal and state laws regarding the processing of particular types of data or economic sectors, disposition of business records, utility tariffs, etc., but there is no general right of privacy in the European sense.

Which laws and regulations apply depends upon the system architecture. For example, if a utility collects and transmits Smart Grid data via BPL and also offers consumers internet access, the utility may be subject to rules governing telecommunications service providers. If a utility sends Smart Grid data to a billing firm in different state, federal laws applicable to interstate commerce or the receiving state's privacy laws may apply. If a utility sends personally identifiable information concerning EU residents to an outsourcer on another continent, the EU *Privacy Directive* limits on transborder data flows will apply. If personally identifiable data may have been compromised, breach notification laws may require the utility to send notices to data subjects in certain jurisdictions. Failure to adopt, discloses, or adheres to suitable privacy and security practices may result in U.S. Federal Trade Commission enforcement action against "unfair and deceptive trade practices."

Utilities will need to consult legal counsel to determine how a contemplated Smart Grid design may implicate various laws and whether the ramifications are acceptable. It is important to do this at the design stage, because it is always more expensive to revise systems after initial deployment.[4]

**Data Minimization**

California (CA) Public Utilities Code Section 6354(e) – Energy utilities must report to municipalities the names and addresses of customers who transport gas or electricity, for purposes of enforcing taxes and fees. Municipalities shall not disclose such customer information to third parties.

**Use Limitation**

CA Public Utilities Code Section 583 –Prohibits disclosure of confidential information provided by California Public Utility Commission (CPUC)-jurisdictional public utilities to the CPUC unless ordered released by the CPUC. CPUC Decision No 97-12-088, 77 CPUC 2d 422 (1997), and D.06-12-029 – Adopting affiliate transaction rules, including prohibiting the disclosure of customer information to affiliates or non-affiliates without prior affirmative customer written consent (Affiliate Rule IV.A.)

**Data Security**

The City of Burbank Water and Power (BWP) Smart Grid Program on the entity's web-page pledges to consumers that *"Protecting your privacy and ensuring the security of your account information remain our highest priorities. Absolutely no personal information is transmitted as part of the meter reading process and BWP will NEVER share your personal information with an unaffiliated third party or without your permission."*[5]

Smart grid deployments are very data intensive. From one way meter reads to demand response to real time pricing applications, the data exchange between utility billing and operations and the networked endpoints require properly engineered and secure data pipes. To enable the multiple services and support various applications, substations are utilized as an anchor for data transport. Mainly due to the substation already having or a plan exists to have high bandwidth transport services, a connection to network

[4] Data Privacy and Security Issues for Advanced Metering Systems, July 1, 2008, Mark F. Foley.

[5] City of Burbank Water and Power (BWP) Smart Grid Program http://www.burbankwaterandpower.com/environment/smartgrid

management systems (NMS), and SCADA observation by control centers via energy management systems (EMS). These are normally critical facilities, large distribution or transmission substations, requiring a constant stream of data to monitor and operate the station remotely.

The data collected from the distributed, networked Smart Grid elements (meters, distributed generation, cap banks, etc.) is relayed via strategically placed collector elements in the utilities territory. A collector is also located at the substation to collect data from nearby elements or serve as the last hop before being inserted into the substations local area network (LAN).

**Substation Network Security**

Once on the substations LAN, a complete separation of Smart Grid traffic from substation operational information is essential. This is to ensure data integrity and protect any potential individuals account or other sensitive information from being accessible to individuals that have access to operational data. At a minimum, two data segregation and isolation technologies should be utilized. The technologies considered and available in modern local area network equipment should be standards based and are not to be vendor specific as they could possibly limit applications supported or need to be completely replaced in the future.

Virtual Local Area Networks (VLANs) are used to maintain the logical separation of data between applications utilizing the same transport hardware. Non operational data and multi-substation traffic such as Voice over IP (VoIP) or inter- and intra-net communications, will utilize VLANs to simplify the physical infrastructure at each station. By sharing the physical infrastructure, traffic must be managed and prioritized so that the data transmitted efficiently uses the available bandwidth. Operational data, such as Generic Object Oriented Substation Events (GOOSE) and MMS messages on an IEC61850 network, should be separated physically as this data exchange is critical.

The wide area network (WAN) transport interface at the substation may utilize either native (such as MPLS or gigabit Ethernet) or encapsulated IP (such as SONET). The type of WAN transport equipment to use is based on what existing systems are in place and the business case or operational need to acquire systems that may support other applications in the future. Again, the hardware must maintain traffic segregation giving priority to SCADA and other energy delivery and operational metering systems.

Native IP has the advantages of being an IP network from Smart Grid End device on one end, to the business operations system on the other. This enables one NMS to monitor and manage the network from end to end for non-critical data applications.

IP Security (IPSec) allows the transmitted data IPSec/VPN tunnels. Encapsulated IP has the advantage of being a known technology that can support high bandwidth applications while still support line protection schemes.

**ZigBee Alliance**

The ZigBee Alliance announced on July 20, 2011 that an update to the ZigBee Smart Energy Version 1 Advanced Metering Infrastructure (AMI) standard is now available for product development and public download. ZigBee Smart Energy version 1.1 adds several features, including dynamic-pricing enhancements, tunneling of other protocols, prepayment features, over-the-air updates and backwards compatibility with certified ZigBee Smart Energy products version 1.0. The Smart Grid Maturity Model (SGMM) User Community requests vendors to take ZigBee Security seriously.

**Energy Independence and Security Act of 2007**

The National Institute of Standards and Technology (NIST) identified five groups of smart grid standards to Federal Energy Regulatory Commission (FERC) under Section 1305 of the Energy Independence and Security Act of 2007 (EISA) for consideration, which requires FERC to adopt in a formal rulemaking proceeding standards and protocols necessary to ensure smart grid functionality and interoperability in interstate transmission of electric power, and regional and wholesale electricity markets.

These suites of foundational smart grid standards would: provide a Common Information Model necessary for exchanges of data between devices and networks, primarily in the transmission (IEC 61970) and distribution (IEC 61968) domains (the IEC numbers reference two related groups of standards); facilitate substation automation, communication and interoperability through a common data format (IEC 61850); facilitate exchanges of information between control centers (IEC 60870-6); and address the cyber security of the communication protocols defined by the preceding IEC standards (IEC 62351).

On July 19, 2011, FERC decided not to institute a rulemaking proceeding with respect to the five groups of standards at this time. The Commission notes that EISA identifies system security, including cyber security, as both a smart grid characteristic and function and recognizes the work NIST has done to provide guidance to industry on this issue. The Commission encourages stakeholders concerned with smart grid cyber security to actively participate in the NIST interoperability framework process, including the SGIP Cyber Security Working Group.[6] The ASAP-SG produced a Department of Energy sponsored public/private work group, produced AMI and Automated Data Exchange (ADE) security profiles that are good examples of system and architecture requirements developed to protect customer privacy that should be followed in designing related solutions and systems. Additionally, the Smart Energy Version 2.0 includes security architecture explicitly designed to protect customer data confidentiality; control of plug-in electric vehicle (PEV) charging, installation, configuration and firmware download

[6] FERC Docket No. RM11-2-000, http://www.ferc.gov/EventCalendar/Files/20110719143912-RM11-2-000.pdf

for Home Area Network (HAN) devices, prepay services, user information and messaging, load control, demand response and common information and application profile interfaces for wired and wireless HANs.[7]

**Demand Response and Smart Grid Coalition**

The Demand Response and Smart Grid Coalition (DRSG) is the trade association for companies that provide products and services in the areas of demand response and smart grid. DRSG links its efforts with the ZigBee Alliance to support the Smart Grid and works to educate and provide information to policymakers, utilities, the media, the financial community and various stakeholders on how demand response and smart grid technologies and practices can help modernize and optimize electricity systems and how customers can use new information and control options for managing their electricity use.

**Regulatory Uncertainties in the United States**

Several major bills addressing cyber security have been introduced since 2010.

In The White House Fact Sheet: Cybersecurity Legislative Proposal, released on May 12, 2011, the Obama Administration enlists Department of Homeland Security (DHS) to cooperate with energy companies, water suppliers, and financial institutions to grade the most serious threats and find ways to resolve them; toughen computer breach penalties, although it would not seek authority for strict top-down rules requiring companies to build specific impediments to computer intrusions. Instead, the proposal relies on incentives for private industry to voluntarily fortify computer security and have those standards reviewed by DHS.

In a Staff Discussion Draft from the US Senate Energy & Natural Resources Committee, pertaining to Cyber Security of the Bulk Power System, dated May 4, 2011: "*If the Commission determines the interim final rule must be issued immediately to protect critical electric infrastructure from a cyber security vulnerability, the Commission may—''(i) issue the interim final rule without prior notice or hearing; or ''(ii) make the interim final rule immediately effective or effective with less than 30 days notice.*"

On July 13, 2011, Senator John McCain calls for a special cyber security panel to produce comprehensive legislature on cyber security. The Senator wrote that cybersecurity legislation "has been drafted by at least three committees and at least seven committees claim some jurisdiction over the issue." He also noted that the White House and the Energy, Commerce and Defense departments have all put forward separate initiatives on the subject. "With so many agencies and the White House moving forward with cyber security proposals, we must provide congressional leadership on this pressing issue of national security," McCain wrote, adding that the best solution would be to have top Republicans and Democrats "step away from preserving their own committees' jurisdiction." Jurisdictional battles in the United States Congress are a major hindrance of advancing Smart Grid cyber security.

[7] Zigbee Smart Energy version 2.0, http://www.zigbee.org/Standards/ZigBeeSmartEnergy/Version20Documents.aspx

## Biographies

**Jerome Farquharson, CISSP,** is the Leader of Burns & McDonnell's Saint Louis security practice. He leads with a multi-disciplined background of cyber and physical security, information systems and business advisory consulting. Mr. Farquharson is an experienced Security Network Engineer with 17 years IT experience that includes experience in Network Design Implementation, Support and Troubleshooting of CISCO Routers, Switches, Firewalls, VPN Devices, Intrusion Detection Systems and network management systems. An innovative, solutions-driven Network Management and Security Specialist with well over 10 years directing the planning, design, deployment and integration of secure high-availability network infrastructure, connectivity and Web services architecture for leading Fortune 500 companies in system and network administration and engineering, hardware evaluation, project management, systems and network security, incident analysis and recovery.

**Jarad Howard, PE,** is an Electrical Engineer specializing in telecommunications, Smart Grid technologies, NERC/CIP cyber security, local and wide-area networking, and network management systems. His background includes the planning, design, engineering, commissioning and deployment of various information technologies for in both the electric utility and telecommunications carrier market sectors. He has spoken at seminars and symposiums on Smart Grid/AMI and cyber security topics. He has experience with commonly deployed relays and their measurement, data recording and event correlation capabilities.

**Anna Wang** is a member of IEEE Power & Energy Society, Women in Engineering, and Reliability Society. She is recognized by the National Association of Professional Women as the 2011/2012 Woman of the Year for demonstrating excellence and dedication within her profession.

Ms. Wang is a Cyber Security and NERC Compliance Consultant at Burns & McDonnell. She has nine years of electrical utility experience, including regulatory compliance, critical infrastructure protection, transmission reliability and operations, business continuity and security architecture evaluation with Tri-State Generation and Transmission Association and American Electric Power. Her area of expertise includes NERC Reliability and Standards Compliance and NEI Cyber Security Controls, NIST Risk Management Framework and Smart Grid Cyber Security and Consumer Privacy Protection.

Ms. Wang received her Master's degree of Information Science from the University of Illinois at Urbana-Champaign. She is a Certified Competitive Intelligence Professional.