Carol Hawk, *Ph.D. is Manager of the Cybersecurity for Energy Delivery Systems (CEDS) R&D Program for the office of Electricity Delivery and Energy Reliability in the Department of Energy (DOE). Dr. Hawk conducted her Ph.D. research in High-Energy Physics at Rutgers University as a member of the Collider Detector at Fermi National Accelerator Laboratory Collaboration. The CEDS R&D program is working to advance the energy sector's Roadmap vision of resilient energy delivery systems designed, installed, operated, and maintained to survive a cyber-incident while sustaining critical functions. In addition, she brings a variety of work experiences to DOE including telecommunications (at Bell Communications Research) as well as fuel cell electrochemistry (at United Technologies Research Center and later at the University of Connecticut). Prior to joining the DOE, Dr. Hawk performed operations research with the Center for Naval Analyses.*

Akhlesh Kaushiva, *P.E., is in the Office of Electricity Delivery and Energy Reliability with the Department of Energy. He has been actively involved in the Smart Grid Investment Grant projects sponsored by DOE as part of the American Recovery and Reinvestment Act. He is also involved in the Smart Grid Cybersecurity aspect of the projects. Prior to joining DOE he had a long career in the electric utility industry and served in various capacities in the area of system planning, power distribution, outage management, mobile dispatch, and GIS. He has a B.S.E.E. with Honors from the University of Maryland and a M.S. degree in Computer Science from the George Washington University.*

The authors express their appreciation for the contributions of staff at Duke Energy Progress, FirstEnergy, the Northern Virginia Electric Cooperative, the Sacramento Municipal Utility District, and many others who graciously shared their expertise throughout the development of this article. Skillful editorial assistance was provided by Rebecca Massello of Energetics Incorporated.

Cybersecurity and the Smarter Grid

Reliability remains a fundamental principle of grid modernization efforts, but in today's world, reliability requires cybersecurity. This article discusses energy sector partnerships that are designing cybersecurity into the smart grid with the vision of surviving a cyber-incident while sustaining critical energy delivery functions.

Carol Hawk and Akhlesh Kaushiva

I. The Power Grid: Beyond Smart

The power grid is already smart, if ''smart'' can describe an engineering masterpiece that is the largest machine ever created by humankind and that has delivered reliable power for over 100 years. Today, reliability remains a fundamental principle of grid modernization efforts.

As the power grid increasingly uses modern computational platforms, field devices, and communication networks, it gains access to new and higher-resolution data. New ways of measuring, analyzing, and communicating data support new capabilities for enhanced grid reliability, resiliency, and efficiency.

In today's world, reliability requires cybersecurity. A cyber-attack on devices that protect and control the power grid could result in power disruption or damaged equipment. It must also be kept in mind that installation of inappropriate cybersecurity controls could interfere with critical energy delivery functions. This article discusses energy sector partnerships that are designing cybersecurity into the

http://dx.doi.org/10.1016/j.tej.2014.08.008

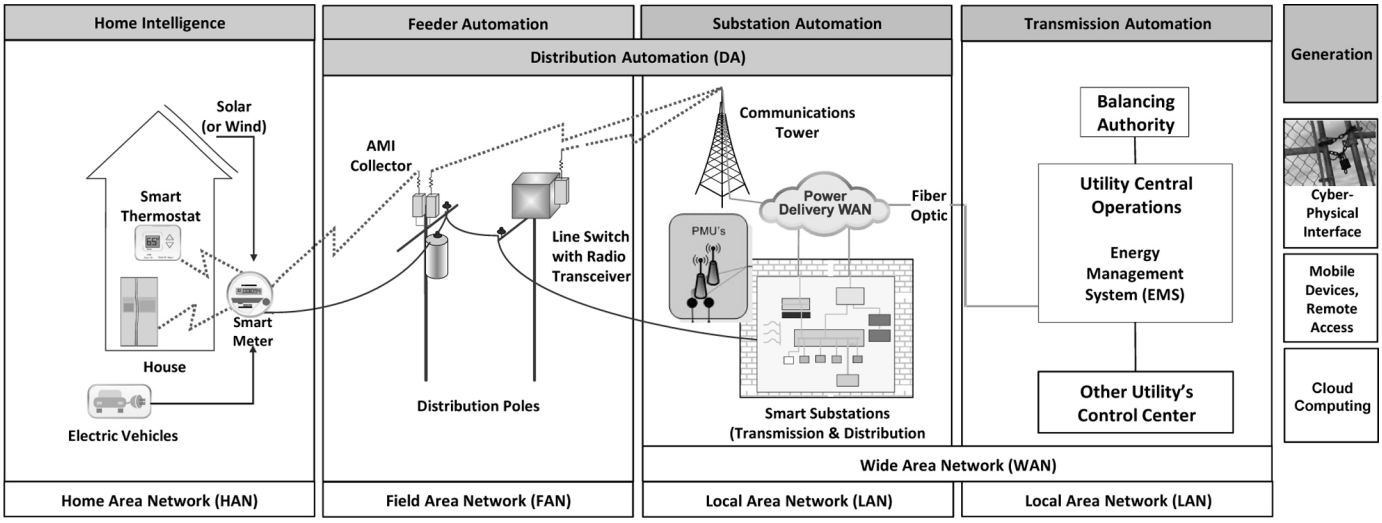


Figure 1: Power Grid Communications and Control Architecture

smart grid with the vision of surviving a cyber-incident while sustaining critical energy delivery functions.

II. Cybersecurity for the Power Grid – First, Do No Harm

Cybersecurity solutions for critical energy infrastructure are imperative for reliable energy delivery. In today's highly connected world, with an increasingly sophisticated cyber-threat, it is unrealistic to assume energy delivery systems are isolated or immune from compromise.

Cybersecurity for the power grid must be carefully engineered to not interfere with energy delivery functions. For instance, the power grid has some legacy devices that are decades old, with limited computational resources and communications bandwidth to support cybersecurity protections. Control and protection devices are widely distributed; some in unmanned, remote substations or on top of poles in publicly accessible areas. Access controls are important and must not jeopardize normal operations or emergency responses. Effective cybersecurity protections are necessary, and must work well within the operational environment of energy delivery systems.

The power grid transmits and distributes electrical power generated from primary fossil or renewable energy resources, such as coal or wind. Computers and networks manage, monitor, protect, and control the continuous, real-time delivery of electrical power (Figure 1).

A. Computers and networks manage, monitor, protect and control the power grid

Operation technology (OT) computers and networks for energy delivery systems allow operators to maintain situational awareness, perform economic dispatch of energy resources, plan for contingencies, and balance generation with load in real time. These capabilities are often provided by an energy management system (EMS) that resides in a utility control center and performs state estimation, contingency analysis and automatic generation control (AGC). The EMS receives data from a supervisory control and data acquisition (SCADA) system that acquires power system operating measurements every two to five seconds from specialized devices in substations.

The EMS state estimator uses SCADA data, data conveyed through the Inter-Control Center Communication Protocol (ICCP) from other utility's control centers, and the laws of physics to estimate the operational state of the power grid every few minutes. This information provides operators with the situational awareness to make informed decisions, such as

http://dx.doi.org/10.1016/j.tej.2014.08.008

optimized power flow for economic and efficient generation dispatch. State estimators also detect and reject corrupted data from malfunctioning sensors. New methods, such as Security-Oriented Cyber-Physical State Estimation (SCPSE), are being developed to detect data that have been maliciously compromised with the intent to misrepresent grid operations (Zonouz et al., 2012).

The EMS performs real-time contingency analysis to anticipate grid instabilities that might result from a major grid component failure, such as the loss of a generator or transmission line. This analysis shows how power grid operating conditions could evolve in response to the loss of particular components at that moment and supports planning to ensure that grid operating limits would not be violated if such a contingency were to occur. Automated remedial action schemes (RASs) or special protection systems (SPS) ensure the grid remains stable even if a major component is unexpectedly lost. From a cybersecurity perspective, physical consequences of malicious commands can be modeled as contingencies to assess risk and develop mitigations well in advance.

The AGC allows a balancing authority to adjust generation to meet power demand in real time as load connects to and disconnects from the grid. Protection and control devices, such as intelligent electronic devices (IEDs) with embedded operating systems, are used at the generation, transmission, and increasingly the distribution levels. These devices measure and automatically react to grid operating conditions within milliseconds, a few cycles at 60 Hz, to prevent equipment from exceeding safe operating limits and keep the grid stable.

From a cybersecurity perspective, physical consequences of malicious commands can be modeled as contingencies to assess risk and develop mitigations well in advance.

There are nearly 100 ANSI standard device numbers describing features of different protective devices (IEEE Std C37.2-2008). Examples include devices that monitor phase differences and protect generators from loss of synchronization with the grid; protect transmission lines from exceeding rated current carrying capacity; monitor over or under frequency conditions, over or under voltage conditions, implement compensating voltage control when needed or, in an emergency, prioritized load shedding to protect grid stability. Capabilities are in place today, and continue to improve, that secure these devices from cyber-exploitation by adversaries seeking to misuse them, causing them to disrupt, instead of protect, power flow.

B. Cybersecurity protections are imperative, and must not interfere with energy delivery functions

Cybersecurity for the smart grid is bringing together two communities that until recently have spoken different languages. Information technology (IT) speaks the language of computers and networks that support utility business administrative processes. OT speaks the language of electronic devices with embedded operating systems streamlined to support energy delivery functions, and operational networks. Utility IT and OT differ in important ways, making cybersecurity protections that are appropriate for one often inappropriate, and even potentially damaging, for the other. However, each has benefits that can be gained from the other.

IT is increasingly being adapted to support OT in utilities so that operating systems, computer platforms, and networks commonly used in IT are now found in some OT architectures. Segmented communication paths are architected to provide business IT systems with secure access to selected OT data, only when needed. The increasing use of IT computers and networks in

 http://dx.doi.org/10.1016/j.tej.2014.08.008

ABB's Collaborative Defense Project

ABB is collaborating with the University of Illinois at Urbana-Champaign (UIUC) on R&D for protection and control devices to recognize and prevent cyber-activity that could jeopardize grid operations. The team is developing IEC 61850 distributed security extensions so substation devices can collaboratively validate that inputs, configuration changes, or power system data make sense within the current operational state of the power grid (Nuqui and Tang, 2009).

OT architectures brings the need to protect these systems against malware developed to attack IT systems.

III. DOE and the Energy Sector Are Partnering to Keep the Smart Grid Reliable and Secure

Industry and government partnered to develop the *Roadmap to Achieve Energy Delivery Systems Cybersecurity*, updated in 2011 (Controlsystemsroadmap.net, 2011). The *Roadmap* presents the energy sector's strategy and set of short-, mid-, and long-term milestones supporting the vision of resilient energy delivery systems that can survive a cyber-incident while sustaining critical functions.

The DOE Office of Electricity Delivery and Energy Reliability (OE) Cybersecurity for Energy Delivery Systems (CEDS) program partners with the energy sector to research and develop cybersecurity protections tailored to the needs of energy delivery systems, aligned with the *Roadmap*. The goal of CEDS is to enhance the reliability and resiliency of the nation's energy infrastructure by reducing the risk that energy delivery could be disrupted by cyber-attacks.

A. Designing cybersecurity into the smart grid at its foundation

Cybersecurity is a cornerstone of the Smart Grid Investment Grants (SGIG) and Smart Grid Demonstration Projects (SGDP) funded by the American Recovery and Reinvestment Act (ARRA) of 2009. Specifically, $3.4 billion of federal funding was allocated to 99 SGIG projects and $600 million allocated to SGDP, with at least 50 percent cost share contributed by recipients. The projects have deployed advanced power system technologies nationwide, including more than 1,000 phasor measurement units (PMUs) and 15 million smart meters in an advanced metering infrastructure (AMI) (Https, 2014b; SmartGrid.gov, 2014). Other outcomes include integrating the advanced technologies of distribution automation (DA) and distributed energy resources (DER). Recipients developed and implemented cybersecurity plans to prevent broad-based systemic failures in the event of a cybersecurity breach.

The cybersecurity plans were informed by the *Roadmap*, the North American Electric Reliability Corporation (NERC) Cybersecurity Infrastructure Protection (CIP) standards, and the NISTIR-7628 among others. DOE worked in partnership with recipients, provided subject matter expertise, and performed site visits to assess cybersecurity plan implementation. DOE hosted two workshops between 2011 and 2013 to review the cybersecurity status of the projects and share lessons learned, such as good industry practices and areas for improvement. For more information, visit www.smartgrid.gov.

B. Phasor measurement units bring unprecedented wide-area visibility of grid operations

PMUs measure synchrophasors of current, frequency, and voltage 30 times each second, or more frequently, revealing dynamic and transient behavior, such as electromechanical grid oscillations with characteristic frequencies of tenths of Hz. PMU measurements are time-synchronized, often through the global positioning system (GPS), and can be time-aligned with microsecond precision across extensive geographic territories. This provides unprecedented visibility into the wide area grid operations, power system state, voltage stability and islanding

http://dx.doi.org/10.1016/j.tej.2014.08.008

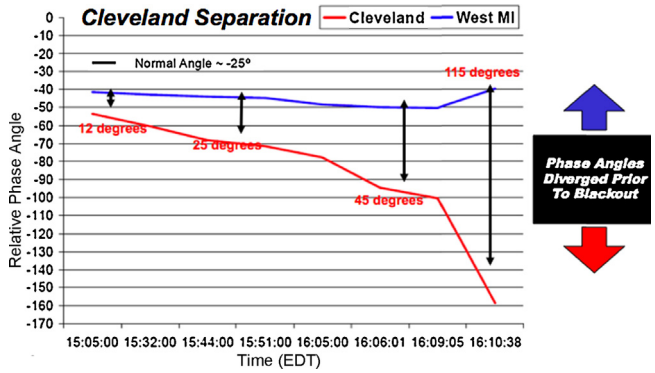


Figure 2: Lack of Wide-Area Visibility Contributed to 2003 Blackout (Cummings, 2005)

conditions, giving real-time indications of grid instabilities that may originate in distant regions. **Figure 2** shows a simulated angular separation during the Aug. 14, 2003, Northeast Blackout where real-time wide-area visibility could have helped prevent a power outage. PMU measurements, and other energy sector data, are being exchanged between utilities with enhanced security using the Secure Information Exchange Gateway (SIEGate), developed in a partnership led by the Grid Protection Alliance (GPA) (Grid Protection Alliance, 2011).

The GPS signals often used to time-synchronize PMU measurements across wide regions have low signal strength and can be jammed or spoofed (Jiang et al., 2013; NERC.com, 2014). Jamming results in a loss of signal that can be mitigated for short intervals by the receiver's internal clock, while spoofing is the intentional adjustment of the time reference provided by GPS. Multiple receivers that cross-check with each other is one of several methods (Liang et al., 2014) available to protect the integrity of precise time synchronization for the power grid. The Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) (Tcipg.org, 2014a), an academic collaboration that performs research to reduce the risk of a cyber-incident disrupting energy delivery, is developing further mitigations. Also, other time synchronization methods are being explored, such as network-based methods, including standards-based approaches to provide interoperability across vendor solutions.

Bonneville Power Administration's (BPA's) Synchrophasor Network

The BPA synchrophasor network received a Global Energy Award from Platts for grid optimization in 2013. BPA is part of the ARRA-funded Western Interconnection Synchrophasor Program, a partnership of 19 utilities to provide real-time visibility of the western power system covering 14 states, two Canadian provinces, and a portion of the Baja Peninsula in Mexico. BPA uses a dedicated secure network to share synchrophasor data with 10 other utilities, gaining visibility of the interconnection operating conditions well beyond the agency's borders. BPA collects 137,000 measurements from across the grid every second and analyzes these data in real time to alert dispatchers when the power system is at risk (Energy.gov, 2014a).

C. Advanced metering infrastructure enables faster outage restoration

Advanced metering infrastructure (AMI) opens two-way communications between the energy user and the utility. This enables informed, economic energy-usage decisions and hastens the location and recovery of distribution-level outages, further enabled by DA. Prearranged demand response (DR) agreements with energy consumers allow for reduced consumption on distribution feeders through dynamic load control during periods of system peak energy usage to avoid emergency voltage reduction. Cost-effective advanced meter reading (AMR) decreases the need for ''truck rolls'' and saves operational costs. Cybersecurity protections are in place, and being further developed, to protect the security and privacy of these data.

Smart meters connect a home area network (HAN) with Zigbee (and Smart Energy Profile (SEP) 1.x) enabled home devices, to a neighborhood area network (NAN). The National Electric Sector Cybersecurity Organization Resource

 http://dx.doi.org/10.1016/j.tej.2014.08.008

(NESCOR) (Smartgrid.epri.com, 2014) has developed a ''SEP 1.x Summary and Analysis (Smartgrid.epri.com, 2003a)'' that provides guidance to further strengthen AMI and HAN cybersecurity protections.

D. Distribution automation enables grid self-healing

In addition to easing outage restoration, DA can avoid additional disruptions by using automated feeder switches to isolate critical facilities and minimize equipment damage.

E. Energy storage provides contingency reserves for grid stability

Distribution automation eases the integration of DER, which include distribution-level equipment and systems that can actively participate in power system operations. Examples are load, plug-in electric vehicles (PEV) with smart chargers, and energy storage that eases the integration of intermittent renewable energy resources, such as wind and solar. NESCOR has developed a report that describes the cybersecurity requirements for DER, reflecting DER functions in the smart grid and taking into account variations of DER architectures (Smartgrid.epri.com, 2003b).

Applied Communication Sciences (ACS) Real-Time Anomaly and Intrusion Detection for AMI and DA

ACS is partnering with Sacramento Municipal Utility District (SMUD) to address security, operations, and engineering needs in the self-forming mesh networks beyond the wireless gateways. For AMI, the project works to ensure that customer privacy is preserved and customer data is protected in automated meter reads. For DA, the project helps utilities continuously validate over-the-air security controls, mitigate supply chain cyber-threats, and monitor the field network health, performance, and security in real-time. Visit www.controlsystemsroadmap.net for more.

In 2009, as part of its ARRA grant proposal, SMUD stated a desire to deploy a wireless RF intrusion detection system for its yet-to-be-deployed smart meter network. When the time came to begin the wireless Intrusion Detection System (IDS) project in early 2012, there were no commercial products available to provide the desired functionality. So SMUD partnered with ACS to jointly develop a solution. The project went live in spring of 2013, and although this work is not yet considered complete, SMUD has already realized a number of benefits from this effort that have further strengthened existing cybersecurity protections and innovated new capabilities as well. They also report lateral benefits from the system, such as enhanced working relationships between information security, the meter shop, and DA teams (Controlsystemsroadmap.net, 2014).

Consolidated Edison Company of New York (Con Edison) Expedites Recovery from Super Storm Sandy

Con Edison is deploying DA to operate resiliently against disruptions, reducing outages and hastening outage restoration. The company has expanded automated overhead switches by 35 percent, resulting in more than 17,000 avoided customer outages. During Hurricane Sandy, Con Edison avoided more than 100 truck rolls through automated operation of overhead circuits to minimize customer impact. Con Edison has also implemented SCADA systems with enhanced cybersecurity that reduce the risk of a cyber-attack.

IV. Advancing the State of the Art of Power Grid Cybersecurity

The following sections present insights of four SGIG recipients that are advancing the state of the art of power grid security by designing cybersecurity into the foundation of the smart grid.

A. Duke Energy Progress

Duke Energy Progress's EnergyWise initiatives leverage existing program/project management organizational structures, standards, and disciplines to manage for on-time, on-budget delivery while ensuring benefits realization. This includes the following activities and business drivers:

http://dx.doi.org/10.1016/j.tej.2014.08.008

- Deploy AMI that establishes a scalable platform for cost-effective advanced meter reading (AMR)-AMI migration and positions for dynamic rates;
- Deploy grid management functionality that replaces emergency voltage reduction with utility-side demand response capability for routine operational use;
- Deploy monitoring capability to critical transmission infrastructure for asset and demand management functionality;
- Deploy feeder automation to advance partial restoration capabilities, and
- Build an advanced analytics engine that forecasts, coordinates and models a comprehensive view of smart grid energy and efficiency capabilities.

The initiatives include a wide range of smart grid technologies. Figure 3 offers a list of the initiatives that challenged the normal approaches and work practices of operations technology (OT), information technology (IT), and supply chain professionals.

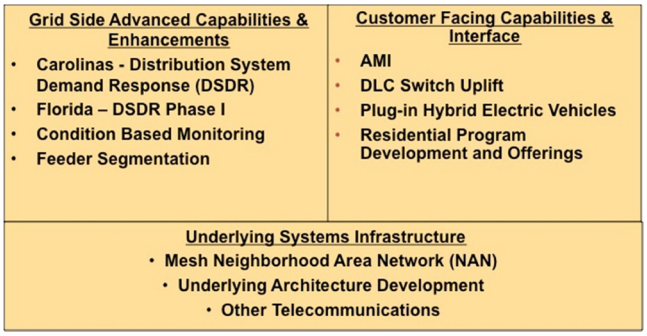


Figure 3: Duke Energy Progress's EnergyWise Initiatives

Duke Energy Progress's fundamental approach to cybersecurity leverages a simple defense-in-depth architecture including the principles of ''least privilege'' and default ''deny access'' controls. Through ongoing threat monitoring activities (including some paid threat monitoring and alerting services), we know that cybersecurity threats continue to increase in number, complexity, and level of impact. At the same time, business needs are driving requirements for increasing access and interoperability across enterprise applications, process computing environments, enterprise networks, and the Internet. These requirements are rooted in the need for sharing of data as a business enabler and increased leverage of automation and intelligent technologies being implemented. Many times these business needs are in direct conflict with security objectives, presenting unique challenges and driving the need to better leverage our existing risk management methodology. This business-risk balanced approach required further maturity of our risk management lifecycle so that more risk evaluation was performed during product selection, implementation, and post-deployment.

The operational technology and information technology collaboration is largely education and awareness of each other's perspective, so together the resulting solution best meets the business needs and provides adequate security. This alignment of skills drives thorough evaluation of the requirements, product capabilities and integration needed to provide the right capability for the business and security capabilities. To ensure communication and coordination, we developed a new Enterprise Architecture Review Process (EARP) and created a committee made up of OT and IT architects and engineers to provide standards, guidance, and governance to our project teams. These formal reviews (gates) require specific artifacts demonstrating adherence to standards and documented follow-up of issues, questions, and resolution of outstanding items. The success of this process has been so positive that some project teams are even soliciting additional EARP ''pre-gate'' reviews aimed at achieving understanding, guidance and consensus of the architecture review committee earlier than required in the formal process. Also, the new reference architecture artifacts created through the process have already paid off in efficiency gains as reuse opportunities have already been realized.

 http://dx.doi.org/10.1016/j.tej.2014.08.008

The OT, IT, and supply chain collaboration ensures that the right foundational capabilities (e.g. network security, authentication, monitoring, configuration management, etc.) are in the procured component or solution. Our Supply Chain Operating Framework includes specific collaboration in the following areas: purchasing, contracting, category strategies (roadmap and strategy sharing), supplier management, and performance monitoring. The recently released Cybersecurity Procurement Language for Energy Delivery Systems has also informed our efforts. (www.controlsystemsroadmap.net, 2014) There are many supply chain vulnerabilities we intend to mitigate through these enhanced processes and increased collaboration will mitigate supply chain vulnerabilities. Hardware integrity during manufacturing includes issues from chip integrity to (digital) birth certificates used in the initial setup and provisioning of new intelligent components as trusted hosts. Poor practices and inadequate planning of the deployment phase could introduce incomplete and/or incorrect implementation configurations, leaving components at risk. There are countless possibilities of substitution of corrupted components in transit, warehouses, and with distributors. Without adequate security controls, testing and verification, IT functions intended to surveil, disrupt, deny, degrade, compromise, or control the performance of a product or system could be introduced. Accidental quality defects or worse case, intentional corruption of components and systems intended to degrade, compromise, or control the system, create vulnerabilities through embedded malware, backdoors, Trojans, etc.

There are many supply chain vulnerabilities we intend to mitigate through these enhanced processes and increased collaboration.

Application vulnerabilities that could be avoided can result from poor coding practices and inadequate testing (e.g., Open Web Application Security Project Top 10 (Owasp.org, 2014), 2011 CWE/SANS Top 25 Most Dangerous Software Errors (Sans.org, 2014), etc.).

Through our engagement with DOE, NIST, and industry peers we further matured our architecture and design approaches to architect cybersecurity into the solution beginning at the concept stage. This ensures that major architectural decisions are influenced by the requirement to be secure and resilient. Even though we were already using numerous guidance documents and interoperability standards for all initiatives (e.g. DHS Cyber Security Procurement Language for Control Systems (USDHS, 2009), ISO/IEC 27000 series (Org, 2014), NIST 800 series (Csrc, 2014), IEEE (Standards.ieee.org, 2014), AMI-SEC (Osgug.ucaiug.org, 2014), etc.) we directly embedded key steps from the NISTIR 7628 (NIST, 2010) into our architecture and design processes. As part of the plan, ongoing cybersecurity evaluations are to be performed during the design and procurement, installation, commissioning, and the ongoing maintenance and support phases of the project. The strategies used at each project phase include these security-related activities:

- Design Phase: Security driven architecture and risk-balanced methodology based on current cybersecurity standards (ISO/NIST). Business impact analysis for disaster recovery. A lightweight, concise privacy impact analysis aimed at identifying sensitive information in the solution.
- Procurement Phase: Technical governance reviews, technology specific risk and vulnerability assessment, code review, and third-party evaluation or testing as required.
- Installation Phase: Change control, security testing and internal controls implementation.

  http://dx.doi.org/10.1016/j.tej.2014.08.008

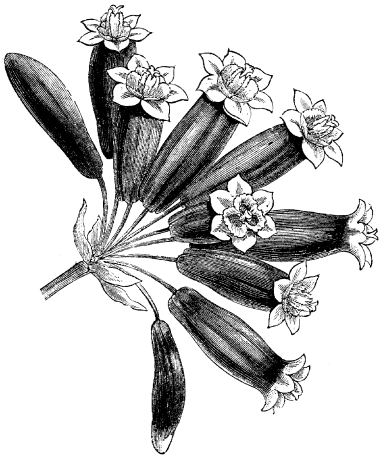
- Commissioning Phase: Training, procedure development, new procedure implementation, and acceptance checklist sign-off.
- Ongoing maintenance and support Phase: Monitoring, logging, alarming, incident and response management, lifecycle management, and system back-up.

Duke Energy Progress's GRID WAN is an example of how these processes manifest themselves in practice. GRID WAN is a dedicated wide area network employing secure gateways, encrypted VPNs, switches, routers, firewalls, and secure remote access to segregate and protect networks. This comprehensive solution supports all smart grid applications.

B. FirstEnergy

FirstEnergy's cybersecurity plan describes the responsibilities for implementing the FirstEnergy Smart Grid Modernization Initiative Cyber Security Program. The plan describes how FirstEnergy uses NIST 800-53 (NIST, 2009), FirstEnergy Cyber Security Programs (based on ISO standards and best practices), and FirstEnergy CIP Cyber Security Programs. The plan contains a description of FirstEnergy's defense-in-depth posture, business practices, cybersecurity programs and project lifecycle management to illustrate FirstEnergy's commitment to cybersecurity.

A number of risks were identified as a part of developing the plan. These risks include: physical access to smart meters and other devices exposed to the public, privacy concerns, and wireless transmission of data. In some cases, these risks required a new thought process and additional controls to be implemented for mitigation.



Many of the controls to mitigate identified vulnerabilities and risks were already in place at FirstEnergy. It is the goal of the plan to ensure that these controls are applied to the new technology deployed as part of the SGIG project. Processes such as project review, patching, and assessments are described as part of the ongoing project lifecycle.

The cybersecurity challenges FirstEnergy has experienced with the SGIG project are those experienced by most cybersecurity organizations. For instance, working with vendors to clarify the need to maintain a balance between proprietary communications and inspectability. For instance, vendors need to understand what is or isn't normal for smart meter communications, especially with regard to implementing the Amilyzer (see below). An additional challenge is the classic conflicting goals of functionality vs. security, i.e. how to make it work while ensuring it is secure. In most cases, this requires new best practices or innovations due to a bolting-on of security by vendors who have always considered physical security aspects, and must now also consider the cybersecurity aspects. Finally, metrics are a challenge. How do you quantify security testing success? Assessments work well to a degree, but is the answer that a device hasn't been exploited a real measure? Or has the vulnerability not been made known or discovered at the time.

Working through the cybersecurity aspects of the SGIG project, we have learned that we need to have an assurance of our engineers' and project managers' awareness of cybersecurity. They must be able to ask themselves, ''Is this a cybersecurity concern?'' Additionally, it is important to be involved in project meetings, to understand what is happening and when, in order to provide the necessary consulting to ensure cybersecurity concerns are addressed and controls are implemented. Vendors need to increasingly consider appropriate cybersecurity controls now.

http://dx.doi.org/10.1016/j.tej.2014.08.008

Utilities have been addressing these for some time, and it is encouraging that vendors have taken the initiative to develop more cybersecurity controls in their devices and update issues found in their software/firmware. These lessons learned offer several examples of how this project has contributed to advancing the state of the art for energy sector cybersecurity.

1. *Amilyzer*

In early 2012, FirstEnergy and researchers at TCIPG started collaborating on a new specification-based IDS system for smart meters called Amilyzer (Tcipg.org, 2014b). The software system passively monitors AMI traffic at the network, transport, and application layers to ensure that smart meters are running in a secure state and that their operations respect a specified security policy. This policy is derived from the electric sector failure scenarios defined by NESCOR (Smartgrid.epri.com, 2014). Amilyzer has been successfully deployed by FirstEnergy in a testing state to monitor a 12,000-meter AMI over the past year.

Amilyzer provides in-depth visibility over the traffic captured between the collection engines and meters. An important challenge has been to translate the large volume of low-level packets captured into high-level actionable information that security engineers can leverage to ensure the resiliency of the infrastructure. Being able to test Amilyzer on a live AMI has enabled the team to greatly improve the C12.22 packet dissection library and to develop a more robust system. The team is now working on finalizing a Web user interface to allow the security team to visualize periodic reports and to write custom IDS signatures. From a research

perspective, traffic analysis algorithms are now being developed to be able to gain better visibility over encrypted traffic without having to share decryption keys with the IDS sensors.

C. Northern Virginia Electric Cooperative

NOVEC recognized the value and the need for a formal, structured, approach to cybersecurity following the initial 2007 deployment of digital substation equipment, generally described with the common term of ''intelligent electronic devices (IEDs).'' While the operational benefits of the technology were realized early on, the potential vulnerability of digital equipment, via the SCADA and substation networks, to unauthorized access and control became a recognized concern.

The SGIG program provided an impetus to elevate cybersecurity to a higher level of active functional management. This initiative takes place within an integrated approach to protect the electric distribution system as well as the key interfacing business systems. The SGIG process recognized the various emerging standards and cyber principles which have provided guidance to develop an effective framework and implementation plan. Some of these guidance documents and standards referenced in the development of NOVEC's plan included *21 Steps to Improve Cyber Security of SCADA Networks* (Energy.gov, 2014b), NIST cybersecurity and interoperability standards, NERC CIP standards, and others.

A guiding principle has been to ensure physical separation of the substation and SCADA networks from the corporate enterprise network and, indirectly, the Internet. NOVEC adheres to the ''Do no harm'' principle by carefully selecting security hardware and software tools, systems, and protocols that will not compromise the ultimate purpose of the IED's and automation system, which is to sustain NOVEC's very high level of system reliability.

http://dx.doi.org/10.1016/j.tej.2014.08.008

Implementation efforts to date have strengthened the security perimeter of the SCADA network, created stronger authorized access controls, stronger remote access controls, and stronger physical security.

Early in NOVEC's automation program we recognized the vital role that a secure communications system plays. NOVEC relies on its private fiber optics-based communications network both for operational reliability as well as security and it has continued to expand the fiber network which currently connects 85 percent of its substations, supplemented with licensed microwave for the remainder. Communications with distribution automation components rely on a combination of fiber and third-party commercial services to which layered security measures are applied prior to receiving transmitted data into the SCADA network.

NOVEC's commitment to cybersecurity includes a vigilant effort to protect the distribution system and power plants under our purview. Periodic security assessments including penetration testing are one component of the active cybersecurity program. Programmatic methods of monitoring, recognizing and assessing vulnerabilities, a disciplined adherence to procedures, followed by appropriate responses, will help to effectively mitigate the impact of potential threats.

V. Evolving the Reliable Grid of the Past into the Reliable Grid of the Future

DOE and the energy sector are partnering to manage cyber-risk, keeping energy delivery reliable as smart grid technologies modernize the power grid. Each day, the sector is coming closer to the *Roadmap* vision that by 2020 resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber-incident while sustaining critical functions (Controlsystemsroadmap.net, 2011).■

References

Controlsystemsroadmap.net, 2011. Roadmap to Achieve Energy Delivery Systems Cybersecurity. Available from: https://www.controlsystemsroadmap.net/ieRoadmap%20Documents/roadmap.pdf (accessed 24.06.14).

Controlsystemsroadmap.net, 2014. Home. Available from: http://www.controlsystemsroadmap.net (accessed 24.06.14).

Csrc.nist.gov, 2014. NIST Computer Security Publications – NIST Special Publications (SPs). Available from: http://csrc.nist.gov/publications/PubsSPs.html (accessed 25.06.14).

Cummings, R.W., 2005, June 7. Blackout Dynamics & Phasor Measurements. ocpresentations_605.zip www.nerc.com.

Energy.gov, 2014a. BPA Wins Platts Global Energy Award for Grid Optimization. Available from: http://energy.gov/oe/articles/bpa-wins-platts-global-energy-award-grid-optimization (accessed 24.06.14).

Energy.gov, 2014b. 21 Steps to Improve Cyber Security of SCADA Networks |Department of Energy. Available from: http://energy.gov/oe/downloads/21-steps-improve-cyber-security-scada-network (accessed 24.06.14).

http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=4639522&queryText%3DIEEE+Std+C37.2%E2%84%A2-2008 (accessed 24.06.14).

https://www.smartgrid.gov/sites/default/files/doc/files/Synchrophasor%20Report%2008%2009%202013%20DOE%20%282%29%20version_0.pdf (accessed 24.06.14).

https://www.gridprotectionalliance.org/pdf/SIEGate_Overview_Flyer.pdf (accessed 24.06.14).

Jiang, X., Zhang, J., Harding, B.J., Makela, J.J., Dominguez-Garcia, A.D., 2013. Spoofing GPS receiver clock offset of phasor measurement units. IEEE Trans. Power Syst. 28 (3) 3253–3262.

Heng, L., Makela, J., Dominguez-Garcia, A., Bobba, R., Sanders, W., Gao, G.X., 2014. Reliable GPS-based timing for power system applications: a multi-layered multi-receiver approach. In: Proceedings of the 2014 IEEE Power and Energy Conference at Illinois (IEEE PECI 2014), Champaign, IL, February.

NERC.com, 2014. Extended Loss of GPS Impact and Reliabilty|NERC.com. Available from: http://www.nerc.com/docs/escc/PNT%20-%20Power%20Systems%20V19.pdf (accessed 24.06.14).

National Institute of Standards and Technology (NIST), 2009. Recommended Security Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53, Revision 3. NIST, Gaithersburg, MD, In: http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updatederrata_05-01-2010.pdf.

National Institute of Standards and Technology (NIST), 2010. Guidelines for Smart Grid Cybersecurity. NIST Interagency Report (IR) 7628. NIST, Gaithersburg, MD, In: http://csrc.nist.gov/publications/PubsNISTIRs.html.

Nuqui, R.F., Tang, L., 2009, December 3. Collaborative Defense of Energy Distribution Protection and Control Devices. US Patent Application 12/472,532.

 http://dx.doi.org/10.1016/j.tej.2014.08.008

27000.org, 2014. ISO 27000 – ISO 27001 and ISO 27002 Standards. Available from: http://www.27000.org/ (accessed 25.06.14).
Osgug.ucaiug.org, 2014. Home – AMI-SEC. Available from: http://osgug.ucaiug.org/utilisec/amisec/default.aspx (accessed 25.06.14).
Owasp.org, 2014. Top 10 2013-Top 10 – OWASP. Available from: https://www.owasp.org/index.php/Top_10_2013-Top_10 (accessed 25.06.14).
Sans.org, 2014. SANS: CWE/SANS TOP 25 Most Dangerous Software Errors. Available from: http://www.sans.org/top25-software-errors/ (accessed 25.06.14).
Smartgrid.epri.com, 2014. EPRI|SmartGrid Resource Center > NESCOR. Available from: http://www.smartgrid.epri.com/nescor.aspx (accessed 26.06.14).
Smartgrid.epri.com, 2003a. Smart Energy Profile (SEP) 1.x Summary and Analysis| EPRI. Available from: http://www.smartgrid.epri.com/doc/SEP%201%20x%2003-21-12%20posting.pdf (accessed 24.06.14).
Smartgrid.epri.com, 2003b. Cyber Security for DER Systems| EPRI. Available from: http://www.smartgrid.epri.com/doc/SEP%201%20x%2003-21-12%20posting.pdf (accessed 24.06.14).
Smartgrid.epri.com, 2014. EPRI|SmartGrid Resource Center > NESCOR. Available from: http://www.smartgrid.epri.com/nescor.aspx (accessed 24.06.14).
Smartgrid.gov, 2014. Smart Grid Investment Grant Program SmartGrid.gov. Available from: https://www.smartgrid.gov/recovery_act/overview/smart_grid_investment_grant_program (accessed 24.06.14).
Standards.ieee.org, 2014. IEEE-SA – The IEEE Standards Association – Home. Available from: http://standards.ieee.org/ (accessed 25.06.14).
Tcipg.org, 2014a. Home|TCIPG: Trustworthy Cyber Infrastructure for the Power Grid. Available from: http://tcipg.org/ (accessed 24.06.14).
Tcipg.org, 2014b. Amilyzer|TCIPG: Trustworthy Cyber Infrastructure for the Power Grid. Available from: http://tcipg.org/amilyzer (accessed 26.06.14).
U.S. Department of Homeland Security (DHS), 2009. Department of Homeland Security: Cyber Security Procurement Language for Control Systems. DHS, Washington, DC, In: http://ics-cert.uscert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809.pdf.
Zonouz, S., Rogers, K.M., Berthier, R., Bobba, R.B., Sanders, W.H., Overbye, T.J., 2012. SCPSE: security-oriented cyber-physical state estimation for power grid critical infrastructures. IEEE Trans. Smart Grid 3 (December (4)) , http://dx.doi.org/10.1109/TSG.2012.2217762, pp. 1790, 1799.

The SGIG program provided an impetus to elevate cybersecurity to a higher level of active functional management.