Quadrennial Technology Review 2015

Chapter 3: Enabling Modernization of the Electric Power System

Technology Assessments

Cyber and Physical Security

Designs, Architectures, and Concepts

Electric Energy Storage

Flexible and Distributed Energy Resources

Measurements, Communications, and Controls

Transmission and Distribution Components

U.S. DEPARTMENT OF
ENERGY

Quadrennial Technology Review 2015

Cyber and Physical Security

Chapter 3: Technology Assessments

Introduction

As understanding of the threats facing the operation, components, and subsystems of the electric power system is gained, a need has emerged for improvements in grid security and resilience. The focus on resiliency implies that threats will not go away and that some attacks, in addition to natural events, will be carried out successfully. The objective is for the system and associated subsystems to be designed and operated in such a way that critical functions will continue during and after an event—maintaining reliability and continued service to customers despite withstanding the loss of more than one key asset. Threats can be composed of many different factors, including intentional bad actors, nation states, natural disasters, and inadvertent human error. As a result, a comprehensive strategy is needed to ensure the nation's electric power system is adequately protected against all hazards.

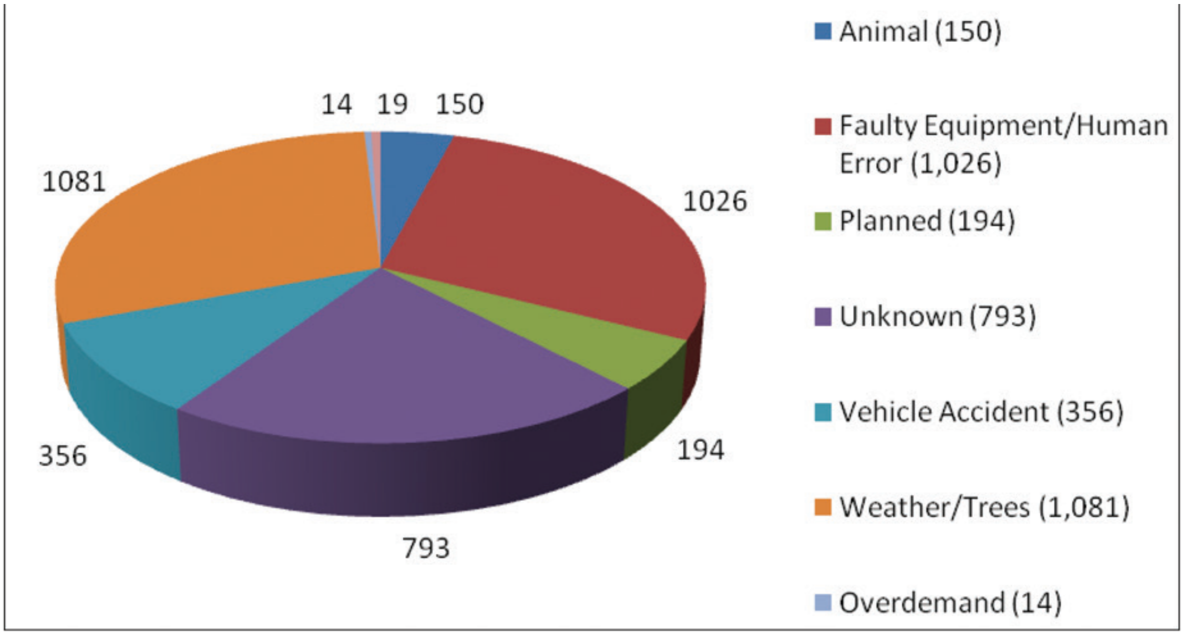
As technology has developed, so have the conveniences to our society, and with convenience comes reliance. Our society and economy have become dependent on computers, instantaneous communications, climate-controlled buildings, and much more, all of which require a stable and reliable supply of electricity. An unreliable electric grid, attributable to any reason, will contribute to losses at the customer and utility levels. Direct costs of power outages could include lost revenue, lost inventory, penalties, and lost wages to employees. Indirect costs may include lost business opportunities, declines in stock value, loss of customer goodwill, driving business to competitors, and low employee morale. Research shows that a majority of these costs are due to the frequency of momentary outages rather than the duration of a sustained event.[1] However, wide-area outage costs can be staggering; estimates of the August 14, 2003, blackout ranged from $4.5 to $12 billion in lost economic activity.[2] Even smaller-scale incidents that do not result in an outage can be costly, as evidenced by the recent physical attack on the Metcalf substation, which cost an estimated $15 million to repair.

While the electric power industry and the North American Reliability Corporation (NERC) have mandatory reliability standards that help provide a basis for grid reliability and resilience, grid modernization is introducing new technologies that do not have well-defined standards. Advanced information and communications technologies are being developed and deployed at a rapid pace to enable new system capabilities and to support the integration of variable and distributed energy resources. Continued advances in energy delivery technologies and the use of legacy devices in ways not previously envisioned are taking place within an advancing cyber threat landscape. Since 2010, the international energy cybersecurity environment has experienced an increase in intelligent cyber-attacks. The sophistication and effectiveness of this new era of malware mark a significant change in state actor-level threats to the energy sector and the U.S. economy. There is also evidence that nation states are increasing cyber-spying and attacks on U.S. utilities and equipment suppliers.[3] These threats demand energy delivery control systems that are secure in every aspect and resilient during a cyber-incident.

Simultaneously, the increased frequency and intensity of extreme weather events and potential attacks on electrical infrastructure require more careful consideration of physical security. Attacks on electric power systems are not new; utilities have faced physical threats ranging from copper theft at substations to the occasional sportsman shooting insulators or conductors. The Metcalf substation attack in 2013 gained national attention because of the apparent military tactics used. However, it is important to consider the source of outages that the electric industry faces annually—theft and vandalism rank fairly low when compared with outages caused by weather, faulty equipment, or unknown circumstances, as illustrated in Figure 3.A.1. Utilities will only adopt physical security measures that align with their risk management strategy; hardening and protecting the entire electric power system—with over 5,800 major power plants, 55,000 substations, and over 674,000 miles of high voltage transmission lines[4,5]—is impractical.

Figure 3.A.1 2014 Reported Power Outages by Cause (Grouped into Eight Possible Causes)[6]

Credit: Eaton



Note: Each power outage was grouped into one of eight possible causes. The number adjacent to the pie piece is the number of outages attributable to that cause.

As technology advances in the electricity sector, the distinction between the cyber and physical domains is shrinking and becoming more interdependent. It should also be acknowledged that the technologies being deployed are significantly diverse and organizations' cybersecurity sophistication ranges from essentially none to highly advance. Electricity cyber and physical security innovations will be required to address a multi-threat environment, including cyber-physical interactions. Because threats will not diminish, it is important that the future electric power system be designed and operated in such a way that it can continue its critical functions after an attack. It is also important that newly developed measures do not interfere with the energy delivery functions of the devices and components they are meant to protect.

Research and development (R&D) efforts for security will need to be industry-driven, field-proven, scalable, interoperable, upgradeable, and commercially available. Solutions will also need to take into consideration the balance between the risks an entity is willing to accept and the risks it must address. Inherent to security approaches is a full life-cycle assessment of technologies, including procurement aspects. Other aspects to consider are social, cultural, and human factors that must be addressed to support the timely and effective planning, response, and restoration processes when there is a "human in the loop." Based on recommendations developed by energy asset owners and operators, suppliers, government entities, national laboratories, and academics, security activities should focus on the following:

- Building a culture of security
- Assessing and monitoring risk
- Developing and implementing new protective measures to reduce risk
- Managing incidents
- Sustaining security improvements

The objective of these activities is to position the energy sector at an advantage over adversaries and reduce the risk that an incident will result in disruption of electricity delivery. The future energy sector security endeavors will be required to address a multi-threat environment with a multidisciplinary and multi-domain approach in order to address the convergence of energy delivery systems.

Within this complex environment, the resilience of a system will be influenced by the costs and benefits associated with the particular solutions an entity is willing to adopt. One component in facilitating improved resilience is well-informed risk assessments. Several efforts are currently underway in the federal and private sectors to improve information sharing and threat analysis capabilities that will aid utilities in these assessments. To ensure a resilient nation, academics, national laboratories, and vendors must set as a priority the dissemination of available security technologies and capabilities that have been thoroughly researched and developed.

While resilience metrics for control systems that manage the grid are still being prototyped,[7] much more effort is needed to adequately assess system reliability and resilience. Energy delivery systems are very complex and can interact across electricity, oil, and natural gas assets that are geographically dispersed yet connected by physical systems and communications networks. Therefore, improved understanding of interdependencies within the electric sector and across the nation's critical infrastructure sectors is critical for security. Energy infrastructure provides fuel and electricity to the country and in turn depends on its transportation, information technology, communications, finance, and government infrastructures to function.[8]

Cybersecurity

Cyber security for energy delivery systems is often divided into measures for systems comprised of operational technology (OT) and information technology (IT) to highlight key differences. Operational systems transfer data and commands that are critical to operating and protecting the grid itself and require operators and engineers to design, run, and maintain the function of the grid. Information systems typically are used to support business, human resources, and other non-operational functions that can be maintained by IT professionals. OT systems are often in place much longer than IT systems, have vulnerabilities related to legacy technologies,[9] and may have limited digital capabilities. Because the life cycle of OT systems is longer, costs associated with upgrading to newer technologies are often higher and harder to justify for the sake of addressing emerging threats, which have a much shorter life cycle. Because modern OT systems are often digital versions of the analog systems they replace, carryover weaknesses—such as lacking the ability to anticipate and manage the risk of failures—persist. OT systems also have differing uptime requirements (often expected to run 24/7 without incident) and data communications requirements than their IT system counterparts. While the speed and volume of network traffic in OT systems can be much less than for a corporate IT network, the timing and packet loss requirements can be much more stringent.

Data accuracy and integrity are important for both IT and OT systems, but an important distinction is the high-speed data transfers needed for reliable electricity operations. Protection schemes, especially wide-area protection, require precise timing and therefore cannot tolerate the latency that could be injected by encryption or other security measures. Although encryption technologies continue to improve, usage of traditional encryption in the OT environment may introduce unwanted network delays and losses that may adversely affect operational systems. New protection methods and technologies are likely needed to accommodate changing requirements for speed, volume, and latency. Some R&D topics related to new protection methods and technologies include communications architectures for OT that provide the basis for adaptive responses or the ability to incorporate more distributed components for increased agility and robustness. Additional avenues for research might focus on optimizing the human interface with the OT environments to both reduce human error and increase the efficiency of response to events.

Another key distinction between these two types of systems is their maintenance. Unlike many IT patches that can be updated frequently, OT patches and upgrades are only installed after extensive testing and validation by the vendor and utility, normally planned weeks or months in advance, to ensure that the change does not jeopardize operations. Due to the high uptime requirements of OT systems, rebooting to see if issues clear is not an option; however, IT systems are often rebooted for maintenance purposes. There are currently technologies being developed that allow for "on-the-fly" upgrades to OT systems with little to no downtime. As these technologies evolve, there will be an increasing need to consider the collaboration and interactions between these two types of systems. This evolution will present its own security challenges.

Basic parameters and objectives for effective cybersecurity R&D, identified by the National Institute of Standards and Technology (NIST), are shown in Table 3.A.1.[10]

NIST describes cyber-physical systems as "smart systems that encompass computational (i.e., hardware and software) and physical components, seamlessly integrated and closely interacting to sense the changing state of the real world."[11] Nowhere is the cyber-physical interface more critical than in the electric grid. For the electricity sector, this term is most commonly linked to "smart grid" technology but has recently expanded to include smart building technology and the entire scope of connected devices collectively known as the Internet of Things (IoT). The introduction of new intelligent, connected devices and components certainly increases the

Table 3.A.1 Cybersecurity R&D Parameters

R&D Parameters	Objectives
Time Latency	■ ≤4 milliseconds for protective relaying ■ Sub-seconds for transmission wide-area situational awareness monitoring ■ Seconds for substation and feeder supervisory control and data acquisition data ■ Minutes for monitoring noncritical equipment and some market pricing information ■ Hours for meter reading and longer-term market pricing information ■ Days/weeks/months for collecting long-term data, such as power quality information
Integrity Assurances	■ Data has not been modified without authorization. ■ Source of data is authenticated. ■ Time stamp associated with the data is known and authenticated. ■ Quality of data is known and authenticated.
Confidentiality	■ Privacy of customer information ■ Electric market information ■ General corporate information, such as payroll and strategic plans

number of potential targets of cyber-attacks. However, it is not clear that the distribution of intelligence across all these points makes the overall grid more vulnerable; wider distribution of intelligence may actually increase overall system resilience by increasing the number of necessary targets to achieve the same result as if the information were concentrated in one location. Another dimension of this evolving cyber-physical paradigm is that both utility personnel and customers can interact with the system. The opportunities and challenges associated with cyber-physical systems are a growing area that requires strong designed-in security to ensure trustworthy systems for all those that interact with them.

As more automation is installed for building environmental control and more opportunities become realized for demand reduction and distributed generation, it is possible that all these various cyber-physical systems will merge without sufficient coordination. The potential for an unintended/unsecure interface may develop at the customer level that would allow access to distribution-level or transmission-level assets and systems. For example, wireless- or smart phone-based applications that remotely control smart devices/systems or connect environmental controls to demand reduction technology and building IT systems can pose vulnerabilities. Identification of potential interfaces that could be exploited and technology solutions for security at all levels is needed.

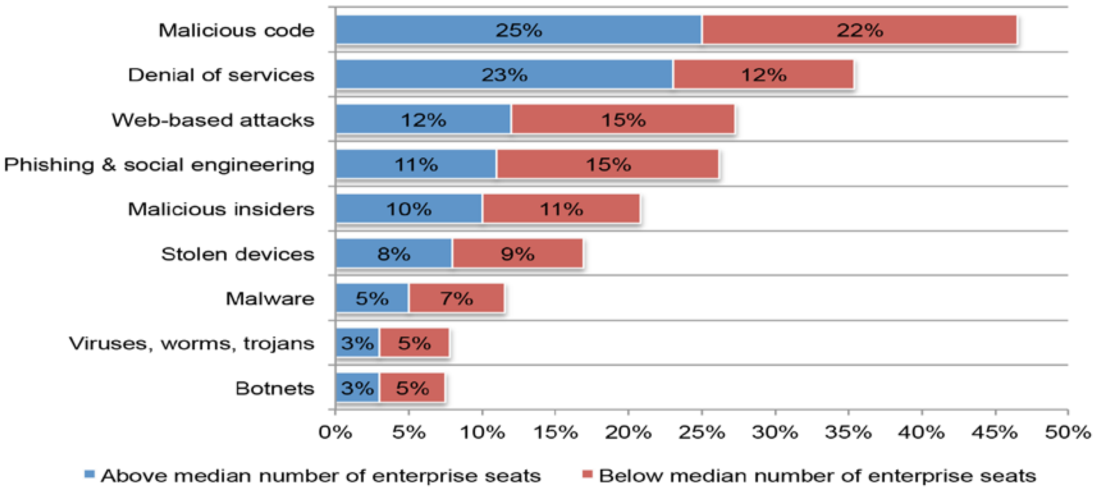
Assessing the current state of cyber security in the energy sector presents a complex issue for numerous reasons. Companies, in part, define their own level of risk acceptance, choose equipment based on acceptable levels of risk, and upgrade or patch equipment accordingly. Naturally, risk tolerance, installed equipment, technologies, procedures, and personnel qualifications will vary across the electricity sector, which has over 3,000 utilities. While critical infrastructure protection standards for transmission system entities exist, distribution system entities are regulated by individual states and municipalities, with no common standard for cyber security. Adding to this complexity is the dynamic threat environment that the electricity sector faces; solutions can become obsolete by the next discovered malware or exploit. Attention should be given to reactive and adaptive methods that focus on detecting the emergence of malicious behavior and rapid remediation.

The financial cost of cyber-incidents on the energy sector can consist of many factors: the direct impact to the utility; the indirect impact to the customers served by the utility, should there be an outage (factoring in extent and duration); and tertiary impacts to the customers. Estimating the potential cost is more difficult than a simple algebraic equation, because components of the equation cannot be measured with precision and the factors involved change drastically and frequently. While the potential impact of cyber-incidents and attacks on the grid is extremely difficult to quantify, the Ponemon Institute reports cyber-crime in the energy and utility sector costs approximately $20 million annually, as illustrated in Figure 3.A.2. Development of a cost analysis tool for cybersecurity events may be useful to the industry. Quantifying the real costs from everyday intrusions, including downtime and staff costs for incident response and recovery, would help entities forecast potential costs of future attacks and justify the need for increased security measures and research. Another consideration would be to develop higher-level metrics for economic impacts—for example, production capacity lost (reduced sales) or operational costs (inefficiencies) related to cyber-incidents. All of these considerations should seek to correlate reliability benefit to consequence wherever possible.

In addition to incidents that impact IT systems, there is evidence of growing threats to OT systems. Reports from the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) indicate increased targeting of the energy sector,[13] with one showing 151 out of 256 reported cyber-incidents occurring in the energy sector.[14] Although primarily anecdotal, the Aurora Project provided a demonstration of the potential effect a successful cyber-attack can have on electrical generating equipment.[15] Cybersecurity experts further agree that the adoption of new digital technologies, such as smart meters and improved controls with renewables and other power sources, can challenge reliability because there are more information and computer technology components, and thus vulnerabilities, being introduced in the grid.

Figure 3.A.2 Average Annualized Cost of Cyber-crime Impacts by Industry Sector (X-Axis is millions USD)[12]

Credit: Hewlett Packard Enterprises



To help guide public and private activities to enhance cyber security across the energy sector, the Department of Energy (DOE), DHS, and Natural Resources–Canada worked with the sector to develop the *Roadmap to Achieve Energy Delivery Systems Cybersecurity*.[16] The roadmap provides a strategic framework for public-private investments in cybersecurity R&D necessary to achieve resilient energy delivery systems that are designed, installed, operated, and maintained to survive a cyber-incident while sustaining critical functions. The objective of these activities is to gain the cyber advantage by developing a dynamic security state to which future attackers must adapt versus the infrastructure responding to the latest threat landscape.

DOE has been working with other federal partners, academia, and industry to implement the roadmap since 2005. Projects include a modular tool set for system-wide, role-based access control, quantum key distribution to securely exchange cryptographic keys for multiple clients, secure gateways for field device protection, and embedded device intrusion detection, among others. By use of the roadmap, significant progress has been made in developing and commercializing tools and guidance. Some recent examples include the following:

- Secure Information Exchange Gateway provides secure, flexible, real-time, and reliable information exchange for electric grid applications. It consolidates data exchange to reduce the external attack surface and the costs of maintaining multiple data exchange systems.
- Padlock is a cybersecurity gateway device that provides strong access controls, central collection of log data, enhanced serial and Ethernet data communications, and security and password management for field devices.
- Exe-GUARD protects energy delivery computers from unexpected cyber activity, including attempts to inject malicious code or alter settings without proper authentication.
- Network Access Policy Tool helps energy utilities map their control system communications paths, including for critical cyber assets, in minutes rather than days and verifies that these paths conform to the utility's security policy.

The areas of assessing risk, information sharing, threat analysis, procurement, and incident response have ongoing federal programs with national laboratory, vendor, and industry participation. There are a number of efforts—including those by DHS, ICS-CERT, DOE's Office of Electricity Delivery and Energy Reliability, NIST, and NERC—that all acknowledge each other but have not yet been fully integrated. These efforts include the

NIST Framework for Improving Critical Infrastructure Cybersecurity[17] and the Electric Sector Cybersecurity Capability Maturity Model[18] for assessing and mitigating risk. Additionally, DHS research assigned environmental risk factors for major components in the energy sector by using the Common Vulnerability Scoring System.[19]

National laboratories and U.S. research institutions should support the development of cybersecurity technologies that evolve ahead of the threat. Attack Technology Analysis and Characterization and Response Analysis and Characterization Tool are two examples of technologies currently being used by some asset owners. Another example of a proactive cyber defense is the use of physical sensing to detect anomalous electromagnetic signals from programmable logic controllers, CPUs, field programmable gate arrays, and application-specific integrated circuits. These technologies could be used to detect attacks using zero day exploits that traditional scanning and patching are not capable of addressing.

Overall, security of the grid can benefit through collaboration and dialogue between the government and private sector, which may involve outreach initiatives to smaller entities to ensure more widespread participation and dissemination of information. DOE's Cybersecurity Risk Information Sharing Program has been developed as an initial step toward helping the industry share risk information. Additionally, the federal government is often in the best position to provide a holistic perspective for grid and energy sector risk analysis. As a trusted source of vulnerability information with robust analysis capabilities, the federal government can play an important role in the information-sharing process and can share, for instance, the most likely attack vectors and prioritization of the most likely targets.

Despite the numerous ongoing activities in cyber security, many other technical advances are needed to address gaps and evolving challenges.

Improved Situational Awareness

Technologies and capabilities to assess the "state of security" for the grid will be needed as cyber and physical threats evolve. Cyber-physical models, analytical tools, and performance metrics can help enable this capability to increase the security posture. Moving to real-time analytics and the ability to co-simulate cyber and physical systems can help perform nontraditional contingency planning, such as managing grid impacts of interruption to heating oil and propane deliveries. While the energy sector has a well-established capability to plan for and survive physical contingencies, it should also be able to survive physical contingencies that result from cyber-incidents. For example, the Open Access Same-Time Information System (OASIS)[20] is an Internet-based tool for sharing information on transmission prices and product availability. While OASIS does not develop control commands to operate the grid, it does provide a gateway for real-time scheduling, day-ahead scheduling, and power flow management. This information helps operators develop strategies for handling load changes and maintenance activities throughout the day. Any physical impact resulting from data compromises might occur far downstream of when the data was compromised, making this a sophisticated threat. Identifying other aspects of nontraditional contingency planning, increasing the speed of detecting compromises, and improving the situational awareness of the security posture, both cyber and physical, are all important areas to investigate.

Scalable Secure Communications

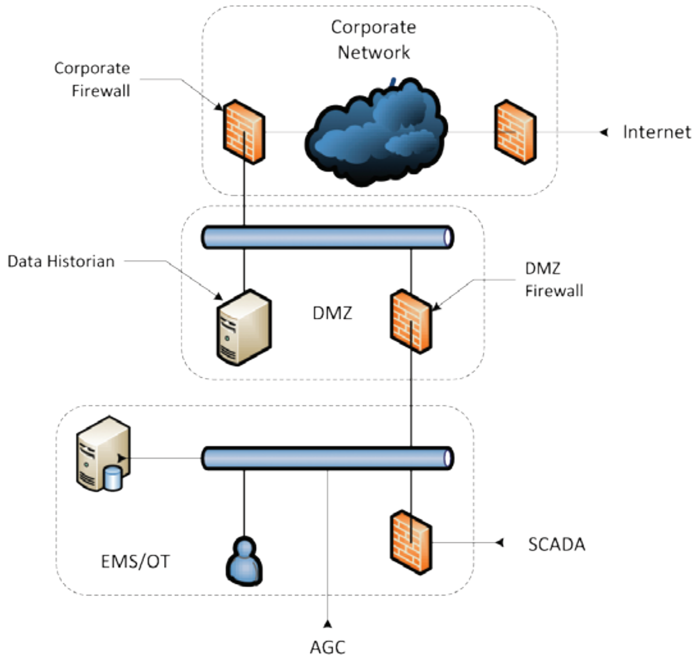
Communicating at speed with thousands (even millions) of devices securely is unachievable with today's technology. The scalability of communications infrastructure presents a daunting challenge, although there is guidance around the secure deployment of Internet Protocol version 6.[21] The use of cloud computing by the electric sector and the trend toward the IoT can support the scaling issue but presents unique challenges of its own for cybersecurity measures. For example, the use of public key infrastructures may not be practical for large-scale deployments. Another aspect of secure communications is the physical security of the assets associated with the underlying IT and OT systems. Technologies that can enable manufacturing of inherently secure devices can facilitate adoption of advanced security technologies. For example, research into "security on a chip" technologies can help assure secure communications with an increased proliferation of sensor devices. High performance data environments, data management techniques, and analytics that can handle the growing amount of data transfers for security purposes are other areas to investigate. Another challenge that needs to be addressed is that protocols engineered for legacy IT and OT components may not operate as intended in current computing and networking environments and are vulnerable to manipulation.

Installation of smart meters will continue to grow, and security measures for communications between the meter and the utility are being designed into the equipment. However, security for communications between customer technologies to the meter requires investigation. Allowing customers to control their energy usage provides flexibility and efficiency for the user. However, if the customer is denied access and control or if the customer's system cannot receive power due to a malicious compromise of the cyber-physical interface, the impacts could propagate back into the distribution system and even the transmission system. Research is required to identify potential vulnerabilities of smart meters that could be exploited via personal devices and to determine the uniqueness of these exploits and if they could be transferable regionally (wide-area attack). Research activities on topics such as lightweight encryption, cryptography, and key management are needed to increase the security of communication as well as the privacy of information in this new environment consisting of ever more devices and associated information.

Trusted Data Exchanges

Currently, utilities employ demilitarized zones (DMZs) that segment corporate and operational networks. However, energy sector information and data are still required to be passed across domains and between organizations for efficient operations. Figure 3.A.3 shows a schematic of this architecture.[22] Organizations should be able to move customer data without compromise, securely transfer corporate or operational data with other organizations if required, and be able to rely on data transfers for operations even if part of the system has been compromised by cyber-attacks. Importantly, the operational networks that control energy delivery must be designed to reject, and be resilient to, a cyber-incident that may have penetrated the corporate network defenses. Research into cybersecurity technologies should consist of end-to-end data delivery, computation, and power applications that are able to respond jointly, quickly, and seamlessly across the various domains.

Figure 3.A.3 Cross-Organizational Chain of Trust



Key: **SCADA** = Supervisory Control and Data Acquisitions; **EMS** = Energy Management System; **AGC** = Automatic Governor Control.

Real-time Investigation, Mitigation, and Recovery

Resilient control systems should be able to survive a cyber-incident while sustaining critical functions and be able to "ride through" or adapt to a cyber-incident. In a modernized grid, control systems should be able to operate with parts of the system or its component devices, including applications and data, compromised by malicious intrusion. Enabling adaptive and self-configuring abilities will require fundamental changes and upgrades to control system architectures and software designs. In the event of an incident, critical control functions should be sustained while forensic investigations proceed to understand the extent and consequence of the compromise, followed by development of mitigation steps and recovery to normal operations. Another potential response to a threat is logical islanding, which extends the classical islanding concept to cyber assets, refusing or distrusting connections from peer systems that appear to be compromised or malfunctioning. Additionally, capabilities to evaluate the robustness and survivability of new platforms, systems, networks, architectures, policies, and other system changes are needed.

State-of-the-Art Cybersecurity Database

Identifying available cybersecurity capabilities is needed to ensure that gaps in cybersecurity technology development are addressed and not overlooked. This activity would complement efforts on evaluating the capabilities of existing technologies and conducting vulnerability assessments. A database will help reduce redundancy of development efforts and identify potential areas of overlap to support greater cyber security. A repository of efforts currently exists that is searchable by organization and maturity.[23] However, there currently is no capability to identify redundancies or gaps or have confidence that all available technologies are identified. The goal of this activity is to minimize the impact of a cyber-attack by supporting the forensic investigation and recovery of data and applications for power delivery. Results of vulnerability assessments could be used to identify the availability of critical assets under an incident, study the impact of applications and data sets under various cyber-attacks, and help refine recovery scenarios. In addition, the database can help identify the appropriate cybersecurity training needed for utility staff and end-use consumers.

Physical Security

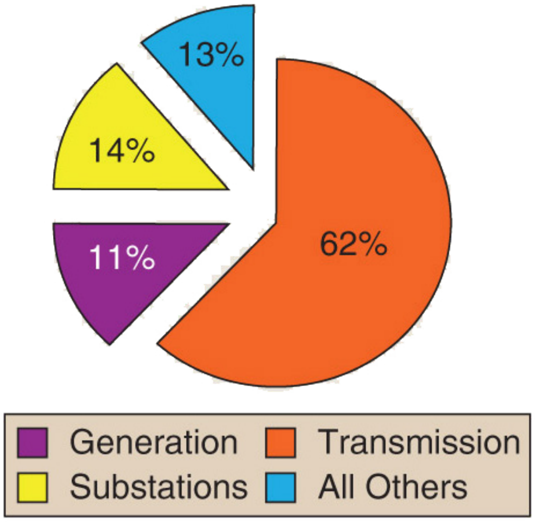
Over the past 35 years, the United States has suffered the effects of a number of major disasters that have destroyed essential components of the energy infrastructure and resulted in significant economic losses. Between 1980 and 2014, the United States sustained 178 weather and climate disasters, where overall damages/costs reached or exceeded $1 billion (including an inflation adjustment to 2014).[24] These events include hurricanes/storms, droughts/heatwaves, flooding, ice storms, and wildfires. In addition to these weather events, there are other types of costly natural disasters such as earthquakes. The high-impact/low-frequency and no-notice characteristics of earthquakes are extremely dangerous and potentially costly, both in lives and property. For example, the 1994 Northridge earthquake in California was responsible for one of the biggest insured property losses in U.S. history—ranking within the top five most catastrophic events based on 2012 dollars.[25] Most of these events have resulted in damage to critical infrastructure, resulting in a considerable loss of vital energy supplies to homes and businesses. The regional nature of natural disasters combined with the criticality of a robust electric grid network further highlights the importance that communications networks and other technologies (e.g., sensors) play in minimizing cascading effects. Cascading effects can go past geographical boundaries and can lead to broader systemic failures. In addition to natural disasters, there are also malicious actors who aim to damage critical grid assets.

Grid physical security is associated with technologies that improve the security posture of generation, transmission, and distribution components as well as the monitoring, communication, and computation hardware that constitute grid control systems. Physical security is an important facet of cyber security because protecting a computer, and other control system equipment, is nearly impossible if the attacker is given physical access to the equipment. Physical security measures include activities that can harden assets, improve situational awareness, deter and respond to man-made threats, and mitigate risks. Protection from winter storms, earthquakes, vandalism, and numerous other physical threats can also be addressed through physical security research and development efforts. Key needs are risk assessment tools and processes to determine the most vulnerable portions of the grid and the most appropriate solution to implement, including management of costs. Efforts will require consideration of the impact of physical threats on the cyber domain, such as attacks and disruptions to critical communications channels, and the resulting effect on system operations.

A formal roadmap has not been developed for physical security, as has been done for cyber security. However, there are a variety of different sources, including the Department of Defense, that have published physical security guidelines. Attacks on electrical systems are not new, and some countries have had to endure them for years. In an analysis of attacks on electrical infrastructure throughout the world, the most common target area is transmission, as indicated in Figure 3.A.4. Additional analysis has been conducted to identify the critical points in the grid that would be susceptible to physical attacks and would result in sustained impacts. Physical attacks can be costly; utilities have incurred financial losses due to theft, vandalism, and other attacks, including copper theft and the occasional shooting of insulators or conductors. In 2013, the assault of the Metcalf substation resulted in $15 million of damage. While no customers lost power, the utility committed to spending $100 million over three years to improve security of its critical facilities.[26]

Figure 3.A.4 International Terrorist Attacks from 1994–2004[27]

Credit: Memorial Institute for the Prevention of Terrorism



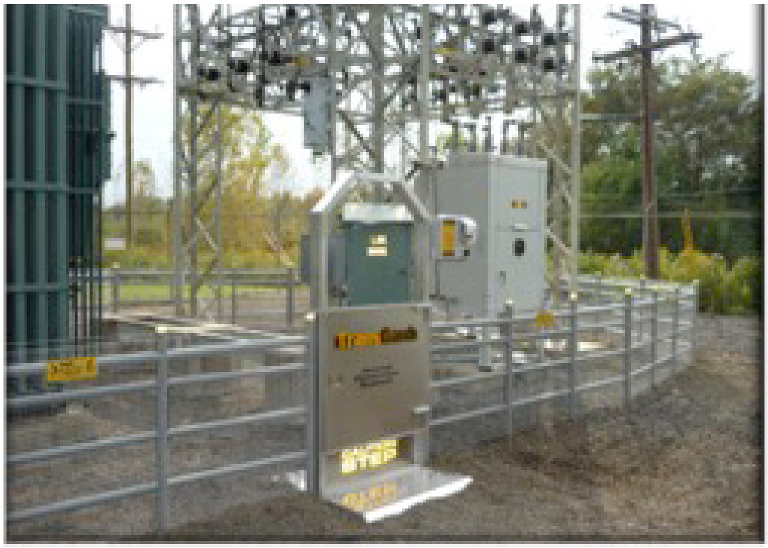
Although implementing physical security measures can be costly, utilities will incorporate technology that best aligns with their risk management strategy. For example, a utility determined that the risk from marmots was high enough to warrant a solution. They developed an electrified fence within the protective barrier of the standard boundary fence, illustrated in Figure 3.A.5, to prevent the rodents from damaging the substation components. This example highlights the unique challenges that different utilities face regarding physical security and the potential difficulty in developing broadly applicable solutions.

Smart Materials

Many substation components are exposed because they require heat transfer to the surrounding air to maintain normal operations and may require access for maintenance. Due to this exposure, these assets are easy targets for ballistic attacks. Efforts are being funded by DHS and the Army Corp of Engineers to understand the impact of physical protection measures for electric grid assets and other high-value targets on the electric grid. Activities include movable armor panels and ballistic testing for the protection of transformers. National laboratories are also investigating the application of military standards for ballistics (i.e., MIL-STD-662F) to materials and armor that can protect grid components. Research and development of smart materials that can be used in electrical transmission and distribution components that prevent or self-heal from damage would be valuable. Components that can benefit from smart materials include insulators (bushings and transmission line), transformers (conservators, cooling vanes, and tank), circuit breakers (bushings and tanks), and voltage stability components (capacitors and inductors). Other smart material innovations that could be applied to transmission and distribution lines include super-hydrophobic coatings that facilitate deicing during winter storms.

Figure 3.A.5 Electrified Marmot Fence at a Distribution Substation in the Pacific Northwest

Credit: Avista Corporation



Operational Response to Intrusion/Damage

Protection relays for physical components are typically set so the system will go to its safest state—de-energized—in the event a threshold limit is exceeded. There are even backup protection mechanisms if the primary protection does not clear the fault. These protection schemes are fairly static, primarily used at the transmission level, and critical for reliable operations. However, if a fault occurs due to vandalism or an attack, protection relays may not be set appropriately and other components can remain energized or exceed thresholds, resulting in permanent damage. Concrete barriers can protect assets but would not prevent an intruder walking inside a substation. Automatic operational schemes could be armed after an intelligent adversary was detected within the boundaries of a substation or switchyard. These schemes could identify resilient configurations for the remaining system to withstand the loss of the compromised substation. In the event of a fault, the substation/switchyard would de-energize to remove the possibility of further system damage and to protect the intruder from injury. Other predictive system configurations—including adaptive relaying, topological switching, and intentional islanding with microgrids—are areas of investigation. Additionally, research is needed to better understand large system behavior, identify when the system is degrading, and enable adaptive technologies for response to threats.

High-Impact Low-Frequency Events

High-impact, low-frequency (HILF) events are those that are rare but have the potential to cause long-term, catastrophic damage to the power system. The energy sector has long studied the effects of HILF events, such as risks posed by coordinated attacks, pandemics, and geomagnetic disturbances (GMDs) or electromagnetic pulses (EMPs).[28] Mitigation solutions for some of the phenomena have been developed and deployed. Impacts from GMDs can be managed by installing series capacitors on transmission lines, applying capacitors in the transformer neutral-to-ground connection, or applying a low-ohmic resistor to the neutral-to-ground connection. This last method of mitigation had a market size of between $120M and $500M in 2010 within the United States.[29] Work published by NERC in 2012 made 33 recommendations in the areas of operations, monitoring, communications, short-/long-term system planning, protection and control, interdependencies with other critical infrastructures, and others that are being explored.[30] Another concern raised by NERC is the extended loss of GPS and the resulting likelihood of reliability impacts,[31] especially with greater use of phasor measurement units. Many of these recommendations currently have research and development efforts at national laboratories.

An area that merits further investigation is HILF events on other sectors where second-order impacts would affect the electrical sector. Examples include inadequate transportation of fuel for electric generation, such as coal by rail[32] or constraints on the natural gas supply, as occurred during the recent "polar vortex." A NERC review[33] of the polar vortex indicated that 19,500 MW of generation was lost due to cold weather conditions. While this event was weather related, an attack on natural gas transportation or the natural gas infrastructure could have a significant second-order effect on the electric subsector. As the electric power system becomes more interconnected, understanding and analyzing the impact of interdependencies from these events, natural and man-made, are critical areas for further research.

While HILF events are often discussed as a single topic, these events (e.g., GMD, EMP, and coordinated cyber-attacks) must be addressed individually due to the different impacts each has on the electric grid. There is no "one-size-fits-all" solution, but more resilient control systems can have broad benefits. Future solutions should consider the mitigation of specific risks as appropriate.

Procurement and Supply Chain

As cybersecurity defenses evolve, the methods of accessing these systems evolve as well. Attackers will look at the entire life cycle of equipment used in energy delivery systems for an opportunity to gain access, and so too must defenders. The initial part of this life cycle is procurement. One of the more recent procurement documents developed by the DOE and DHS provides baseline procurement language for individual components, individual energy delivery systems, and assembled or networked energy delivery systems.[34,35] The document identifies a host of requirements, primarily for the supplier, which provide the prospect for technology development.

Securing the procurement and supply chain processes is important because critical portions of the grid contain parts that are developed, manufactured, and shipped from third parties. Fraudulent parts often fail at higher rates, and therefore can impact overall reliability. A greater threat would be a determined adversary who can preinstall malware on an embedded computer or equipment before it is shipped to a utility, thereby compromising the energy system before it is even put into use. A recent example of supply chain compromise can be found in the proliferation of the Havex remote access tool among various industrial control system owners. Ensuring tamper-free components, software, and equipment should go beyond documentation, which can be incomplete, whether through oversight or malicious activity. Technologies that identify a secure chain of custody (from source through development) and that can be easily passed to the asset owners upon purchase will allow for vulnerabilities—accidental or intentional—to be identified at the point of origin.

System Recovery

While cyber- and physical-security measures can mitigate and prevent the impact of incidents, there will be times where the system will fail or otherwise be compromised from known or unknown threats. R&D into technologies and mechanisms that can accelerate system recovery and support the system while under duress are critical to improving the resilience of the grid. For instance, while improvements to control systems and distribution automation can facilitate recovery from disruptions, there are steps in the restoration process that will require human intervention, such as the replacement of damaged cyber and physical assets that will need to be coordinated at a macro level. Since the electric system is composed of many separate systems, gaining a resilence- and recovery-based understanding related to the more complex issues involved with a system of systems is crucial and underscores the need for additional research in this area.

Damage Assessment and Predictions

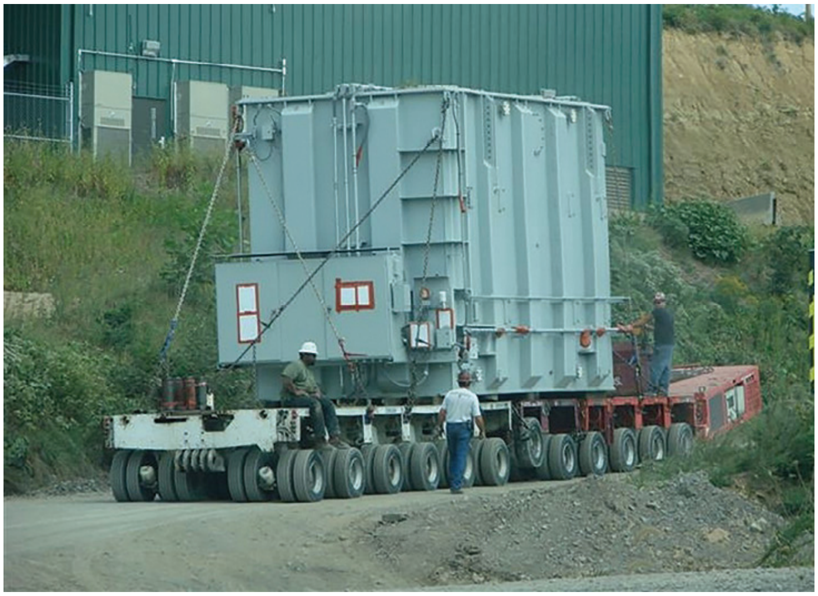
Analysis and prediction of how a storm or an event (e.g., HILF scenarios) may damage assets in an area can facilitate preparation and prioritization of resources for responding to the event. These capabilities can be extended to include the assessment and prediction of compromised assets resulting from a cyber-attack or analyzing the acceptable loss of equipment while still allowing for continued operations of the electric system. Proper preparation, staging, and training can accelerate restoration, but advanced analytics after an event can also facilitate recovery. Opportunities exist to integrate data from various channels and sources, which may be limited or incomplete, to support system restoration. Examples include utilizing social media, integrating weather forecasting with outage management systems, and considering flood and transportation models in logistics and planning. More R&D related to effective analytics and predictive models may make these efforts more fruitful.

Large Power Transformer Availability

Large power transformers (LPTs) are critical assets with lead times of 35 weeks or more after receipt of order. In the event LPTs are damaged, the availability and suitability of a replacement becomes the priority. Working toward identifying potential opportunities to reduce the time of large power transformer replacement improves the overall resilience of the grid. Another challenge is the transportation of these large pieces of equipment as shown in Figure 3.A.6. Improvements to logistics and more portable designs can help with system recovery. Standardization of transformer specification can also reduce this lead time to approximately 20 weeks and cut costs by 15% or more.[36] Broader use of standards can help systems recover, but many legacy substations still face challenges from customized solutions. Industry currently has transformer sharing programs, but opportunities exist to identify new mechanisms to ensure transformer availability. For example, retrofitting of transformers from coal plant retirements can serve as a temporary supply of LPTs and could shorten the time of replacement from months to weeks for critical facilities.

Figure 3.A.6 Shipment of One of the Largest Transformers Manufactured by ABB

Credit: ABB



Portable Power Delivery Equipment

As with transformers, damage of other critical energy delivery assets can influence the time it takes to recover from an event. Portable power delivery equipment that can be used to help restore power to communities may be a useful area to explore. A prototype for a recovery transformer has been demonstrated, and concepts of mobile substations have been explored.[37] While not a permanent replacement, these technologies could allow power plants to come on line at a reduced capacity until an actual replacement could be manufactured, shipped, and installed. Other options for portable power delivery equipment may benefit from further investigation.

Endnotes

[1] LaCommare, K. H.; Eto, J. H. "Understanding the Cost of Power Interruptions to U.S. Electricity Consumers." LBNL-55718. Berkeley, CA: Ernest Orlando Lawrence Berkeley National Laboratory, September 2014. Accessed March 27, 2015: http://certs.lbl.gov/pdf/55718.pdf.

[2] "National Electric Delivery Technologies Roadmap." U.S. Department of Energy Office of Electric Transmission and Distribution. January 2004. Accessed March 27, 2015: http://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/ER_2-9-4.pdf.

[3] "Security Firms Tie Russian Government to Utilities Hacks." Bloomberg Politics. October 30, 2014. http://www.bloomberg.com/politics/articles/2014-10-30/security-firms-tie-russian-government-to-utilities-hacks.

[4] Edison Electric Institute, *EEI Statistical Yearbook 2013*, Table 10.6, 2013.

[5] *Platts UDI Directory of Electric Power Producers and Distributors, 122nd Edition of the Electrical World Directory,* 2014, p. vi. http://www.platts.com/IM.Platts.Content/downloads/udi/eppd/eppddir.pdf.

[6] "Blackout Tracker: United States Annual Report 2014." Eaton. Accessed March 27, 2015: http://www.eaton.com/blackouttracker.

[7] Rieger, C. G. "Resilient Control Systems Practical Metrics Basis for Defining Mission Impact." Idaho Falls, ID: Idaho National Laboratory. Resilient Control Systems (ISRCS), 2014 7th International Symposium, August 2014. Accessed March 27, 2015: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=6900108&abstractAccess=no&userType=inst.

[8] "Energy Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan." U.S. Department of Energy, 2010. Accessed March 27, 2015: http://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-2010.pdf.

[9] "Cyberexperts: A 'Lost Decade' Since 9/11 to Address Infrastructure Threats." *The Christian Science Monitor,* January 17, 2014. Accessed March 27, 2015: http://www.csmonitor.com/USA/2014/0117/Cyberexperts-a-lost-decade-since-9-11-to-address-infrastructure-threats.

[10] "Guidelines for Smart Grid Cybersecurity. Volume 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements." NISTIR 7628 Revision 1. U.S. Department of Commerce. Accessed March 27, 2015: http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf.

[11] "Foundations for Innovation in Cyber-Physical Systems Workshop Report." Energetics Incorporated. Prepared for National Institute of Standards and Technology, January 2013. Accessed March 27, 2015: http://www.nist.gov/el/upload/CPS-WorkshopReport-1-30-13-Final.pdf.

[12] "2014 Cost of Cyber Crime Study." Ponemon Institute, October 2014. Accessed September 11, 2015: http://www.ponemon.org/blog/2014-global-report-on-the-cost-of-cyber-crime.

[13] "ICS-CERT Year in Review: Industrial Control Systems Cyber Emergency Response Team." U.S. Department of Homeland Security, National Cybersecurity and Communications Integration Center, 2013. Accessed March 27, 2015: https://ics-cert.us-cert.gov/sites/default/files/documents/Year_In_Review_FY2013_Final.pdf.

[14] "Trends in Incident Response in 2013 Overview." ICS-Cert Monitor. National Cybersecurity and Communications Integration Center. U.S. Department of Homeland Security, December 2013. Accessed March 27, 2015: https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2013.pdf.

[15] "Challenges Remain in DHS Efforts to Secure Control Systems." OIG-09-95; p. 8. U.S. Department of Homeland Security, August 2009. Accessed March 27, 2015: http://www.oig.dhs.gov/assets/Mgmt/OIG_09-95_Aug09.pdf.

[16] "Roadmap to Achieve Energy Delivery Systems Cybersecurity." (Update of the 2006 "Roadmap to Secure Energy Sector Control Systems.") Energy Sector Control Systems Working Group, September 2011. Accessed April 5, 2015: https://www.controlsystemsroadmap.net/ieRoadmap%20Documents/roadmap.pdf.

[17] "Framework for Improving Critical Infrastructure Cybersecurity." National Institute of Standards and Technology, February 12, 2014. Accessed April 5, 2015: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

[18] Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2). Office of Electricity Delivery & Energy Reliability. Accessed April 5, 2015: http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/electricity-subsector-cybersecurity.

[19] Mell, P.; Scarfone, K.; Romanosky, S. A Complete Guide to the Common Vulnerability Scoring System Version 2.0. June 2007. Accessed April 5, 2015: https://www.first.org/cvss/cvss-guide.

[20] See for example PJM's OASIS system. Accessed on May 21, 2015: http://www.pjm.com/markets-and-operations/etools/oasis.aspx.

[21] Frankel, S.; Graveman, R.; Pearce, J.; Rooks, M. "Guidelines for the Secure Deployment of IPv6: Recommendations of the National Institute of Standards and Technology." U.S. Department of Commerce and National Institute of Standards and Technology, December 2010. Accessed April 5, 2015: http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf.

[22] "Cyber Security for Industrial Control Systems." Power Engineering, November 1, 2011. Accessed April 5, 2015: http://www.power-eng.com/articles/print/volume-115/issue-11/features/cyber-security-for-industrial-control-systems.html. Figure based on Figure 2, ICS Network, Source Rkneal Engineering.

[23] "Roadmap to Achieve Energy Delivery Systems Cybersecurity." (Update of the 2006 "Roadmap to Secure Energy Sector Control Systems.") Energy Sector Control Systems Working Group, September 2011. Accessed April 5, 2015: https://www.controlsystemsroadmap.net/ieRoadmap%20Documents/roadmap.pdf.

[24] "Billion-Dollar Weather and Climate Disasters: Table of Events." National Oceanic and Atmospheric Administration. Accessed April 19, 2015: http://www.ncdc.noaa.gov/billions/events.

[25] “Costliest U.S. Natural Disasters.” *Wall Street Journal,* May 30, 2014. Accessed April 19, 2015: http://www.wsj.com/articles/costliest-u-s-natural-disasters-1401488111.

[26] Baker, D. “FBI: Attack on PG&E South Bay Substation Wasn’t Terrorism.” *SFGate,* September 10, 2014. Accessed April 19, 2015: http://www.sfgate.com/business/article/FBI-Attack-on-PG-amp-E-substation-in-13-wasn-t-5746785.php.

[27] Amin, S. M.; Anthony M.; Giacomoni, A. M. “Smart Grid—Safe, Secure, Self-Healing.” *IEEE Power & Energy Magazine,* January/February 2012. Accessed April 19, 2015: http://magazine.ieee-pes.org/january-february-2012/smart-grid-safe-secure-self-healing/.

[28] “High-Energy, Low-Frequency Risk to the North American Bulk Power System.” Office of Electricity Delivery & Energy Reliability, June 2010. http://energy.gov/oe/downloads/high-energy-low-frequency-risk-north-american-bulk-power-system-june-2010.

[29] Kappenman, J. “Low-Frequency Protection Concepts for the Electric Power Grid: Geomagnetically Induced Current (GIC) and E3 HEMP Mitigation.” Metatech Corporation. Prepared for Oak Ridge National Laboratory, January 2010. Accessed April 19, 2015: http://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity/ferc_meta-r-322.pdf.

[30] “Severe Impact Resilience: Considerations and Recommendations.” Severe Impact Resilience Task Force. North American Electric Reliability Corporation, May 9, 2012. Accessed April 19, 2015: http://www.nerc.com/docs/oc/sirtf/SIRTF_Final_May_9_2012-Board_Accepted.pdf.

[31] “Preliminary Special Reliability Assessment Whitepaper: Extended Loss of GPS Impact on Reliability.” North American Electric Reliability Corporation (undated). Accessed April 19, 2015: http://www.nerc.com/docs/escc/PNT%20-%20Power%20Systems%20V19.pdf.

[32] Comments submitted by Dairyland Power Cooperative of La Crosse, Wisconsin, for the Quadrennial Energy Review Public Stakeholder Meeting in Chicago, Illinois. Dairyland Power Cooperative. August 8, 2014. Accessed April 19, 2015: http://energy.gov/sites/prod/files/2014/08/f18/chicago_qermeeting_craig_statement.pdf.

[33] “Polar Vortex Review.” North American Electric Reliability Corporation. September 2014. Accessed April 19, 2015: http://www.nerc.com/pa/rrm/January%202014%20Polar%20Vortex%20Review/Polar_Vortex_Review_29_Sept_2014_Final.pdf.

[34] “Cybersecurity Procurement Language for Energy Delivery Systems.” Energy Sector Control Systems Working Group (ESCSWG). April 2014. Accessed April 19, 2015: http://www.energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf.

[35] “Cyber Security Procurement Language for Control Systems Version 1.8.” Idaho Falls, ID: Idaho National Laboratory, February 2008. Accessed April 19, 2015: http://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/SCADA_Procurement_Language.pdf.

[36] Gill , J. “How Standardized Power Transformers Step Up More than Voltage for Wind Farms.” *Windpower,* June 26, 2014. Accessed April 19, 2015: http://www.windpowerengineering.com/construction/transportation/standardized-power-transformers-step-voltage-wind-farms/.

[37] “Benefits of Using Mobile Transformers and Mobile Substations for Rapidly Restoring Electrical Service.” U.S. Department of Energy, August 2006.

Glossary and Acronyms

Application specific integrated circuit (ASIC)	An integrated circuit customized for a particular use rather that designed for a general-purpose use.
Common Vulnerability Scoring System (CVSS)	CVSS provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. Its quantitative model ensures repeatable accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores. Thus, CVSS is well suited as a standard measurement system for industries, organizations, and governments that need accurate and consistent vulnerability impact scores.
Critical infrastructure protection (CIP) standards	On November 21, 2013, FERC approved, with modifications, the North American Electric Reliability Corporation's (NERC) Version 5 Critical Infrastructure Protection (CIP) Reliability Standards, CIP-002-5 through CIP-011-1.
Cryptographic key	A piece of information that determines the functional output of a cryptographic algorithm.
Cyber-physical system	A system that encompass computational and physical components, integrated and closely interacting to sense the changing state of the real world.
Cybersecurity	While CIP standards for transmission system entities exist, distribution system entities are regulated by individual states and municipalities with no common standard for cybersecurity.
DHS	U.S. Department of Homeland Security
DOE	U.S. Department of Energy
Electromagnetic pulse (EMP)	A short burst of natural or man-made electromagnetic energy that may occur in the form of a radiated, electric, or magnetic field or conducted electrical current depending on the source.
ES-C2M2	Electric sector cybersecurity capability maturity model established as a result of the Obama Administration's efforts to improve electricity subsector cybersecurity capabilities, and to understand the cybersecurity posture of the energy sector.
FERC	Federal Energy Regulatory Commission
Field programmable gate array (FPGA)	An integrated circuit designed to be configured after manufacturing "in the field."
Geomagnetic disturbance (GMD)	GMD occurs when solar storms on the sun's surface send electrically charged particles toward earth. This could potentially affect the power grid operations.

High-impact, low-frequency (HILF) events	Those that are rare but have the potential to cause long-term, catastrophic damage to the power system.
ICS-CERT	Industrial control systems cyber emergency response team
Information technology (IT)	Information systems typically are used to support business, human resources, and other non-operational functions that can be maintained by IT professionals.
Internet of Things (IoT)	The network of physical objects (or "things") embedded with electronics, software, sensors, and connectivity that enables it to achieve greater value and service by exchanging data with operators and/or other connected devices. Each thing has a unique identifier in its embedded computing system but can interoperate within the existing Internet infrastructure.
Large power transformers (LPTs)	Critical assets with lead times of 35 weeks or more after receipt of order.
National Institute of Standards and Technology (NIST)	NIST is the federal technology agency that works with industry to develop and apply technology, measurements, and standards.
North American Reliability Corporation (NERC)	The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to assure the reliability of the bulk power system in North America.
OE	DOE's Office of Electricity Delivery and Energy Reliability
Open Access Same-Time Information System (OASIS)	An Internet-based tool for sharing information on transmission prices and product availability.
Operational technology (OT)	Operational systems transfer data and commands that are critical to operating and protecting the grid itself and require operators and engineers to design, run, and maintain its function.
Programmable logic controllers (PLC)	A digital computer used in machines for automation of industrial electromechanical processes; designed for multiple arrangements of digital and analog inputs and outputs, extended temperature ranges, immunity to electrical noise, and resistance to vibration and impact.
Quantum key distribution (QKD)	Uses quantum mechanics to guarantee secure communication and enables two parties to produce a shared random secret key known only to them, which can then be used to encrypt and decrypt messages.
Recovery transformer (RecX) program	One of the federal initiatives by SmartGrid.gov . The goal of this program is to increase the resilience of the nation's electric transmission grid by drastically reducing the recovery time associated with transformer outages. The first prototype transformer was designed by the RecX consortium and is now installed at a CenterPoint Energy substation for testing.
Role-based access control (RBAC)	An approach to restricting system access to authorized users.

Supervisory control and data acquisition (SCADA) data	A system that operates with coded signals over communication channels to provide control of remote equipment.