The U.S. Electrical Grid: Surviving Cyber-Terrorism and Solar Flares

Robert J. Lambrechts

In celebrating the beginning of the twenty-first century, the National Academy of Engineering set about identifying the single most important engineering achievement of the twentieth century. The Academy compiled a list of twenty impressive accomplishments that have affected virtually everyone in the developed world. The Internet took thirteenth place on this list and "highways" the eleventh. At the top of the list, as the most significant engineering achievement of the twentieth century, was electrification made possible by the grid. Electrification powers almost every pursuit and enterprise in modern society. It has lighted the world and improved countless areas of daily life, including food production and processing, air conditioning and heating, refrigeration, entertainment, transportation, communication, health care, and computers. National Academy of Engineering, Greatest Engineering Achievements of the 20th Century (2011), www.greatachievements.org. Our centuries-old electric grid consists of more than 9,200 electric generating units with more than 1 million megawatts of generating capacity connected to more than 300,000 miles of transmission lines. U.S. Department of Energy, The Smart Grid: An Introduction (2008).

The grid evolved its simple local connections about a century ago to the current "smart grid" concept. There is growing concern, however, over its vulnerability to attack as well as damage through natural phenomena. This article provides a brief history of the legal and regulatory evolution of the grid and the inherent vulnerabilities that have precipitated that evolution. It explores the efforts of the federal government to improve security of the grid through the advancement of critical infrastructure protocols. The article concludes by considering the impact of major solar storms on the grid's ability to operate.

Early electric power systems prior to the turn of the nineteenth century consisted of isolated stations, which served small, independent pockets of customers. As some of these power systems grew to cover larger geographic areas, it became possible to connect previously isolated systems so neighboring systems could, to their mutual benefit, share generation and voltage stability resources. Tying power systems together with these early interconnections, however, also introduced the risk that a single significant disturbance could collapse all of the systems tied to the interconnection. Generally it was decided that the benefits outweighed the risks, and by 1915 interconnections began to flourish and grow in size. By the end of the 1960s there were virtually no isolated power systems remaining in the lower forty-eight states and southern Canada; practically all power companies were attached to large interconnections.

Mr. Lambrechts is a partner in the Overland Park, Kansas, office of Lathrop & Gage LLP. He may be reached at blambrechts@lathropgage.com.

The electricity industry in the late 1800s was an unregulated, competitive market. Within a few years, 85 percent of the electric industry was controlled by just sixteen holding companies. Joseph P. Tomain, *Electricity Restructuring: A Case Study in Government Regulation*, 33 Tulsa L. J. 827, 830 (1998). Although this consolidation led to technological advances and greater efficiency, the holding companies were susceptible to stock manipulation and shareholder abuses. Responding to these abuses, in 1935 Congress passed both the Public Utility Holding Company Act (PUHCA), 15 U.S.C. § 79, significantly limiting the entities an electric utility holding company could own, and the Federal Power Act, 16 U.S.C. § 824, which gave the Federal Power Commission (the predecessor to the Federal Energy Regulatory Commission (FERC)) authority to regulate the transmission of electric energy in interstate commerce and the sale of such energy at wholesale in interstate commerce. By the mid-sixties, industry expansion slowed considerably, economies of scale were not being realized, costs were increasing, and generation was overbuilt. Traditional regulation was failing both consumers and investors, and policymakers began thinking about reform. By 1978, the country's energy situation was moving into a crisis mode. The Carter administration responded with the National Energy Act of 1978, designed to increase energy efficiency, modernize utility ratemaking, and encourage the creation of a new electricity market. Pub. L. No. 95-617. One piece of the Act, known as the Public Utility Regulatory Policies Act (PURPA), 16 U.S.C. § 824a-3, specifically targeted the electricity industry. PURPA encouraged independent power production and the growth of nonutility-owned generation facilities known as qualifying small power production facilities (QFs). The central question facing regulators was how to provide nonutility power producers with access to transmission lines to create a competitive market in the transmission sector without placing the utility companies at a competitive disadvantage.

Regulators began addressing this issue with the Energy Policy Act of 1992 (1992 EPAct). Pub. L. No. 102-486. The 1992 EPAct allowed FERC to order transmission-owning utilities to "wheel" power for wholesalers (transmit power from a wholesale generator to customers), thus opening access to the transmission grid. 16 U.S.C. §§ 824j-824k. FERC exercised this newfound authority in 1996 with Order Number 888, *Promoting Wholesale Competition through Open-Access Non-discriminatory Transmission Services by Public Utilities and Transmitting Utilities*, 61 Fed. Reg. 21,540 (May 10, 1996), which required transmission-owning facilities to file open-access nondiscriminatory tariffs and to unbundle their transmission and generation operations. That same day, FERC issued Order Number 889, *Open-Access Same-Time Information System (formerly Real-Time Information Networks) and Standards of Conduct*, 61 Fed. Reg. 21,737 (May 10, 1996), to make information about access to

the transmission system available to the public. FERC Order Number 2000, *Regional Transmission Organizations*, 65 Fed. Reg. 809 (Jan. 6, 2000), fostered regional transmission organizations (RTOs) and Independent System Operators by establishing transmission guidelines for RTOs. These orders were central to the disaggregation of the vertically integrated electric utilities into three separate sectors: generation, transmission, and local retail distribution to end users.

Since restructuring began in 1978, utilities have had a significant financial incentive to invest in wholesale generation facilities free of state utility regulation. Utilities, however, receive only a low, government-set return on their transmission investments in the power grid, which is regulated as a common carrier under traditional public utility rate regulation. Consequently, investment in the grid has lagged and it is now ill equipped to handle today's growing power demands.

The Grid: Its Configuration and Blackouts

North America has three "major" grids: the Western Interconnection, the Eastern Interconnection, and the Electric Reliability Council of Texas (or ERCOT). Electric utilities within each grid are electrically tied together during normal system conditions and operate at a synchronized frequency of 60 Hertz. The Western Interconnection stretches from Western Canada to Baja California in Mexico, and eastward over the Rockies to the Great Plains. The Eastern Interconnection is also electrically tied together during normal system conditions and reaches from central Canada eastward to the Atlantic coast (excluding Quebec), south to Florida, and west to the foot of the Rockies (excluding most of Texas). The third major North American grid is the Electric Reliability Council of Texas (ERCOT), successor to the Texas Interconnected System, formed in 1941 so power companies could provide their excess generation capacity to Gulf Coast industry supporting the U.S. war effort.

Sharing of capacity by interconnection reduces the amount of reserve capacity that must be built by individual networks to ensure reliable operation when supplies are short. The interconnected utilities are in a "marriage" that dictates or constrains key aspects of their technology choices and operating procedures. This became readily apparent in 1965.

On November 9, 1965, a relatively minor system disturbance triggered failure of a power system protection component that was not properly configured. The interconnection was operating near peak capacity due to the extreme cold weather and high heating demand. The small initial outage quickly cascaded into the Northeast Blackout of 1965; over 30 million people in an 80,000 square-mile area were without electricity for up to 12 hours.

This disturbance revealed that interconnections had evolved without adequate high-level planning and operating oversight to try to prevent such events and with varying operating standards and procedures that had been developed somewhat independently by each member on the interconnection. Restoration of power was hampered due to the lack of common practices and coordination procedures. Furthermore, power system protection schemes were often designed with only a local power system's design in mind, meaning that they might operate improperly in response to protection schemes activating in neighboring systems. The 1965 Blackout revealed the necessity to develop common operating and protection standards and plans to coordinate power system restoration efforts.

The North American Electric Reliability Council (now Corporation) (NERC) was formed on June 1, 1968, by the electric utility industry to promote the reliability and adequacy of bulk power transmission in the electric utility systems of North America. NERC's mission was to ensure that the bulk power system in North America remained reliable. NERC was formed to assist the regional councils by developing common operating policies and procedures as well as training resources and requirements.

Even with the best efforts of NERC, on August 14, 2003, 50 million Americans lost power in what marked the worst blackout in United States and Canadian history. The cascading power outage first hit Toronto, then Rochester, Boston, and, finally, New York. It took just 13 minutes for the blackout to spread throughout the 80,000 square-mile Canada-United States Eastern Interconnection power grid. Power was not restored for four days in some parts of the United States. Parts of Ontario suffered rolling blackouts for more than a week before full power was restored; estimates of total costs associated with the blackout in the United States are $7–10 billion (U.S. dollars). Electricity Consumers Resource Council (ELCON), *The Economic Impacts of the August 2003 Blackout* (Feb. 9, 2004).

In the past twenty-five years, grid congestion and unusual power flows have steadily increased, even as customer expectations of reliability and cyber-physical security have been rising. Yet, a major outage occurs about once every decade and costs in excess of $2 billion. Less extensive outages, which are commonplace, are costly to customers and for society. On any given day, an estimated 500,000 customers are without power for two hours or more in the United States. Annual losses to the U.S. economy from power outages and disturbances are estimated to total between $75 billion and $180 billion, S. Massoud Amin, Securing the Electricity Grid (2010).

In 2001, NERC warned Congress that the grid was not designed for the way in which it was then being used. The grid was originally built to transfer relatively small amounts of power over short distances. Marsha Freeman, *U.S. Electric Grid Is Reaching the End Game*, Executive Intelligence Review (Sept. 22, 2006), www.larouchepub.com/other/2006/3338electric_grid.html. When one region of the country has a surplus at a time when another region needs additional megawatts of power, power is transferred over 1,000-mile power lines to keep supply and demand balanced across the grid. In 1972, a typical utility may have engaged in only a few of these electromagnetic transactions each week. Now, it is common for thousands to be carried out, often by computer, in much the same way that stocks are traded. Deregulation of the electric power industry has created this market-driven system, where power can be immediately traded over long distances to provide consumers with access to cheaper electricity from various suppliers in the grid's electricity market. This trading has increased the flow of electricity over evermore congested transmission lines, thereby drastically increasing the risk of major power outages.

Congress responded to these increased risks through the Energy Policy Act of 2005 by adding a new section 219 to the Federal Power Act, which directed FERC to develop incentive-based rate treatments for transmission of electric energy in interstate commerce that would encourage private investment in new transmission lines. 16 U.S.C. § 824 *et. seq.* FERC's transmission infrastructure investment rules

implement this statutory directive in a variety of ways, such as allowing full recovery of prudently incurred construction work in progress, pre-operations costs, accelerated depreciation, and full recovery of prudently incurred costs of abandoned facilities. 18 C.F.R. pt. 35.35.

There are other challenges besides financing. There is evidence that North America's grid-based bulk power systems are dangerously exposed to homegrown as well as foreign threats. The root of this exposure is in the shift from closed, proprietary control systems to increasing dependence on modern, standard platforms and applications. Driven by cost considerations and competition, utilities are adopting standard Internet protocol-based network technologies to tie into control systems, such as supervisory control and data acquisition (SCADA) systems and distributed control systems (DCS), for efficient management and communication across main stations and remote locations. The challenges facing North America's bulk power system are illustrated by the revelation that the Stuxnet worm ruined many of Iran's uranium enrichment centrifuges. *See* William J. Broad, John Markoff, and David E. Sanger, *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, New York Times (Jan. 11, 2011) at A1. We face the danger that similar technology could get into the hands of people intent on crippling North America's bulk power system.

Smart Grid Development

In the Energy Independence and Security Act (EISA) of 2007, Congress established the development of a Smart Grid as a national policy goal. Pub. L. No. 110-140, title XIII (codified at 15 U.S.C. § 17381 *et seq.*). EISA directs the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) to coordinate the development of a framework to achieve interoperability of smart grid devices and systems and to maintain the reliability and security of the electricity infrastructure. *See* www.nist.gov/smartgrid.

By adding monitoring, analysis, control, and communication capabilities to the national electrical delivery system, the Smart Grid will allow utilities to move electricity around the system as efficiently and economically as possible. Web-based portals and applications are essential to business, but they also open up electricity suppliers to the kinds of attacks that can plague financial institutions, online retailers, healthcare providers, and potentially nuclear power plant operations as evidenced by the Stuxnet infestation. Central control stations increasingly rely on standard Windows and Linux systems security procedures. A smart grid, however, is inherently more open as it marries information and automation technologies with our current electrical infrastructure. Unfortunately, the robustness of the Smart Grid and its capacity to evolve and reach its full capability is severely limited by the need to protect the system against hackers and cyber-terrorists.

Threats to grid cyber-security are growing in frequency and complexity and will require vigilance to thwart. According to Pike Research, the business segment that services the grid cyber-security market will likely see revenue grow to $3.7 billion annually by 2015. *Smart Grid Cyber Security, 2010*, http://news.cnet.com/8301-1009_3-10447430-83.html (2010). Pike Research also estimates that cyber-security spending will make up roughly 15 percent of total smart-grid capital investment by 2015 and that cumulative investment in the security sector could reach $21 billion between 2010 and 2015.

Critical Infrastructure Protocols

In this new environment, once-closed control systems will require comprehensive information security programs, with well-defined policies and processes supported by appropriate tools. Accordingly, FERC, under Section 215 of the Federal Power Act, adopted the once-voluntary NERC Critical Infrastructure Protocol (CIP) standards as the mandatory and enforceable Reliability Standard for the electric power industry. Order 706 (Docket RM06-22-000) *Mandatory Reliability Standards for Critical Infrastructure Protection Infrastructure Protection*, 122 FERC ¶ 61,040 (Jan. 18, 2008). The standards (CIP-002 through CIP-009) are designed to ensure that utilities, owners, and operators of the bulk power system in North America have appropriate procedures in place to protect critical infrastructure from cyber attack. The standards are enforced under Section 215 of the Federal Power Act by the eight regional reliability entities, NERC, and/or FERC.

The protocols mandate a broad range of security actions. The electronic security protocols (CIP-002, 003, 005, 007, and 009) require the utilities that make up the bulk electric system to maintain an inventory of all electronics that either are critical assets or necessary to the operation of critical assets. The physical security protocol (CIP-006) requires utilities to ensure the physical security of all critical cyber-assets. Requirements include installation of a physical security perimeter around all critical cyber-assets, identification and control of all physical access points to critical cyber-assets, and maintenance of an access log for all critical cyber-assets, via keycards, video, or manual log. The personnel security protocol (CIP-004) requires that each person who accesses critical cyber-assets, including the utility's personnel, contract workers, and vendors, must be investigated to assess the risk that he or she poses to security. The training and awareness protocol (CIP-004) requires that everyone who has access to critical cyber-assets, including the utility's personnel, contract workers, and vendors, must be trained regarding cyber-security. NERC's CIP-009 requires a recovery plan, including backup strategies, data restoration strategies, and spare parts and equipment. Finally, all CIP standards mandate documentation and review of all procedures and policies every year.

One of the most important aspects of these standards is the determination of whether an asset is deemed to be a "critical cyber asset" and thus subject to the CIP Reliability Standards, pursuant to an entity's risk-based assessment methodology. NERC defines "critical cyber assets" as "cyber assets essential to the reliable operation of critical assets" and defines "critical assets" as "facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System." NERC, *Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets* (2009). FERC adopted NERC's proposal that each responsible entity should develop its own risk-based assessment methodology to identify its critical assets. After receiving many comments on this issue, however, FERC required that NERC provide additional guidance on the development of the assessment methodology and identified certain issues that NERC should consider when developing its guidance. An analysis of these CIP Reliability Standards and NERC's assessment methodology guidance should be a critical part of each responsible entity's consideration.

In its January 2010 report, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0, NIST Special Publication 1108 (Jan. 19, 2010), NIST described a high-level

conceptual reference model to facilitate design of an architecture for the Smart Grid overall and for its networked domains. This publication included an initial set of seventy-five standards applicable to the Smart Grid, priorities for additional standards to resolve important gaps, an action plan under which designated standards-setting organizations will address these priorities, and an initial Smart Grid cyber-security strategy and associated requirements.

In September 2010, NIST issued its first Guidelines for Smart Grid Cyber Security, which include high-level security requirements, a framework for assessing risks, an evaluation of privacy issues at personal residences, and additional information for businesses and organizations to use as they craft strategies to protect the modernizing power grid from attacks, malicious code, cascading errors, and other threats. NISTIR 7628, *Guidelines for Smart Grid Cyber Security v1.0* (Sept. 2010). These guidelines identify 137 interfaces—points of data exchange or other types of interactions within or between different Smart Grid systems and subsystems. The *Guidelines* report "drills down" from the initial release of the *NIST Framework and Roadmap*, providing the technical background and additional details that can inform organizations in their risk-management efforts to securely implement Smart Grid technologies. The second volume of this three-volume set of guidelines focuses on privacy issues within personal dwellings. It covers topics such as evolving Smart Grid technologies and associated new types of information related to individuals, groups of individuals, and their behavior within their premises and whether these new types of information may contain privacy risks and challenges that have not been legally tested yet.

Cyber-security, such as that embodied in the critical infrastructure protocols, must balance the cost of implementing security measures against the likelihood and impact of any security breaches. This balancing of cost versus impact must take into account that excessive costs could impact customer rates but that inadequate security measures could allow unnecessary power outages to those same customers. The cost/impact balancing also must recognize that no single security measure is fully effective in preventing a security breach and that security breaches will undoubtedly occur. The multiple layers of security measures outlined in the critical infrastructure protocols must be applied and methods must be developed so that if one security barrier fails another is there to prevent intrusion. In addition, these protocols will provide mechanisms to create an audit trail for forensic analysis as well as possible legal actions.

Solar Electromagnetic Pulses

As if threats to our electrical power supply from cyber-attacks were not sufficiently challenging, on August 1, 2010, the Space Weather Prediction Center (SWPC) of the National Oceanic and Atmospheric Administration (NOAA) issued a warning that an electromagnetic pulse (EMP) from an impending solar storm might damage the electric grid in the United States. The alert warned that a Coronal Mass Ejection (CME) from the sun could affect Earth, noting, "There is a 10% chance that this CME will result in a severe geomagnetic storm." Peter Vincent Pry, *Senate Fumbles EMP Protection*, WorldnetDaily (Aug. 19, 2010).

A major solar storm in 1859 produced auroral displays and significant shifts of Earth's magnetic fields and caused several telegraph stations to burn down. Compared to today, the impacts of that storm were relatively minor because semiconductors were not in existence at that time and telecommunications were still in their infancy. Today, a major solar storm could severely damage electronic systems, including communication satellites, and cause continent-wide electrical blackouts. Storms of about half the intensity of the 1859 storm occur every fifty years or so; the last such storm occurred in November 1960, leading to world-wide geomagnetic disturbances and radio outages. Hearing Before H. Comm. on Homeland Security, Subcomm. on Emerging Threats, Cybersecurity, and Science and Technology, 111th Cong. (July 21, 2009) (testimony of Joseph McClelland, Director, Office of Electric Reliability Federal Energy Regulatory Commission). The National Academies of Sciences predicts that a solar geomagnetic storm as severe as the event that occurred in 1859 could cost $1–2 trillion and recovery would take four to ten years. National Academy of Sciences, Severe Space Weather Events: Understanding Societal and Economic Impacts (2008).

The grid is particularly vulnerable to solar storms because transformers are electrically grounded to Earth and susceptible to damage from geomagnetically induced currents. Damaged or destroyed transformers across the country would reduce grid functionality and prolong power outages. A repeat of the geomagnetic storm that occurred in 1859 would burn out and melt the copper windings and leads of approximately 350 of the highest-voltage transformers in the United States. These transformers weigh over 100 tons apiece and typically cannot be serviced in the field. Because of their size they cannot be flown in from overseas factories where they are currently made. National Academy of Sciences, Severe Space Weather Events: Understanding Societal and Economic Impacts (2008) at 77. Replacement would be slow: most transformers damaged by space weather incidents would not be repairable, and currently the world-wide waiting list for transformers is about three years. Stuart Burns, *The National Grid at Risk*, MetalMiner (July 22, 2010), http://agmetalminer.com/2010/07/22/the-national-grid-at-risk. The current solar cycle—climaxing in 2012 with possible major solar storms—bears a striking similarity to the one that produced the 1859 mega-blast. A repeat of such an intense geomagnetic storm would certainly disrupt life in the United States for years, perhaps even decades, to come.

According to one author of NAS's *Severe Space Weather Events*, the United States can protect its grid from solar EMP by outfitting it with surge suppressors. With about 5,000 transformers in the North American grid and each surge suppressor costing an estimated $50,000, the proactive course of action against solar EMP would cost approximately $250 million—a small fraction of what it would cost to repair the grid should a powerful solar storm impact Earth.

This problem received some legislative attention in the last Congress. House of Representatives bill H.R. 5026, known as The GRID Act (Grid Reliability and Infrastructure Defense Act), was approved by the House when it came to the floor on June 9, 2010. The bill would authorize FERC to mandate protection of the power grid from both man-made and solar EMP. The then-pending Senate energy bill made no mention of protecting the grid from EMP, only from cyber-attacks. These legislative initiatives expired with the end of the 111th Congress. Whether and how the 112th Congress will address twenty-first century protection of the grid, the most important engineering achievement of the twentieth century, are unknown.