

More than Compliance

The Future of Smart Grid

Jessica Lin

University Honors in Business Administration

Spring 2012

Capstone Advisor: Richard Linowes, Kogod School of Business

Table of Contents

Executive Summary.....2

What is the “Smart” Grid?.....3

Why Smart Grid? Problems with the Current Grid.....6

Environmental and Social Impacts.....6

Understanding Smart Grid Communication9

Securing the Smart Grid - Risk of Cyber Threats.....11

Smart Grid Threats – Case Study 15

Current Standards..... 16

Beyond Compliance Recommendations17

Conclusion22

Executive Summary

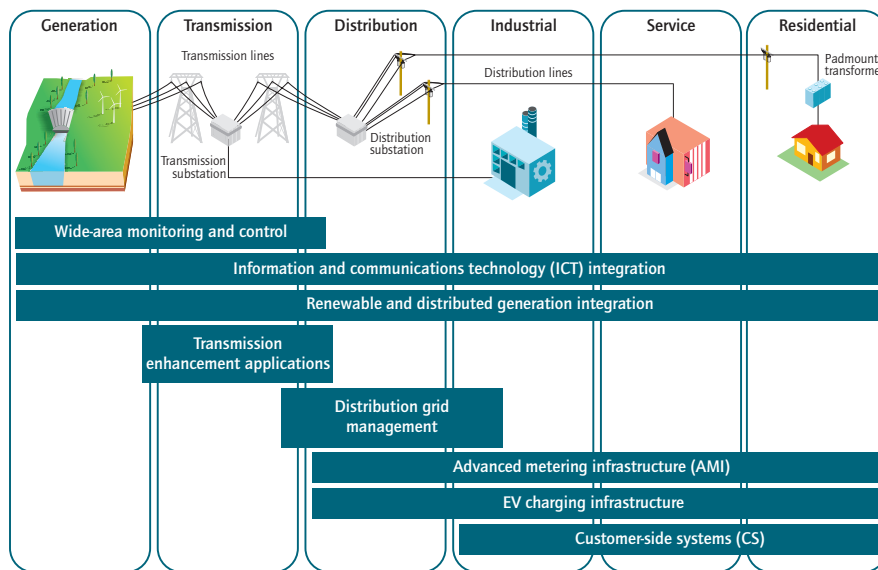
Considerably one of the most powerful infrastructures in the United States, the North American electrical system combines complex integrations of the electrical grid with reliable distribution of electricity to consumers across the country. However, with increasing demand of power and the higher costs of electricity, the U.S. infrastructure is no longer capable of providing reliable services while maintaining the grid. By 2020, the estimated costs of the electrical grid (\$197 billion) will be twice the amount of the investment now (\$107 Billion) to revamp the grid.

The United States recognizes this huge potential challenge and has planned an investment \$3.4 billion in investments as a part of the American Reinvestment and Recovery Act and will also match by industry funding for a total public-private investment of over \$8 billion¹. The deployment of smart grid technologies seeks to decrease utility bills for customers as well as decrease the negative impacts of power on the environment. The smart metering infrastructures installs a two-way communication between the utility and the customer, educating electricity use while simultaneously providing more control to the customer on their energy use. However, with the advanced technology come the threats from advanced cyber criminals. This capstone strives to create a comprehensive cyber security strategy for utilities with the advancement of technologies and the increased sophistication of cyber criminals.

¹ “Recovery Act: Smart Grid Investment Grants.” Office of Electricity Delivery & Energy Reliability. <http://energy.gov/oe/technology-development/smart-grid/recovery-act-smart-grid-investment-grants>.

What is the “Smart” Grid?

Because of the rapid change in technologies, experts, even in the energy sector, do not have a full definition of ‘Smart Grid’. The Department of Energy defines Smart grid as “a class of technology people are using to bring utility electricity delivery systems into the 21st century, using computer-based remote control and automation.”² Figure 1 shows the deployment of new technologies throughout the processes in smart grid. More



Source: Technology categories and descriptions adapted from NETL, 2010 and NIST, 2010.

KEY POINT: Smart grids encompass a variety of technologies that span the electricity system.

Figure 1: Smart Grid Technology Areas

*“Technology Roadmap – Smart Grid.” International Energy Agency. 2011
http://www.iea.org/papers/2011/smartgrids_roadmap.pdf*

² “Smart Grid.” Department of Energy <http://energy.gov/oe/technology-development/smart-grid>.

specifically, the Smart Grid is a new electric power system that monitors and controls grid activities through automation, and allows two-way flow of electricity and information between the power plants, the utility company and the consumers. Through the combination of new technologies involving complex networks and grid innovations, the smart grid will enhance efficiency and reliability by reducing the information gap between utilities and consumers through advanced metering infrastructure (AMI) and data management technologies.

Title XII of the Energy Independence and Security Act of 2009 highlights ten characteristics of a Smart Grid:

1. Increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid.
2. Dynamic optimization of grid operations and resources, with full cyber security.
3. Deployment and integration of distributed resources and generation, including renewable resources.
4. Deployment and incorporation of demand response, demand-side resources, and energy-efficiency resources
5. Deployment of ‘smart’ technologies (real-time, automated, interactive technologies that optimize the physical operation of appliances and consumer devices) for metering, communications concerning grid operations and status, and distribution automation.
6. Integration of ‘smart’ appliances and consumer devices
7. Deployment and integration of advanced electricity storage and peak-shaving technologies, including plug-in electric and hybrid electric vehicles, and thermal-storage air conditioning
8. Provision to consumers of timely information and control options
9. Development of standards for communication and interoperability of appliances and equipment connected to the electric grid, including the infrastructure serving the grid.

10. Identification and lowering of unreasonable or unnecessary barriers to adoption of Smart Grid technologies, practices and services.

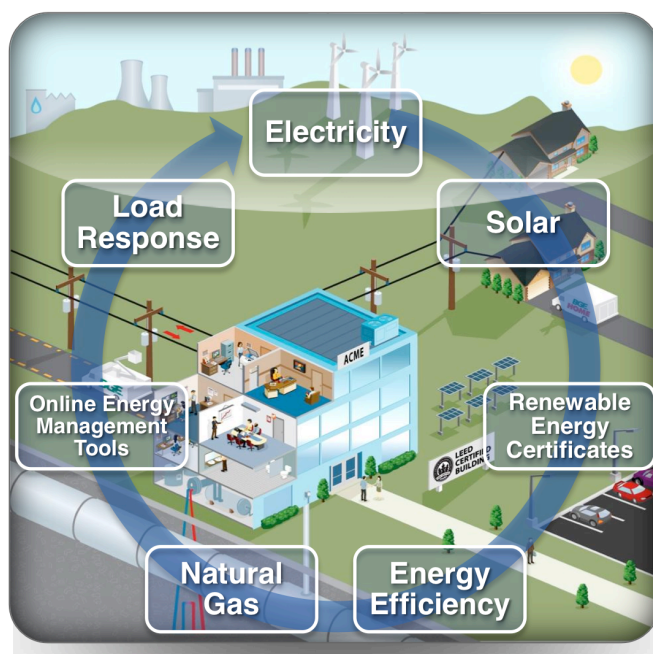


Figure 2: The Future of Power

Connaughton, Jim. "Energy Policy." 25 October 2011
American University Presentation

combination of industrial generation and technology provides the consumers with smart demand responses, leading to better load responses and better reliability.

For consumers, the benefits of smart grid are the reduction in utility bills due to better meter readings as well as the ability to control energy use remotely. Dynamic pricing by the utilities through the two-way communications increases education of peak hours and when to use energy at its cheapest. The differentiated pricing plans could result in reduction during the peak load by 34%, balancing the grid by shifting demand³. By balancing the grid, the utility will then be able to provide more reliable service and for the consumers, this means less electrical outages. With remote energy control, consumers

³ "Environmental Impacts of Smart Grid." National Energy Technology Laboratory. 10 January 2011. PDF

Along with the interconnectivity of smart grid, it additionally recognizes the necessity of smooth interoperability with green energy technologies. Figure 1 exhibits the future of the power system and the consumers. The future of power combines the generation from solar and renewable energy sources with online energy management tools brought by smart meters. This

can essentially manage the appliances in their phone wherever they are. Forgot to turn off the lights in the kitchen? The future of the smart grid allows consumers to log into an online application and determine which appliances or lights need to be shut off or turned on.

Why Smart Grid? Problems with the Current Grid

The current electrical grid is built on old technologies that cannot handle the increased usage. Because of this increased demand for reliable electricity and the lack of supply, the system constraints worsen and reliability issues increase. The 2003 Northeast Blackout had an economic loss of \$6 billion – and the blackout lasted around 7 hours to a couple of days. According to the Department of Energy, the current grid is estimated to cost more than \$100 billion average per year, doubling the cost of electricity in real terms. With the Smart Grid, the potential for increased reliability is high and concurrently, there will be decreased reliance on foreign energy sources.

The initial investment for a great American grid turnover would be roughly \$107 billion, as of 2012; however, according to the American Society of Civil Engineers, without this revamp investment, the cost of the grid for United States households and businesses could be upwards of \$197 billion by 2020⁴. This means that utilities and their customers can save \$100 billion in future costs by investing now; furthermore, that \$100 billion savings will undoubtedly increase as the technologies advance.

⁴ St. John, Jeff. “US Grid Has \$107B in Investment ‘Gaps’ by 2020.” Green Tech Media. 26 April 2012. <http://www.greentechmedia.com/articles/read/u.s.-grid-has-107b-in-investment-gaps-by-2020/>.

Environmental and Social Impacts

The major justifications for the smart grid, beyond reliability, are economic and environmental. The United States Department of Energy defines the goals of the smart grid as follows⁵:

- Ensuring its reliability to degrees never before possible
- Maintaining its reliability
- Reinforcing our global competitiveness
- Fully accommodating renewable and traditional energy sources
- Potentially reducing our carbon footprint
- Introducing advancements and efficiencies yet to be envisioned

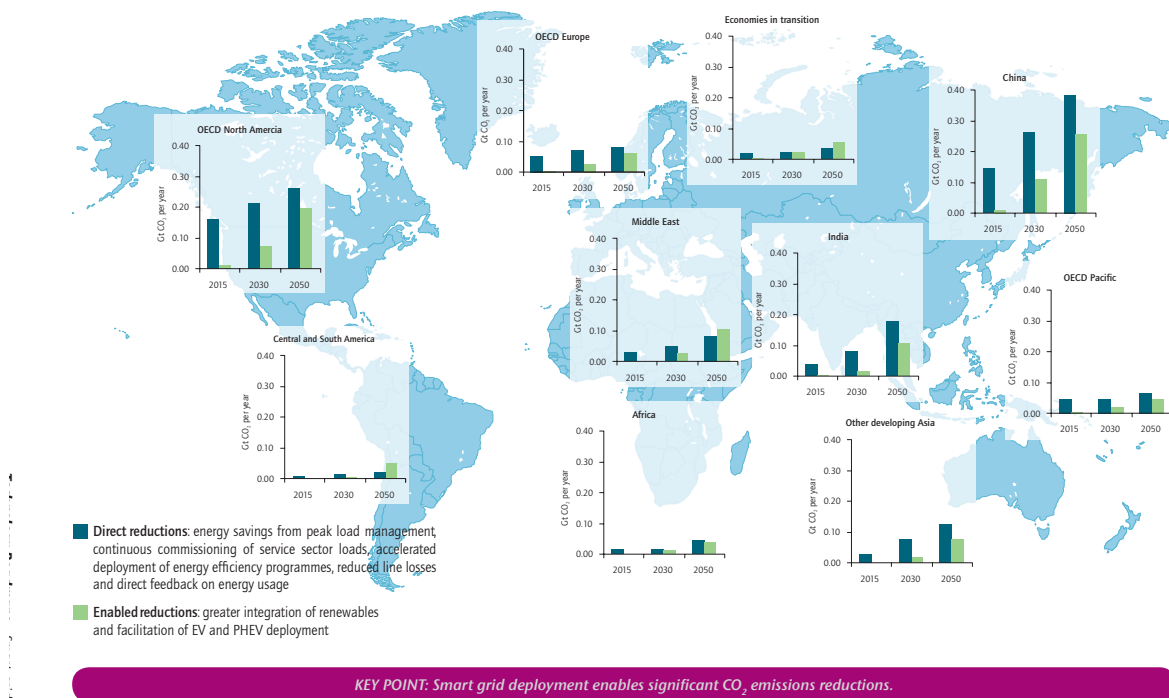


Figure 3: Regional CO₂ Reduction from Smart Grid deployment

Both direct reductions, in dark blue, and enabled reductions, in green, have significant environmental impacts globally. *Source: "Technology Roadmap – Smart Grid." International Energy Agency. 2011 PDF*

⁵ The U.S. Department of Energy. "Technology Providers." 2009
<http://www.oe.energy.gov/DocumentsandMedia/TechnologyProviders.pdf>.

The strong environmental impact of a better grid promotes the investment in smart grid. Smart grid provides the opportunity to integrate renewable energy easily while simultaneously handling increasing demand of electricity. Because of its better interoperability with green energy sources, such as solar and wind, the Smart Grid promises to reduce carbon emissions by 15% by 2020. It is expected to reduce household electricity bills by 10% due to more accurate readings from smart meters. The real-time metering allows two-way communication between a central control point and every meter within the architecture. This information from the smart meter technology then permits customers to monitor consumption habits in real time and improve energy efficiency and usage. The two-way communication also increases the reliability of the grid with real-time communication so the power company can immediately remediate an issue.

A simple way the Smart Grid would reduce carbon emissions is by customer education about their electrical use during peak hours, also known as demand response. Demand response, according to the Federal Energy Regulatory Commission (FERC), is “changes in electric usage by end-use customers from their normal consumption patterns in response to changes in the price of electricity over time, or to incentive payments designed to induce lower electricity use at times of high wholesale market prices or when system reliability is jeopardized⁶.” The two-way communication of the advanced metering infrastructure allows dynamic pricing and concurrently lays out the times of high electricity prices for consumers. Additionally, demand response is affected by

⁶ “Environmental Impacts of Smart Grid.” National Energy Technology Laboratory. http://www.netl.doe.gov/energy-analyses/pubs/EnvImpact_SmartGrid.pdf.

distributed generation sources, mostly from renewable energy sources, thereby reducing carbon emissions from coal generation.

Understanding Smart Grid Communication

Essentially, the basic definition of a ‘smart’ grid is computerizing the electrical grid. The Department of Energy defines the key feature of the smart grid is automation technology that lets the utility adjust and control each individual device or millions of devices from a central location⁷. The smart grid infrastructure consists of smart meters connected to consumers’ homes and a remote data management center, monitoring and controlling the meter usage. Figure 2 displays the interconnected systems between customers and all of the functions of the grid, with all functions connecting by to the operations, also known as the

command center. Through multiple network routes, domains are connected to each other; however, each domain is also considered a segmented entity.

About 60 million smart meters are expected to be deployed across the United States by 2019,

giving customers unprecedented access to information and control over their electricity use⁸. The costs associated with the deployment of each smart meter are around \$50 to

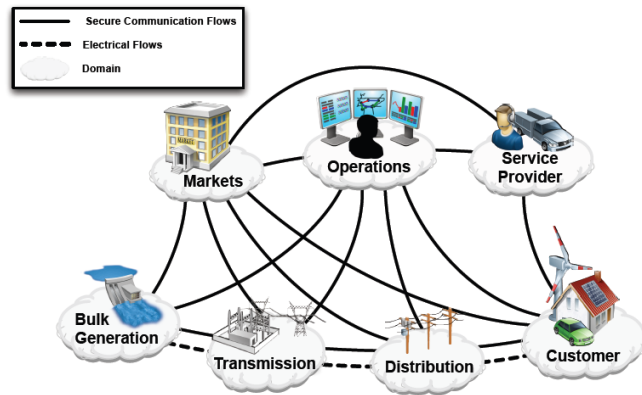


Figure 2. Interaction among actors in Smart Grid domains through secure communication flows and flows of electricity.

Source: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0 (NIST SP 1108)

⁷ “Smart Grid.” Department of Energy <http://energy.gov/oe/technology-development/smart-grid>.

⁸ “Smart Grid.” Department of Energy <http://energy.gov/oe/technology-development/smart-grid>.

\$200 per unit.⁹ The system architecture of the Advanced Metering Infrastructure (AMI) includes a meter, a collector, a meter control system, and a meter data management. Each device associated with the grid is given two-way digital communication technology and sensors to gather data and communicate that data to utility's network operations center via a wireless network. The AMI realizes the need of real-time meter readings, providing utility services remotely to consumer and aggregate energy usage. This may represent more exact billing information.¹⁰ More importantly, for the utility, the goal of the smart metering program is to change the behavior of the consumer so the utility companies can also reduce its costs and overhead to further improve the quality of service. Through a wireless network, consumers, incentivized to monitor their energy use, can control the power in their homes, remotely turning on or shutting off lights and appliances.

The potential for advanced metering infrastructure is beyond basic consumer savings in utility bills and rather includes consumption data analysis, capacity planning, demand management, rate design, and reduction of peak power consumption. Because of the constant push and pull of data between two systems, the utilities have a more detailed view of consumer energy use, including consumption patterns. This information can then lead to better delivery efficiency and reliability. Furthermore, according to Greentech Media Research, along with eMeter, a Siemens Business, the data analytics delivered by smart meter technologies has the opportunity to integrate electric vehicles smoothly and

⁹ Sorebo, Gilbert N. & Echols, Michael C. Smart Grid Security: An End-to-End View of Security in the New Electrical Grid. Taylor & Francis Group, LLC. Florida, 2012. 52

¹⁰ Sorebo, Gilbert N. & Echols, Michael C. Smart Grid Security

accommodate the necessary power demanded through analyzing its charging trends and identifying changes in distribution sizing¹¹.

The traditional electrical utility runs in three steps – generation, transmission and distribution. The smart grid will incorporate the three phases in addition to distributed generation, incorporating energy from different resources. With the modern, smarter grid technologies, the adaption of operational communication and technologies across all segments is integral. Along with operational communication and technology, security analysts must be integrated in all operations across the grid because of the potential risks.

Securing the Smart Grid - Risk of Cyber Threats

Smart Grid technologies were partially created in order to incentivize energy users to change their behavior; the technology reads and understands how a person uses energy during different hours of the day. However, this poses a huge risk for the utility's customers – if a malicious third-party hacks into the smart metering system and collects the data on customers' usage, that third-party can essentially manipulate the appliances and electricity connected to the metering system. The inherent two-way communication between electric systems and the deployment of a large number of devices located outside of the controlled utility environments suddenly introduces many more potential access points for cybercriminals. There are three inherent vulnerabilities in the Advanced Metering Infrastructure¹²:

1. Components physically available to anyone

¹¹ "Understanding the Potential of Smart Grid Data Analytics." eMeter & GTM Research. January 2012 <http://www.emeter.com/documents/anylst-papers/Understanding-the-Potential-of-Smart-Grid-Data-Analytics.pdf>.

¹² Sorebo, Gilbert N. & Echols, Michael C. Smart Grid Security – An End-to-End View of Security in the New Electrical Grid

2. Components communicate to IT systems through authorized access point
3. Utilities are reliant on telecommunication providers for protection from collectors

A major risk found by IOActive, a security services firm, is that “hackers could hack into smart meters to take command control of the advanced metering infrastructure, allowing for the en masse manipulation of service to homes and businesses.”¹³ Because smart grid encompasses the ‘computerization’ of the electrical grid, the risks and threats display similar aspects; threat vectors for the smart grid include access points, remote access points, physical access points and so forth.¹⁴ The remote access attack can include “denial of service” attacks that, in simple terms, put the utility in the position in which it is completely blind to any aspect of the grid. The risks that only applied to financial institutions are now very relevant to the utility infrastructure and utility information technology.

Additionally, the increased number of interconnections presents more opportunities for “denial of service” attacks, malicious code in software or firmware, compromised hardware, privacy and confidentiality breaches, and so forth. Each smart meter deployed could be a potential entry for attack. Because the integral design of the smart meters calls for remote control, the impending threat would remotely manipulate the smart meters. These attacks can direct increased energy use and further espionage of consumers’ financials and private information. A basic, blended attack can be such that a cyber criminal monitors the consumers’ energy behavior, recognizes time periods when no one is home, and breaks into the home. Another example of a straight-forward attack

¹³ Ebinger, Charles & Massy, Kevin. “Software and Hard Targets: Enhancing Smart Grid Cyber Security in the Age of Information Technology.” Energy Security Initiative. February 2011. Policy Debrief. 8

¹⁴ Sorebo, Gilbert N. & Echols, Michael C. Smart Grid Security 244

on the utility computer system would be the breach of the utility with a 3 million-person customer base, stealing the social security numbers of each consumer; if we estimate the identity protection costs of each person affected by the attack to be between \$5 and \$15, then the utility is liable for \$15,000,000 per month for every month for the life of every customer.¹⁵ In essence, the risk associated with cyber threats costs multiple millions, and into the billions, more than the actual investment on the security.

Beyond network attacks through smart meters are the system and application attacks. Current grids and future smart grids use the Supervisory Control and Data Acquisition (SCADA) systems as an overarching system. At its initial stage, the SCADA systems seemed to be too obscure to be exploited by threats; however, the systems evolved and can run on common hardware and software platforms¹⁶. Because SCADA systems are often directly connected to the Internet, the systems have inherent vulnerabilities, allowing for remote control of the system. Similarly, application attacks are becoming increasingly common as people become more dependent on mobile phones and Internet. The widely marketable aspect of smart grid is the ability for consumers to control the energy use of their homes through the Web or smartphone applications. However, as seen through the attack on Google¹⁷, Web application security is not consistent with the rate of Web application deployment. The inherent vulnerabilities of

¹⁵ Flick, Tony & Morehouse, Justin. Securing the Smart Grid – Next Generation Power Grid Security. 26

¹⁶ Flick, Tony & Morehouse, Justin. Securing the Smart Grid – Next Generation Power Grid Security. 119

¹⁷ The 2009 Google Attack, more famously known as Operation Aurora, was a cyber attack through Microsoft Internet Explorer, exploiting Google and at least 20 other companies. The attack connected computer systems to a remote server after the user access a malicious webpage; through that connection, the intruders were then able to steal company intellectual property and gain access to user accounts. To learn more, go to <http://www.mcafee.com/us/threat-center/operation-aurora.aspx>.

the web applications allow a petty cyber criminal or someone who is just having fun to have the ability to turn on the lights of an entire community or manipulate a light show at his or her leisure.

In the 2009 Black Hat Conference, ioActive, a leading computer security services provider, demonstrated the potential for the sabotage of an entire smart meter network. This potential of remote disconnect and manipulation of demand response programs needed for reliability is of the biggest concern, according to the North American Electric Reliability Corporation (NERC). Additionally, Michael Assante, President and CEO of NBISE, states that utilities should be most concerned with attacks that manipulate the digital targets in an unintended fashion, not just the disabling of the targets¹⁸. As attacks become more complex and display an uncertain level of intricacy, security measures need to be able contain them as well as strive for minimal damage. Ignoring the issues simply will not make it disappear.

In March 2012, nCircle, a leader in security compliance auditing solutions, partnered with EnergySec, a Department of Energy funded public-private partnership that works to enhance the cyber security of electric infrastructure, to survey over 104 energy security professionals. The survey showed the following results¹⁹:

- 61% of energy security professional do not believe that current smart meter installations have sufficient security controls to protect against false data injection;
- 75% of energy security professionals believe smart grid security has not been adequately addressed in smart grid deployment;

¹⁸ Assante, Michael. "Smart Grid a Transformation – Implications for our Workforce." Smart Grid Security East. 2011. Keynote Address http://www.youtube.com/watch?v=i7X_dv_UUYU.

¹⁹ "Security and Compliance Trends – nCircle 2012 Smart Grid Cyber Security Survey." nCircle http://www.ncircle.com/index.php?s=resources_surveys_Survey-SmartGrid-2012.

- 72% of energy security professionals believe smart grid security standards aren't moving fast enough to keep up with deployment

Because of the major push of smart grid technologies in the energy sector, new cyber security standards have not been able to keep up. Similar to a double-edged sword, the United States cannot suffice with the current grid; yet, the new grid presents a new realm of threats. A major challenge facing cyber security and smart grid is the maintenance of reliable systems. In order to implement security controls for the smart grid threats, redundant controls may be absolutely necessary; however, these extra controls potentially hinder the performance of the utility technology. Increasing encryption levels and adding authentication controls could add more costs and processing power for the smart meters, but lax encryption keys imposes a major threat for the metering systems.

It may seem unreasonable that any individual or entity would want to attack the American power grid; however, according to the National Security Agency (NSA), Russia and China have both “probed the electrical grid to find vulnerabilities to exploit it if they needed to attack it.”²⁰ While the likelihood of an attack on the US electrical grid may be low now, any opportunity or motive could set off a significant attack. The potential liabilities and costs, as well as general panic, ensued by the shut down of an infrastructure as enormous as the grid are matters of national security.

Smart Grid Threats – Case Study

According to Joe Weiss, a managing director of Applied Control Solutions LLC, internet-based terrorists would be capable of causing blackouts “on the order of nine to

²⁰ Wingfield, Brian. “Power-Grid Cyber Attack Seen Leaving Millions in Dark for Months.” Bloomberg 1 February 2012. <http://www.bloomberg.com/news/2012-02-01/cyber-attack-on-u-s-power-grid-seen-leaving-millions-in-dark-for-months.html>.

18 months” by disabling critical systems.²¹ However, many utility companies remain ignorant to the threat because utilities do not consider themselves as a traditional target for cyber espionage.

The 2010 Stuxnet attack in Iran displayed the potential of the manipulation of an industrial grid to target utility generators; the Stuxnet worm is currently being called the “most sophisticated cyberweapon ever deployed.”²² Stuxnet is an advanced malware discovered in July 2010, which attacked and infected at least 22 manufacturing sites including one U.S. manufacturing plant. Experts dissecting the malware determined that it had been built to manipulate nuclear centrifuges and to send the centrifuges out of control by a change in rotational speed of the machinery. Additionally, in order to not be recognized, the worm was designed to record the normal operations of the nuclear plant and to play it back while the worm was destroying the centrifuges.²³ It demonstrated the ease of attacking a central control system network through external devices, including infected laptops and project files. Furthermore, due to the sophistication of the weapon, Stuxnet exploited the system for an extended period of time without any detection. Because of the multiple pathways, such as remote contractors and control networks, it provided numerous avenues for the bug to disrupt the system.

Current Standards

The North American Electric Reliability Corporations has also created a set of cyber security standards, which have been reviewed and approved by the Federal Energy

²¹ Wingfield, Brian. “Power-Grid Cyber Attack Seen Leaving Millions in Dark for Months.”

²² “Stuxnet.” New York Times Topics. 15 January 2011.

http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_malware/stuxnet/index.html?8qa.

²³ “Stuxnet.” New York Times Topics. 15 January 2011

Regulation Commission (FERC). Utilities can be fined as much as \$1 million a day for violations and noncompliance. NERC's 8 Critical Protection Reliability Standards for the bulk power system serves only as a compliance measure for the current grid. The smart grid encompasses far more risks and cyber threats that are not addressed.

After the recognition of smart grid cyber security issues, the National Institute of Standards and Technology (NIST) created a comprehensive guideline for smart grid cyber security. Under the Energy Independence and Security Act (EISA) of 2007, the NIST has "primary responsibility to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems."²⁴ However, the EISA does not have a fully developed definition for "full cyber security," making the process for a cyber security framework ambiguous. As of February 2012, NIST has created an updated Framework and Roadmap for Smart Grid Interoperability Standards, released to improve compliance measures for utility companies across the country. NIST has developed a three-phase plan for smart grid standards; to accelerate the identification of existing standards applicable to the smart grid and establish a consensus; establish a Smart Grid Interoperability Panel (SGIP) that sustains the development of additional standards; and to create a conformity testing and certification infrastructure.²⁵

Beyond Compliance Recommendations

The bottom line is that a cyber intrusion occurs every 5 minutes. Any company can find the inherent business value in good security practices, not only for the customer but

²⁴ Section 1301 of the Energy Independence and Security Act of 2007 (P.L. 110-140).

²⁵ "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0." NIST Special Publication 1108R2, February 2012. 6
http://www.nist.gov/smartgrid/upload/NIST_Framework_Release_2-0_corr.pdf.

also, more importantly, for the business. In an enormous infrastructure like the electrical grid, reliability becomes the largest issue, especially when developing a comprehensive cyber strategy with active controls. The grid functions smoothly because of a weaker encryption key; with stronger encryption keys, more processing power will be needed. This further increases costs in the deployment of smart meters and garners less reliability, because costs need to be cut somewhere.²⁶ However, the sophistication of today's cyber threat requires stronger encryption and a full-bodied cyber security strategy. The cyber security in place must be beyond compliant to current laws and standards simply because the government has not caught up to the technological changes. Rather than being reactive to vulnerabilities, cyber security strategies should use risk-based techniques and be proactive in its defense. Thus, smart grid companies' cyber security plan must include:

- **Security Awareness Program** - Internally, CEOs, Presidents, CFOs and investors need to have a basic concept of the technical risks involved in the operations of the grid; this understanding will ensure and protect the company to the best of its capabilities as well as protect customers' security and privacy. The issues with cyber threats are no longer a problem for the Information Security Officers; directors across the board should understand the implications of the decisions being made. Best practices within the data management control center should be implemented, including a level of education related to control systems security and additional training for risks as the advancement of technologies continue.
- **Access Restrictions** – The dynamic and complex nature of the smart grid and the multiple networks it connects complicate traditional security measures. However, at its core, the utility company should enforce restrictions in the segmented domains and networks. Utilities must regulate how each of the networks and domains connect with one another and restrict access for each of them. For

²⁶ Sorebo, Gilbert N. & Echols, Michael C. Smart Grid Security, 65

example, smart devices associated with the Customer should not communicate with plant control systems in the Bulk Generation domain.²⁷

- **Authentication & Encryption**– Strong authentication methods include at least two of three authentication categories – Something I know; Something I possess; and Something I am. For example, a two-factor authentication method would be a password for the smart meter (Something I Know), and then scanning of a smart card (Something I Possess). Additionally, two-factor authentication should be included in any web-application or mobile application. The authentication component is typically the first vulnerability a cyber criminal will exploit; therefore, companies need to ensure that the basic vulnerability is covered. Ensure the integrity of the AMI architecture with two-factor authentication methods. With encryption, although stronger encryption calls for more processing power, it is nonetheless required. Another potential solution is SEED-based key. The SEED-based key exchange allows meters to understand the algorithm to decrypt a key without having to store the key in its memory.²⁸ This system would only allow one-way communication down from the meter control system to the meters and collectors; the meters and collectors then can only initiate requests if the meter control systems allowed it. Strong authentication methods would be necessary if the consumers want to directly log into their own meter control system.
- **Strong Logging Accountability** – In the case of a breach, strong logging capabilities come in handy when instigating forensics. Utilities should implement logging and monitoring on all devices within the application, operating system and network level. These measures provide the basic intrusion detection logs as well as intrusion prevention.
- **Whitelisting and “Deny by Default” Firewalls** – Because of the push and pull aspect of data, the firewalls implemented by utilities should have default deny rules for all inbound and outbound access. By placing these default to deny rules,

²⁷ Flick, Tony & Morehouse, Justin. Securing the Smart Grid – Next Generation Power Grid Security. 116

²⁸ Sorebo, Gilbert & Echols, Michael. Smart Grid Security, 65

the utility will minimize the probability that a successful compromise of an internal asset is able to communicate with a remote command and control server²⁹.

- **Robust Penetration Testing**– Penetration testing is the most important method in preventing threats through proactive defense. Robust and consistent testing identifies and exploits flaws in applications and controls set by exploiting the perimeter security controls to access internal data. It recognizes the high probable potential of a risk or threat in the systems and allows for constant updates. Dynamic penetration testing must be conducted within each separate segment of the smart grid technologies.
- **Incident Response Plan** – Procedures for recovery must be put into place in case of an attack. Count on being attacked, rather than being ignorant to the impending threat. Utilities should assume a breach will take place and have appropriate measures to remediate and contain the breach. Containment should stop the threat, if possible, and more importantly, the systems should continue to operate for business continuity. Within the plan, patch management and remediation tactics contain the attack and also reimages data. After these containment measures, a root cause analysis must be performed to ensure that the right controls are set for future defense. For example, the Incident Response Plan should include the remediation actions if multiple AMIs are compromised at the firmware level). Additionally, an incident response plan creates a framework for business continuity in case of a utility breach;
- **Resilience Plan** – A comprehensive Patch Management Program provides a preventative measure for the grid, although it does not fully protect against unknown vulnerabilities. Patches must also be audited and updated frequently, including after penetration testing. Additionally, not only is security needed in the database and application level, but also the hardware level. Developing the appropriate methodology to prevent the various threat vectors is obligatory for a sound resilience plan.

²⁹ Flick, Tony & Morehouse, Justin. Securing the Smart Grid: Next Generation Power Grid Security. p155

- **Internal Monitoring** – Cyber criminals are not only malicious outsiders; they can also include the internal threats, leaking sensitive data. Utilities need to recognize that it is unnecessary for certain staff members and even directors to have access to sensitive information. There is no reason to increase the risks of an internal malicious actor when a simple solution is in place.
- **New partnerships** that embrace expertise and redefine relationships from suppliers to partners. Utilities should implement **Active Supply Chain Monitoring**, which includes source code review of any applications and devices used on the grid. Additionally, in the investment of smart meters and other impending smart grid technologies, utility companies must demand the security compliance measures of these components. Legal contracts between the supplier and the company must be robust; however, utilities must recognize that the power grid infrastructure is liable for any damages, not the supplier. Therefore, utilities need to ask the smart meter vendors the right questions such as - What security events are logged by the smart meters? What protects communications from one smart meter to another? What are the configuration options within the smart meter and what have you implemented?³⁰
- **Investment in Research & Development** – In a Bloomberg survey of network managers at 21 energy companies, utilities average around \$45.8 million a year on computer security, preventing 69% of *known* cyber strikes against their system. In the upcoming year or two, companies estimate an increase annual spending of around \$69.3 million to avert 88% of attacks.³¹ However, these investments are for the current grid, rather than the increasing deployment of smart grid technologies. In order to protect and resist cyber threats, budgets for investment in cyber security must increase dramatically. According to a 2011 study by the Electric Power Research Institute, power companies will need to spend about \$3.7 billion between now and 2030 to protect against cyber threats on the smart grid.³² For utilities to maintain competitive advantage as well as simply having good

³⁰ Sorebo, Gilbert N. & Echols, Michael C. Smart Grid Security 69

³¹ Wingfield, Brian. "Power-Grid Cyber Attack Seen Leaving Millions in Dark for Months."

³² "Estimating the Costs and Benefits of the Smart Grid: A Preliminary Estimate of the Investment Requirements and the Resultant Benefits of a Fully Functioning Smart Grid." Electric

business practices, it must set priorities and find the balance between reliability and security for its consumers.

Additionally, utilities across the line, including generation and transmission, should push United States for dynamic compliance measures, being proactive in its energy risk assessment rather than reactive to cyber attacks on the grid. Along the same lines, utility industries should engage in communication with appropriate government authorities to facilitate discussion about emerging threats and foreseeable vulnerabilities in order to have better preparation. Industries should communicate to the US government that its compliance measures and standards should not incentivize utilities to hide information on breaches and attacks; rather, the standards and compliance concerns should dynamically fit the changing environment.

Conclusion

The future of power is here with improving technologies created daily. Environmental impacts can no longer be ignored, and nation-states across the world recognize the need for investment. By 2018, the United States plans having a cumulative spending of \$14 billion for securing the US smart grid and its deployment, ensuring the improvement of the grid³³. However, with each technological advance on infrastructure, a case of strong security deployment is necessary. While the attack on the grid does not seem likely, given the right motivation and the capability, the smart grid could nonetheless be exploited. This potential exploitation has massive financial impacts not only for utility companies, but also for every entity that relies on electricity. Within the

Power Research Institute, 29 March 2011.
http://my.epri.com/portal/server.pt?Abstract_id=000000000001022519

next year or so, the average budget for security will increase to about \$69.3 million, averting 88% of attacks. Despite the percentage of intrusions averted, the new smart grid adds more points of intrusions and even more unknown gaps in security. Cyber criminals are smarter than ever, with more working for the 'bad guys' than the good. Utilities need to recognize the urgency of the matter and realize that compliance and 88% is no longer acceptable.

Works Cited

1. “Recovery Act: Smart Grid Investment Grants.” Office of Electricity Delivery & Energy Reliability. <http://energy.gov/oe/technology-development/smart-grid/recovery-act-smart-grid-investment-grants>.
2. “Smart Grid.” Department of Energy <http://energy.gov/oe/technology-development/smart-grid>.
3. “Environmental Impacts of Smart Grid.” National Energy Technology Laboratory. 10 January 2011. PDF http://www.netl.doe.gov/energy-analyses/pubs/EnvImpact_SmartGrid.pdf
4. St. John, Jeff. “US Grid Has \$107B in Investment ‘Gaps’ by 2020.” Green Tech Media. 26 April 2012. <http://www.greentechmedia.com/articles/read/u.s.-grid-has-107b-in-investment-gaps-by-2020/>.
5. The U.S. Department of Energy. “Technology Providers.” 2009 <http://www.oe.energy.gov/DocumentsandMedia/TechnologyProviders.pdf>.
6. Sorebo, Gilbert N. & Echols, Michael C. Smart Grid Security: An End-to-End View of Security in the New Electrical Grid. Taylor & Francis Group, LLC. Florida, 2012.
7. “Understanding the Potential of Smart Grid Data Analytics.” eMeter & GTM Research. January 2012 <http://www.emeter.com/documents/anylst-papers/Understanding-the-Potential-of-Smart-Grid-Data-Analytics.pdf>.
8. Ebinger, Charles & Massy, Kevin. “Software and Hard Targets: Enhancing Smart Grid Cyber Security in the Age of Information Technology.” Energy Security Initiative. February 2011. Policy Debrief.
9. Flick, Tony & Morehouse, Justin. Securing the Smart Grid – Next Generation Power Grid Security. Elsevier, 2010.
10. Wingfield, Brian. “Power-Grid Cyber Attack Seen Leaving Millions in Dark for Months.” Bloomberg 1 February 2012. <http://www.bloomberg.com/news/2012-02-01/cyber-attack-on-u-s-power-grid-seen-leaving-millions-in-dark-for-months.html>.
11. “Stuxnet.” New York Times Topics. 15 January 2011. http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_malware/stuxnet/index.html?8qa.
12. Section 1301 of the Energy Independence and Security Act of 2007 (P.L. 110-140).

13. "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0." NIST Special Publication 1108R2, February 2012. 6
http://www.nist.gov/smartgrid/upload/NIST_Framework_Release_2-0_corr.pdf.
14. "Estimating the Costs and Benefits of the Smart Grid: A Preliminary Estimate of the Investment Requirements and the Resultant Benefits of a Fully Functioning Smart Grid." Electric Power Research Institute, 29 March 2011.
http://my.epri.com/portal/server.pt?Abstract_id=000000000001022519