Teaching the Smart Grid: Why Data Management is Essential to the Future of Electricity

Alexandra Nilles
The Colorado School of Mines
2013 IEEE WISE Intern

Contents

1 Preface

1.1 About the Program

Founded in 1980, the Washington Internship for Students of Engineering (WISE) program is a collaborative effort between several professional engineering societies. The WISE goal is to bring together future leaders of the engineering profession in the United States who are aware of, and who can contribute to, the increasingly important issues at the intersection of science, technology, and public policy. Each student in the WISE program spends the summer researching a technology-relevant public policy issue in the heart of the nation's capitol. For more information please visit http://www.wise-intern.org/.

1.2 About the Author

Alexandra Nilles is majoring in Engineering Physics at the Colorado School of Mines, where she is also pursuing a minor in Public Affairs through the McBride Honors program. In the future, Alexandra plans to pursue a PhD in physics, and is interested in computational physics and materials. Alexandra is a member of the Society of Physics Students and enjoys exploring the Rocky Mountains and learning to dance in her spare time.

1.3 Acknowledgements

The author is extremely grateful to IEEE for the opportunity to live and research in DC. Dr. Ken Lutz was invaluable in the development of the ideas in this paper, and was very generous with his time and expertise. Special thanks go out to Erica Wissolik, for her organizational help and useful contacts, and to Chris Brantley for contacts and editing help. Thanks also go to Dr. Gail Marcus, the faculty member in residence, for all of her guidance and for planning all of this summer's experiences. Many other individuals and organizations were very helpful throughout the program, including many people at the Department of Energy, the National Institute of Standards and Technology, and the Federal Energy Regulatory Commission.

2 Executive Summary

The current condition of the US electric grid is inadequate and requires updates to be able to handle a changing landscape of energy generation and use. Efforts to shift to a "smart grid" have led to the collection of immense amounts of data. Currently, this data is not being used as effectively as it could be. Grid management is based on powerful computer models which use past behavior to predict current conditions on the grid. The ultimate goal of the smart grid is to have real-time data collection and analytic capabilities.

A paradigm shift is required to take advantage of new technologies and IT capabilities to create a truly "smart" grid, one that can respond in real time to events without needing human intervention. Our increasingly digital society is functioning on time scales that are much shorter, and complexity levels much higher, than human operators are able to deal with. The result may be increasing amounts of grid failure. The immense amount of technical research and development that has been done on new data architectures and analytics will be best implemented through a public-private partnership which is used to create and enforce standards for data formats and communications strategies.

This paper concludes that industry-developed standards, combined with public guidance and funding for sensitive issues such as privacy and cybersecurity, are the best tools to use as the smart grid develops. Government supervision and input can help the standards development process focus on long-term goals, such as establishing a Common Information Model (CIM) to assist with communication between sectors of the grid. Enforcement agencies such as FERC and NERC should incorporate these voluntary, consensus-based standards into regulation, while focusing on the areas of data management efficiency, privacy, and security.

3 Introduction

As the United States of America moves into the 21st century, its economy is becoming increasingly dependent on electricity. Online commerce requires stable power supplies for servers, defense installations need to have secure electricity sources in emergencies, and power outages cost our economy billions of dollars annually in lost hours of work [1]. It is a national imperative to maintain and improve electrical infrastructure.

The system that generates and provides electric power is called the electric grid. Often referred to as the world's largest machine [2], the grid is a complex technological network. The grid can be divided into three sectors: generation, transmission, and distribution. Generation includes all power plants and the infrastructure needed to create electricity. Transmission refers to the transfer of electric energy away from generators: this category includes the high-voltage power lines that stretch across the country. The transmission network is a highly non-linear system, with many interconnections and deliberate redundancies. Distribution describes the local substations that control and deliver electricity to consumers after it has been transported from the power plants. Distribution networks are generally radial: power lines extend away from substations to consumers, and are rarely interconnected after they leave the substation [3].

As new technologies are added to the grid, these previously defined boundaries are beginning to break down. For example, consumers can now produce electricity using solar panels or other generation methods. The distribution networks were not designed for this use, and the electrical sector needs to adapt. To this end, modern digital technologies are allowing us to collect data on electricity usage at an unprecedented rate. Currently, there is a need for a comprehensive and standardized method of organizing and using this data. This paper will explore the current physical and political state of US electric grid data management, and will investigate different options for managing smart grid data in a way that allows the US to optimize grid design without sacrificing security or privacy.

4 Background and Issue Definition

4.1 A Brief History of the Grid

The US electric grid was envisioned in the late 1800s, and the grid has been built organically (mostly through private enterprise) over the last century and a half. The grid was initially constructed from many small, isolated electrical networks, which became more and more interconnected as demand for electricity grew [4]. This interconnectivity was accelerated in 1992 with the passage of the Energy Policy Act. This act changed regulations in the energy markets and created today's economic environment, where electricity is treated as a commodity [5]. Before the 1990s, a single company would usually control generation, transmission and distribution for one geographic area. After deregulation, generation became a separate industry and electricity generated in one area was often sold to distant consumers. This increased the complexity and number of internal connections in the US electric grid.

Unfortunately, with increased complexity comes increased instability: a failure in one part of the grid has the potential to impact many other parts of the network. Combined with an aging infrastructure, this means that the US electric grid is becoming more expensive to maintain while power losses are becoming more frequent. Private spending to build and maintain infrastructure is up 43% since 2002, while the amount of downtime on the grid has increased about 10% (see Figure 1) [6].

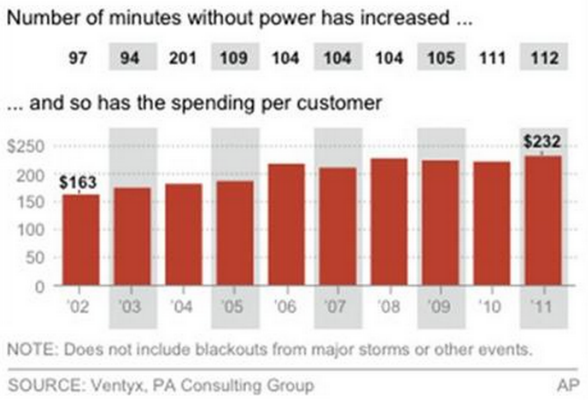

Figure 1: The effects of aging infrastructure and changing demand [6].

Adding to the stresses on the grid, many US states are currently establishing Renewable Portfolio Standards, which set requirements for how much of the state's energy must be provided by renewable sources [7]. However, renewable sources are often variable in nature: the wind doesn't blow at the same rate all the time, and the sun isn't always shining. In order to deal with this variability in supply, the grid will need to include sophisticated network designs and management algorithms that can match a constantly changing supply of energy to a constantly changing demand for energy. Data collection in the grid can play a major role in helping to develop and perform the complex calculations necessary to keep the grid stable. However, if the massive amounts of data collected are not managed correctly, negative consequences can arise.

As part of a policy effort to combat these problems, the Energy Independence and Security Act of 2007 set up various committees to investigate the possibility of a "Smart Grid." The legislation also assigned various responsibilities to the Department of Energy (DOE) and the National Institute of Standards and Technology (NIST). The current policy approach to the smart grid will be explained later in more detail, but first, the idea of a smart grid must be defined.

4.2 What is the Smart Grid?

The proposed "smart grid" is defined by NIST as "a modernized grid that enables bidirectional flows of energy and uses two-way communication and control capabilities that will lead to an array of new functionalities and applications" [8]. In order to develop this modernized grid, and facilitate "communication and control capabilities," owners and operators of the grid require more information about the status of the grid, and they need this information faster. As a result, an enormous amount of electrical metering and sensing technology is currently needed, as well as new communications pathways between groups that use, act on, and manage the grid. Figure 2 demonstrates how information domains such as markets and operations will be linked to physical domains such as generation and transmission in

the smart grid. The solid lines represent communication flows, while the dotted lines represent electrical flows. The importance of communication in the smart grid is clear, and well-managed data architectures are necessary to facilitate this communication.

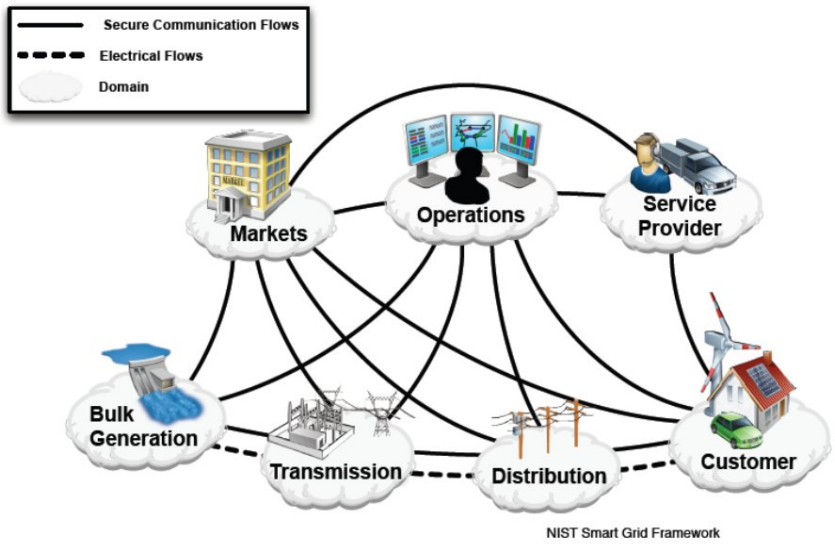

Figure 2: A representation of information and electricity flow in the smart grid [9].

One major source of data in the smart grid is the information collected by "smart meters." Smart meters are digital devices that measure the energy use of a consumer and are able to transmit that data at near real-time rates (typically once every 15 minutes to one hour) [10]. These meters are only one type of data collection device that will be part of the smart grid; other measurement tools will also be discussed, but smart meters will have the most visible impact on everyday consumers. The two-way communication cited by NIST is key to the use of smart meters. Traditional meters simply report data to the utility. Smart meters can potentially be used to communicate back to consumers and control their energy use, in order to better manage stresses on the grid such as peak demand.

Peak demand is a term used to describe a time period of very high demand for power. In the US, daily peak demand for a community usually occurs near the end of the traditional workday, as people come home from work and turn on lights, air conditioning, and other appliances. Electric utilities are required to build enough generating capacity (i.e. power

plants) to meet peak demand. Unfortunately, this means that much of this capacity goes unused during the rest of the day, when demand for electricity is lower. Peak demand creates both inefficiency and instability in the grid. The instability occurs because of physical stresses on the grid during large fluctuations in power use [11]. In order to reduce peak demand and "smooth out" demand for power throughout the day, smart meters can potentially communicate with homes or businesses to reduce energy usage at times of high demand. This is commonly referred to as a "demand response" strategy. See Figure 3 for an example of daily energy use and how demand response could reduce the effects of peak demand.

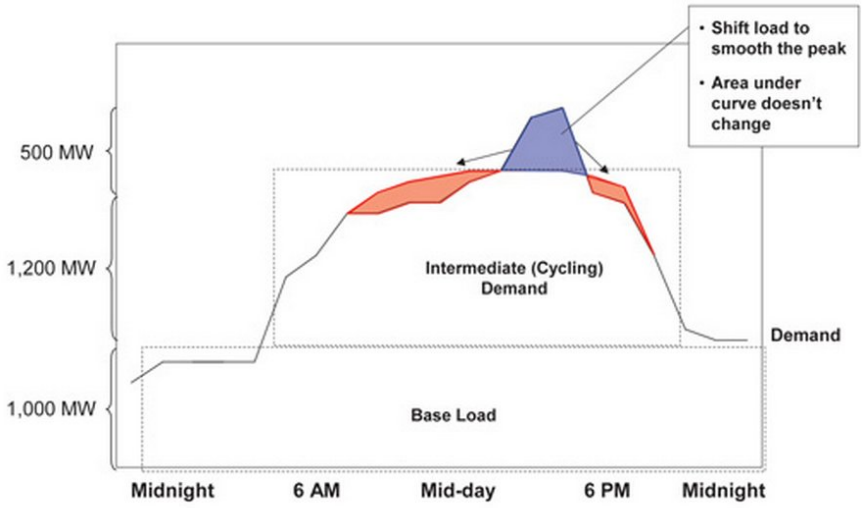

Figure 3: Example daily energy use [12].

An effective demand response strategy requires data collection and communication on a vast scale.

An additional characteristic of the smart grid includes using data to monitor grid infrastructure and sense when equipment is approaching failure, in order to prevent blackouts due to aging equipment. Many new types of digital sensors are being deployed, with another notable example being Phasor Measurement Units (PMUs), also called "synchrophasors." PMUs provide detailed information about voltage and current levels, frequencies, and phases. They can transmit 30 data points per second, as opposed to current sensors which send data

once every two to four seconds [13]. PMUs can be used to detect unusual stresses on the grid, and potentially could interact with technology such as switches to prevent damage to infrastructure. Ideally, smart grid data could be used in real time to control the flow and use of electricity in the grid.

Most of the technical details of such smart grid technologies are outside the focus of this paper. Instead, the focus will be on how government can help industry effectively manage the enormous amounts of energy consumption data, as well as the security and privacy implications of this data collection. Virtually every part of the electric industry could benefit from having more information and a faster response time to events on the grid, and public policy can help play a role in the coordination and management of this data usage.

4.3 The Importance of Data Management

The amount of data being collected on the grid is skyrocketing. About 10,000 terabytes of smart grid data were collected in 2010, and the number is expected to increase to 75,000 terabytes in 2014 [14]. By comparison, all of the information in the Library of Congress makes up about 15 terabytes. There is a very real danger of being overwhelmed with data. A study published in the proceedings of the Innovative Smart Grid Technologies Conference found that having smart meters that can control consumer energy use in response to electricity prices can cause chaotic fluctuations in price and energy use if the relevant data is not properly managed. The authors concluded that "it is possible that in a few years all of the smart meters and wind farms installed today will be regarded as another 'bridge to nowhere' unless we create the right architecture to make use of these resources" [15]. There are many possible data structures that have been developed out of research which could organize, simplify, and optimize data management for the grid. However, since the electric infrastructure is owned by many private companies, policy solutions are necessary to coordinate the management of the physical and logical structure of the grid.

There are three main areas of the smart grid that can be affected by policy. The first is infrastructure: policy can encourage investment in the physical power lines and monitoring systems of the grid. The second is management: government can help establish standards which make management approaches more uniform across the industry. The third policy-sensitive area is security: it is in the national interest of the United States to make sure that the electric grid is stable and protected from outside attacks. Data management involves all three of these areas: effective sensor infrastructure is necessary to collect data on grid behavior, the data must be managed in a standardized way to encourage effective data analysis on a nationwide scale, and the security and privacy of data and physical infrastructure must be assured. In order to effectively use data, policies need to encourage organized data collection and processing.

5 Current Policy, Stakeholders and Key Conflicts

Current US policy toward the smart grid was primarily laid out in the 2007 Energy Independence and Security Act [16]. This act assigned the Department of Energy (DOE) the responsibility of conducting smart grid research, development, and demonstrations. The National Institute of Standards and Technology (NIST) was given the mandate of developing and coordinating standards for smart grid technology.

One major player in energy regulation is the Federal Energy Regulatory Commission (FERC). FERC has jurisdiction over interstate energy transmission and markets. FERC issues and enforces regulatory requirements for interstate energy commerce, and thus has some authority to issue regulations pertaining to smart grid development and data management on a national scale.

In 2006, FERC appointed the North American Electric Reliability Corporation (NERC) to be the Electric Reliability Organization for the United States, a position which was created by Congress in 2005. NERC is a private organization with the authority to develop reliability

standards and can enforce compliance through financial penalties [17].

The American Recovery and Reinvestment Act of 2009 (ARRA) provided $4.5 billion to private electricity companies for the purpose of accelerating the development of smart grid technologies. It is estimated that by the end of 2014, this funding will have supported the deployment of 15.5 million smart meters [18]. Additionally, it is estimated that between 2010 and 2014 about 1,000 PMUs will be networked, many of which also used ARRA funding [13].

Since smart grid data collection technology was installed opportunistically, while funding was available, many private companies have not yet developed a comprehensive strategy for organizing and using the data provided by the meters. A 2012 survey of US utility companies found that "utilities tend to have last-gen business intelligence (BI) reporting solutions that they call "analytics," but that typically amount to not much more than reporting tools or descriptive analytics (primarily based on older database architectures running SQL), as opposed to the real-time and predictive software using complex event processing" [19]. Real-time analysis and response to data is the ultimate goal of the smart grid, but there are several challenges that must be overcome before this real-time capability can be implemented.

One major challenge is economic. Utility companies can be hesitant to implement untested technologies, as the financial consequences of failure are so large. Additionally, it is expensive and time-consuming to update software architectures, which means that many utilities are using outdated IT systems. Government policy must compete with the power industry's reliance on so-called "legacy" devices and systems, which NIST defines as technologies that "have aspects (including devices, systems, protocols, syntax, and semantics) that exist due to past design decisions, and these aspects may be inconsistent with the current architectural requirements of the Smart Grid and may not include the latest Smart Grid innovations" [9]. When policy requires improvements to the grid, these legacy systems must either be replaced or adapted to meet new requirements. These increased costs have the potential to generate strong private sector resistance to policy changes.

Another challenge when creating data management policy is the concern for consumer

privacy. A 2010 DOE report found that smart grid data collection could potentially contain information about consumers such as "daily schedules (including times when they are at or away from home or asleep), whether their homes are equipped with alarm systems, whether they own expensive electronic equipment such as plasma TVs, and whether they use certain types of medical equipment" [20]. This type of information is understandably sensitive, and smart grid policies must determine that the consumer's reasonable expectation of privacy is being met. At the same time, if access to data is controlled too strictly, it creates a barrier for utilities, academic researchers, or third-party application developers who need data to create new technologies.

The final major conflict that will be considered is the need to pursue cybersecurity for the smart grid. A May 2013 report from the House of Representatives concluded that "the electric grid is the target of numerous and daily cyber-attacks [and] most utilities only comply with mandatory cyber-security standards, and have not implemented voluntary NERC recommendations" [1]. Many important cybersecurity standards are currently voluntary, and take the form of a "checklist" of standards that private companies should meet. Additionally, upgrades to cybersecurity take money and time, while the likelihood or nature of a cyber attack is difficult to predict. A more holistic approach to cybersecurity is needed - one that is motivated by the immense potential costs of an attack on the grid. For example, a blackout in the Northeastern US in 2003 lasted two days and cost an estimated $6 billion, and placed immense stress on all consumers who lost power [21]. If an accidental outage could have such major impacts, the potential consequences of a malicious attack are quite intimidating. Much policy still needs to be developed to deal with this threat, as well as to deal with the issues of privacy and economics.

6 Policy Alternatives

When evaluating policy alternatives, there are several important factors to consider. First of all, the electric grid is entirely dependent on the private power industry, so policies which work against the financial interests of the private sector will encounter much resistance. Secondly, the importance of technology and innovation in solving the grid's problems cannot be understated - policies which limit innovation or restrict the use of new technological solutions will be harmful in the long run.

The overall goal of data management policy is to get the smart grid to a point where data can be collected, analyzed, and responded to in real time. There is an immense amount of work being done to overcome the technical barriers in this field, but many of the remaining barriers are political: an effective smart grid requires cooperation among members of a very competitive industry. The role of government is to coordinate efforts among local, state, and federal entities who are involved in the grid. Potential policy alternatives include government encouragement and coordination of standards development, the development of regulations based on standards, and financial support of infrastructure improvements.

6.1 Standards

The development of industry-wide standards is a crucial part of smart grid policy. The Energy Independence and Security Act of 2007 mandated that NIST has the "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" [16]. The key word in this mandate, especially when it comes to data management, is interoperability. When operators of the grid are attempting to use smart grid data to manage their assets, they need to take data from many different sources and integrate it, which means that data formats need to be compatible. A recent article in the IEEE Smart Grid Newsletter summarized the challenges surrounding data integration:

> "Asset management applications are heavily data driven requiring data from across the enterprise (from the Geographic Information System or GIS, the work management system, the maintenance management system, outage management system, on-line monitoring system(s), meter data management systems, equipment catalogs, standards, planning and archived operational histories). Often such information is lacking altogether or inaccurate. This is because information is siloed within various utility departments, without adequate integration at the backend. Manual data transfers and processes involving copy-paste and single point-to-point integrations make the process of asset management error-prone and in most cases very time consuming" [22].

In order to ensure that data and hardware for the smart grid will be useful across all domains of the power system, and to avoid the "siloing" of information, the Smart Grid Interoperability Panel (SGIP) was established by NIST to aid in the identification and development of standards for the electric industry. The SGIP is a public-private partnership with members that come from "all seven integrated domains of the power system - customers, markets, service providers, operations, bulk generation, transmission, and distribution" [23]. The members of the SGIP work together to identify a portfolio of voluntary consensus-based standards for many smart grid applications, including data formats and management.

There are many initiatives by NIST and the SGIP that are already working in the data-management sphere. Under the 2007 Energy Act mandate, NIST developed multiple priority actions, defining areas that are essential for developing interoperability for the smart grid. Many of these Priority Action Plans (PAPs) have been successful in creating or identifying consensus-based standards. For example, NIST and the Smart Grid Interoperability Panel have recommended that FERC consider the Common Information Model (CIM) standard that has been developed by the International Electrotechnical Commission (IEC), an international standards-developing organization [24]. The IEC defines their CIM as "a layered architecture which ensures implementation of standard methodology at each layer. Both information and context layers are semantic with the defined rules for translation to the implementable physical syntax" [25]. A CIM is essential for streamlining communication between all the different sectors of the grid. A way to visualize the structure of such com-

munications is the Open Systems Interconnection (OSI) model, as seen in Figure 4.

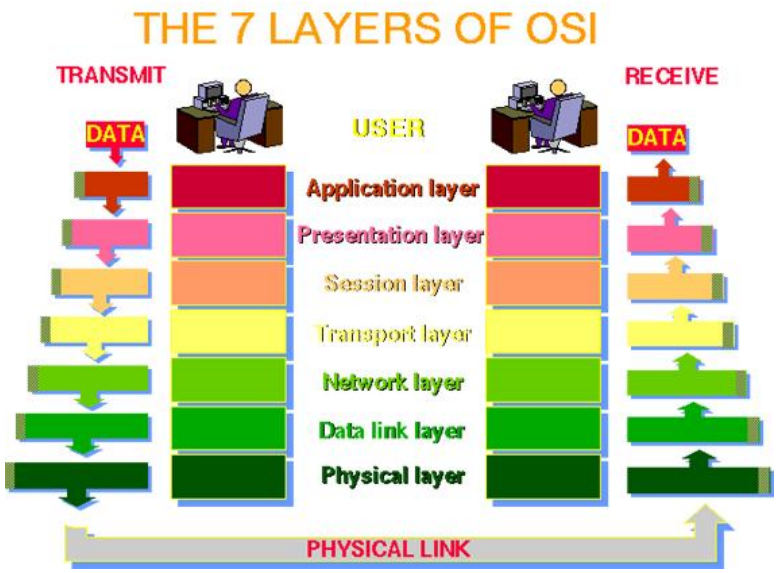

Figure 4: The Open Systems Interconnection communications model [26].

The "application" and "presentation" layers are the most important for developing data standards: the application level is where data interacts with software and the end user. The presentation layer establishes communication between entities on the application level, and this layer is where data translation and encryption would occur. A CIM would allow for a standard communications syntax that smart grid developers could use to ensure that application and presentation processes occur as efficiently as possible. This communication between different layers and sectors of the smart grid is essential as the grid becomes more complex.

When it comes to cybersecurity, government is currently the largest driving force behind standards development: "As a key element of the Recovery Act, DOE is leading an interagency team to develop the cybersecurity requirements that are needed for the Smart Grid. This Cyber Security Working Group (CSWG), a subgroup of the Smart Grid Interoperability Panel (SGIP), has producing cybersecurity guidelines that were published in the National Institute of Standards and Technology Interagency Report 7628" [27]. The large

role of government in cybersecurity standards-setting makes sense if the integrity of the grid is seen as an issue of national security, as well as an issue of interest to private companies. However, the effectiveness of nonenforceable standards must be examined.

Overall, standards creation is an effective method of influencing data management for several reasons. First of all, the process of writing standards involves many different stakeholders, so when consensus is reached, the likelihood of the standard being adhered to is much higher than if the standard was dictated without stakeholder input. Second, standards can help encourage innovation by providing consistent data formats or hardware specifications that entrepreneurs can depend on while creating new technologies. For example, if a third-party developer is trying to create a smart-phone app that helps consumers manage their energy use, it is immensely helpful if all utilities consistently make energy-use data available.

On the other hand, standards creation has some limitations as a policy tool. First of all, NIST and the SGIP have no authority to enforce these standards - they are entirely voluntary. Additionally, conformance with these standards is verified somewhat inconsistently. This can cause serious discrepancies in data quality. For example, one test found that readings taken by PMUs from different companies differed by 47 microseconds, which corresponds to an error of 1 degree at 60 Hz and is far larger than the acceptable error set by standards [28]. There is some demand from industry groups and organizations to introduce conformity assessment, where an independent third party checks adherence to standards, although this movement is only just beginning. For example, the IEEE Conformity Assessment Program just recently established a PMU conformity assessment program on June 13, 2013 [29]. So far, conformity assessment initiatives have had little to no government support. While government involvement in standards coordination has been effective in areas under NIST's jurisdiction, standards are a limited tool when it comes to implementing some policies, such as with the cybersecurity concerns discussed in Section 5.

6.2 Use of Standards in Regulation

One possible solution to the limitations of voluntary standards is to mandate adherence to privately-developed standards in regulations. The North American Electric Reliability Corporation (NERC) is largely responsible for maintaining the reliability of the North American power system, and can enforce compliance with standards, as well as recommend voluntary standards. In December 2010, NERC released a report outlining the challenges facing smart grid integration with current bulk power systems, with an emphasis on stability and security of the grid [30]. However, in the report, NERC developed a work plan which focused on assessment and coordination of smart grid research efforts, and did not focus on specific standards that should be enforced to assist smart grid development. As the SGIP successfully identifies and develops standards through consensus processes with large groups of stakeholders, NERC may revise and update its enforceable set of Reliability Standards. One example of an area where increased regulation is needed is with CIM standards, as discussed in Section 6.1. At this point, many private and public entities have agreed that the IEC CIM should be implemented, but without more regulatory action, many more traditional utilities are unlikely to devote serious resources to this problem because they are reluctant to restructure their IT systems.

One downside to creating legislative regulations (through Congress) or enforceable standards (through NERC or FERC) is that smart grid technology is advancing rapidly, and regulations often take months, if not years, to develop and enforce. If regulations are developed that require outdated technologies, the US runs the risk of stagnating technological growth. Policies that have the force of law must be carefully structured to allow for, or even require, industry adaptation to new technologies. One example is a (currently voluntary) standard developed by the Smart Grid Interoperability Panel that requires that smart meter firmware be able to be updated remotely, without needing a technician to physically visit the meter every time it needs to be updated [31]. Issues like this would need to be taken into consideration for all mandatory smart grid regulation.

6.3 Infrastructure Funding

Government can also encourage improvements such as effective data management by funding new infrastructure. Both physical and "cyber" infrastructure are expensive to install and generally have slow or non-obvious financial returns. The goal of the smart grid funding in the American Reinvestment and Recovery Act was to "accelerate the modernization of the nation's electric transmission and distribution systems and promote investments in smart grid technologies, tools, and techniques" [32]. However, as ARRA funding runs out, the power industry is seeing a slowdown in smart grid development. After the 15.5 million ARRA-funded smart meters have been installed, the majority of homes and businesses in the US will still have little to no interaction with smart grid technologies. The US power industry runs the risk of losing momentum with smart grid technology rollout, which means that data analysis software development could seem less important and become outdated.

Policy options in this arena include straightforward grants (such as were included in the stimulus package), rebates or tax incentives for companies installing smart grid technologies, or research funding through the DOE's mandate to encourage smart grid research. Of course, in today's fiscal climate, this policy alternative is the least politically realistic. However, the large role that the grid plays in the economic well-being of the US, as well as the need to have a secure grid for national defense, means that the grid is one of the easier infrastructure investments to justify. It is even possible that some funding, especially for the area of cybersecurity, could come from defense funds.

It is easier to fund physical hardware improvements to the grid than to fund improvements to new data architectures, as the costs of changing data management strategies include time lost while training employees, installing software, and troubleshooting. Regardless, both types of infrastructure are equally important for collecting, analyzing, and responding to smart grid data. Financial incentives can also make cybersecurity initiatives more attractive for private companies, who are often reluctant to do more than the bare minimum to protect against digital threats.

7 Policy Recommendations

The policy recommendations of this paper fall into three categories: how to make data management more efficient, how to manage consumer privacy, and how to manage the security of grid data.

When it comes to the efficiency of data management, the standard identification and development efforts of the SGIP and NIST have been quite effective so far, and policies should continue to support public-private partnership in the development of standards. However, further steps must be taken to enforce those standards. As the US moves forward, more enforcement and conformity assessment of standards should be introduced by government agencies if private industry fails to do so. Just because standards are developed through consensus does not mean that those standards will be upheld uniformly. As technologies become mature, regulations can be put in place that will not limit technological innovation. Other technologies, such as smart meters, can be designed to be modified and updated as software for data management matures. When it comes to issues of high technical complexity, regulators should look to the standards identified by NIST and the SGIP.

One of the most important standards which should be developed into future regulation is the Common Information Model (CIM) standard developed by the IEC. If a CIM is made mandatory, there will be a common syntax that developers of the grid can use. It would not be necessary for utilities to completely restructure their data collection and communication procedures, but it would be necessary that the utilities be able to translate their data into a form specified by the CIM. The ability to communicate among different actors and levels in the grid is essential.

The second policy area that requires work is consumer privacy. Very little has been done on a large scale to address concerns about the nature of data being collected. An ideal privacy policy would require that as much identifying information is stripped from data as possible. Additionally, there is the problem of data persistence: in the current political climate, many consumers do not want their personal data to be stored for indefinite periods

of time. Data lifetimes should be established, and data should be deleted after this time passes. The final privacy policy recommendation is that consumers should have as much access to and control over their own data as possible. For example, consumers need to be able to decide whether third-party developers, such as smartphone app developers, are allowed to access their data. Some good work is being done in this area by the Green Button Initiative, led by the executive branch, which seeks to standardize what data consumers and third parties can access [33]. However, these types of efforts require more support and widespread application.

On the cybersecurity front, this paper recommends that NIST and the Smart Grid Interoperability Panel continue work on cybersecurity standards. These standards should be incorporated into regulation. Since the health of the electric grid is essential to the prosperity and security of the US, the smart grid community should be actively coordinating with defense agencies who have the most technical expertise in cybersecurity. Moreover, this is not an issue where a standard or regulation can be put into place and then ignored: continual updates to standards should be expected as technological threats change. This places a burden on industry to maintain compliance with cybersecurity requirements, so this should be minimized as much as possible, but the risks of an attack on the grid are real and such an attack would have a devastating impact.

Overall, current efforts to update the grid and foster interoperability are proceeding well. An immense amount of technical and engineering expertise is being brought to bear on the challenges facing the grid. However, there is a role for government in coordinating interoperability requirements, ensuring consumer privacy, and maintaining the security of the grid. As the US moves forward, the amount of data collected on the grid will only increase, and a coordinated plan is necessary to make good use of this resource.

References

[1] "Electric Grid Vulnerability: Industry Responses Reveal Security Gaps." Staff of Congressmen Edward J. Markey and Henry A. Waxman, May 2013.

[2] J. Achenbach, "The 21st Century Grid." National Geographic, July 2010.

[3] M. Brain, "How Power Grids Work." Online, 2000. http://science.howstuffworks.com/environmental/energy/power.htm.

[4] P. F. Schewe, *The Grid: A Journey Through the Heart of Our Electrified World*. National Academies Press, 2007.

[5] E. J. Lerner, "What's Wrong With the Electric Grid?." The Industrial Physicist, American Institute of Physics, Online, 2003. http://www.aip.org/tip/INPHFA/vol-9/iss-5/p8.pdf.

[6] J. Fahey, "US Power Grid Costs Rise, But Service Slips." Associated Press, Online, 2013. http://bigstory.ap.org/article/us-power-grid-costs-rise-service-slips.

[7] M. Koerth-Baker, *Before the Lights Go Out*. John Wiley & Sons, Inc., 2012.

[8] "Smart Grid: A Beginner's Guide." National Institute of Standards and Technology, Online, May 2013. http://www.nist.gov/smartgrid/beginnersguide.cfm.

[9] "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0." Office of the National Coordinator for Smart Grid Interoperability, National Institute of Standards and Technology, February 2012. http://www.nist.gov/smartgrid/upload/NIST_Framework_Release_2-0_corr.pdf.

[10] Pepco, "Smart Meter FAQ." Online, 2013. http://www.pepco.com/energy/blueprint/smetersdc/faq.aspx.

[11] EnergyAction, "Peak Demand - What is it?." Online, 2013. http://energyaction.com.au/peak-demand-what-is-it.

[12] J. Piel, "Energy Management and Conservation Solutions: Automate the Grid." Cooper Power Systems, July 2011.

[13] A. Silverstein, "NASPI Update and Technology Roadmap." North American SyncroPhasor Initiative, NERC Operating Committee Meeting, December 2011.

[14] "The Smart Grid Utility Data Market." SBI Energy, 1 December 2010. http://www.sbireports.com/Smart-Grid-Utility-2496610/.

[15] G. Wang, "Real-time Prices in an Entropic Grid." Innovative Smart Grid Technologies Conference, DOI 10.1109/ISGT.2012.6175822, January 2012.

[16] "H.R. 6. Energy Independence and Security Act." U.S. House. 110th Congress. 1st Session. Washington, Government Printing Office, 2007. http://www.gpo.gov/fdsys/pkg/BILLS-110hr6enr/pdf/BILLS-110hr6enr.pdf.

[17] "Compliance and Enforcement." North American Electric Reliability Corporation Website, 2013. http://www.nerc.com/pa/comp/Pages/Default.aspx.

[18] "A Policy Framework for the 21st Century Grid: A Progress Report." Executive Office of the President, National Science and Technology Council, February 2013. http://www.whitehouse.gov/sites/default/files/microsites/ostp/2013_nstc_grid.pdf.

[19] "Data Analytics and Smart Grid: The Rising Tide for Power Utilities." Green Tech Grid, December 2012.

[20] "Data Access and Privacy Issues Related to Smart Grid Technologies." Department of Energy, October 2010. http://energy.gov/sites/prod/files/gcprod/documents/Broadband_Report_Data_Privacy_10_5.pdf.

[21] J. Minkel, "The 2003 Northeast Blackout: Five Years Later." Scientific American, August 2008.

[22] S. Varadan, "Achieving Smart Asset Management." IEEE Smart Grid Newsletter, July 2013. http://smartgrid.ieee.org/july-2013/906-achieving-smart-asset-management.

[23] "About Us." Smart Grid Interoperability Panel, 2013. http://sgip.org/about_us/.

[24] G. Arnold, "Letter from George Arnold (NIST) to Jon Wellinghoff (FERC)." US Department of Commerce, 6 October 2010.

[25] J. Fremont *et al.*, "Common Information Model (CIM) Enabling Smart Grid Interoperability." International Electrotechnical Commission White Paper, 2011.

[26] D. Petri, "OSI Model Concepts." PETRI IT Knowledgebase. http://www.petri.co.il/osi_concepts.htm.

[27] "Cybersecurity." Recovery Act Smart Grid Programs. http://www.smartgrid.gov/recovery_act/overview/standards_interoperability_and_cyber_security/cyber_security.

[28] S. Meliopoulos, "SynchroPhasor Measurement Accuracy Comparison." Technical Report for the North American SynchroPhasor Initiative, December 2007.

[29] "IEEE Conformity Assessment Program (ICAP) Establishes Synchrophasor Conformity Assessment Steering Committee." Marketwired Press Release, June 2013.

[30] "Reliability Considerations from the Integration of Smart Grid." North American Electric Reliability Corporation, December 2010. http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/SGTF_Report_Final.pdf.

[31] "Priority Action Plan 0: Meter Upgradability Standard." NIST Smart Grid Collaboration Wiki, NEMA SG-AMI 1-2009, March 2012.

[32] "Smart Grid Investment Grant Program." Recovery Act Smart Grid Programs. http://www.smartgrid.gov/recovery_act/overview/smart_grid_investment_grant_program.

[33] "Green Button: About." http://www.greenbuttondata.org/greenabout.html.