Chapter 16
Societal Implications of the Smart Grid: Challenges for Engineering

Joseph Herkert and Timothy Kostyk

Abstract The smart grid, which would combine advanced information and communication technologies with a new generation of electric power production, transmission, and distribution technologies, has been highly touted as a solution to modernizing the U.S. electric grid while simultaneously addressing other policy goals such as improving energy efficiency and expanding the use of renewable energy resources. As with any large scale socio-technical system, however, the smart grid raises a number of societal issues that are interwoven with its technical capabilities. This chapter discusses three such issues – privacy, security, and equity – and argues for addressing them concurrent with the development of the smart grid, as well as educational reforms that will better position engineers to recognize and address such issues.

Keywords Smart grid • Privacy • Security • Equity • Education

Introduction

The world's electricity systems face a number of challenges, including ageing infrastructure, continued growth in demand, the integration of increasing numbers of variable renewable energy sources and electric vehicles, the need to improve the security of supply and the need to lower carbon emissions (IEA 2011). In the United States and some other countries, the electrical power grid is deteriorating. In the U.S. the annual number of large power outages has been increasing since the late

J. Herkert (✉)
College of Letters and Sciences, Consortium for Science, Policy & Outcomes, Arizona State University, 250D Santa Catalina Hall, 7271 E. Sonoran Arroyo, Mesa, AZ 85212, USA
e-mail: joseph.herkert@asu.edu

T. Kostyk
College of Letters and Sciences, Bachelor of Arts in Interdisciplinary Studies (*BIS*) and Organizational Leadership (OGL) programs, Arizona State University, 411 North Central, Mail Code 1901 Phoenix, AZ 85004-0696, USA
e-mail: Timothy.Kostyk@asu.edu

© Springer International Publishing Switzerland 2015

S.H. Christensen et al. (eds.), *Engineering Identities, Epistemologies and Values*, Philosophy of Engineering and Technology 21,
DOI 10.1007/978-3-319-16172-3_16

1990s (Amin and Schewe 2007). For two consecutive days in July of 2012, India experienced blackouts that took down large portions of the country's power grid. The second outage was the largest in history, leaving more than 600 million people, nearly a tenth of the world's population, without electricity (Romero 2012). The numbers, duration, and impact of power failures have severe implications for an energy-intensive way of life, economic stability, and even national security.

One proposed engineering response is widely known as the "smart grid." The increasing occurrences of outages and instances of cyber intrusions between 2000 and 2008 were considered so threatening to U.S. economic viability and security that the federal government, as part of the American Recovery and Reinvestment Act of 2009, earmarked more than $3.3 billion in smart grid technology development grants and an additional $615 million for smart grid storage, monitoring, and technology viability as an initial investment in building the smart grid. In addition, utilities have begun to mount demonstration projects and government and professional societies have begun the development of smart grid standards. Worldwide, investment in smart grid technologies totaled nearly $14 billion in 2012, topped by the U.S. at $4.3 billion and China at $3.2 billion. Major investments also occurred in the rest of Asia and the European Union (Rogers 2013).

The smart grid will be comprised of three fundamental structural elements: replacement of aging core physical infrastructure items including transmission lines and switching equipment with more efficient and reliable newer technologies; two-way distributed and loosely coupled supply and demand connectivity to the grid, which allows consumers to supply electricity through technologies such as photovoltaic cells and wind power; and, most importantly, highly optimized two-way information and communication technology (ICT) systems architectures and networks that control the grid through process- and rule-based programs to match power demand with supply in order to improve efficient use of energy resources. The conceptual model at the core of the smart grid is based upon a framework developed by the U.S. National Institute of Standards and Technology (NIST) that is composed of seven distinct domains – Markets, Operations, Service Provider, Bulk Generation, Transmission, Distribution and the Customer – and the resulting relationships among the domains (see Fig. 16.1).

One aspect of the NIST model is especially noteworthy; the domain model is based on a services based architecture (known as "actor-application") where each domain can literally exist anywhere. A home or business can possess generation capabilities transmitted to a distribution point within a building or plant, maintained by a control panel on a computer with excess power sold to a neighbor or across the country by markets controlled by internet based companies. For example, as noted in a recent *New York Times* article, "Google won federal approval in February to buy and sell electricity on American electricity markets." It also plans to offer "tools for measuring the electricity consumption of home appliances through partnerships with companies like General Electric" (Bhanoo 2010). In the future the intelligence to control these services is predicted to be "cloud" based internet applications much like the banking system of today (NIST 2012).

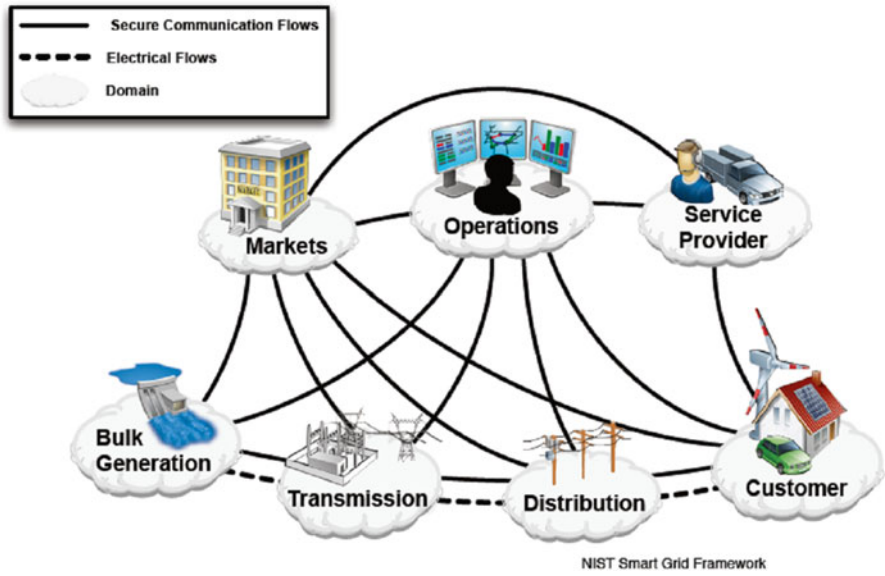

Fig. 16.1 NIST smart grid framework (NIST 2012, p. 42)

The European Union (EU) plan for Smart Grid development has taken the NIST model to the next level of complexity and flexibility. The EU model, developed by the Smart Grid Coordination Group of three standards organizations, Comité Européen de Normalisation (CEN), Comité Européen de Normalisation Électrotechnique (CENELEC), and European Telecommunications Standards Institute (ETSI), extends the NIST model by incorporating two additional actors: Distributed Energy Resources and Microgrid technologies architecture (see Fig. 16.2). Together these additional actors allow for a Smart Grid that is more modular in design with the ability to integrate power sources which can be isolated from the main grid into smaller grids. This extended NIST model allows more resilience and security by allowing the smaller grids the ability to disconnect from the large grid in the case of security breaches or disruptions or damage to other parts of the physical grid. A side benefit from a segmented grid built on Microgrid technologies is the ability to introduce privacy based data restrictions within individual Microgrids. (CEN-CENELEC-ETSI 2012).

Benefits of the Smart Grid

The fundamental differences between the existing grid and the smart grid are the ICT and distributed connectivity capabilities where the solid lines in Figs. 16.1 and 16.2 represent data networks which can exist via the internet or cloud and where the components can exist within the same building or across the country. It has been estimated that a smart grid could save U.S. utilities and their customers as much as

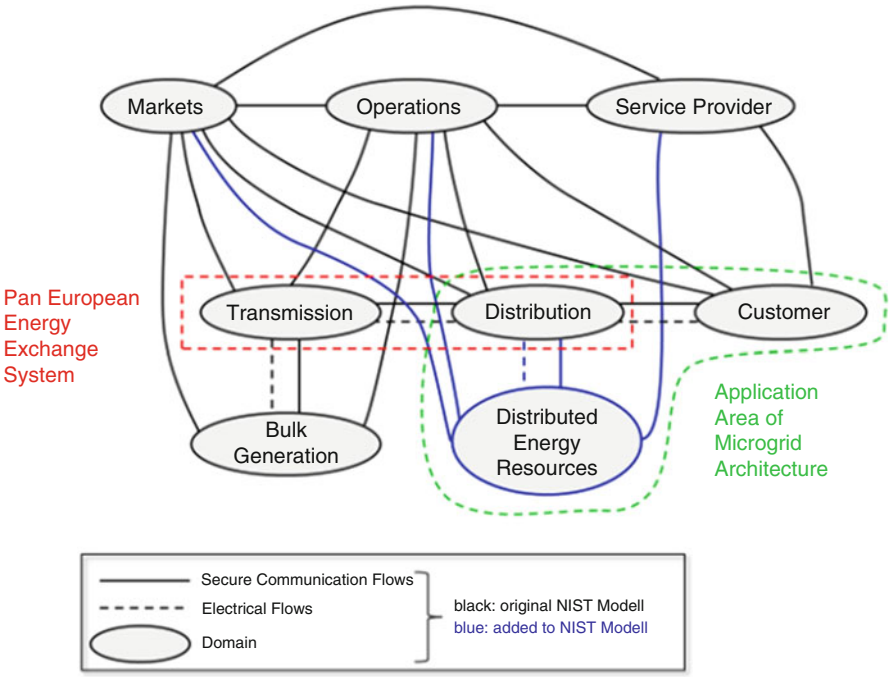

Fig. 16.2 EU extension of NIST framework (CEN-CENELEC_ETSI 2012, p. 21)

$20.4 billion annually by 2030 (Zeller 2010); however, the potential benefits of the smart grid extend well beyond the energy cost savings.

Amin (2004) has noted: "All economic and societal progress depends on a reliable and efficient energy infrastructure; for instance, banking and finance depend on the robustness of electric power, cable, and wireless telecommunications. Transportation systems including military and commercial aircraft and land and sea vessels depend on communication and energy networks. The linkages between electric power grid, telecommunications, and couplings of electric generation with oil, water, and gas pipelines are ever increasing and continue to be a lynchpin of energy supply networks." According to the International Energy Agency (IEA 2011) the Smart Grid has six key characteristics that will contribute to a stronger energy infrastructure and thus provide enhanced economic benefits (See Table 16.1).

Many of these characteristics rely upon the smart grid's ICT backbone. For example, an important aspect of Characteristic 2 (see Table 16.1) is the ability, utilizing smart grid ICT technologies, to spread the risk of price shocks in conventional fuels for power generation to other forms of power generation using substitute or renewable sources. Prior to the development of smart grid technologies it was difficult or even impossible to integrate these power sources on a large scale into the traditional transmission system. Additionally, smart grid technologies, specifically emerging Microgrid technologies (Farhangi 2010), provide the consumer the ability to interface with multiple power sources, thereby allowing individuals and businesses the opportunity to seamlessly replace or augment more expensive power

Table 16.1 Smart grid characteristics (IEA 2011)

Characteristic	Description
1. Enables informed participation by customers	Consumers help balance supply and demand, and ensure reliability by modifying the way they use and purchase electricity. These modifications come as a result of consumers having choices that motivate different purchasing patterns and behavior. These choices involve new technologies, new information about their electricity use, and new forms of electricity pricing and incentives
2. Accommodates all generation and storage options	A smart grid accommodates not only large, centralized power plants, but also the growing array of customer-sited distributed energy resources. Integration of these resources – including renewables, small-scale combined heat and power, and energy storage – will increase rapidly all along the value chain, from suppliers to marketers to customers
3. Enables new products, services and markets	Correctly designed and operated markets efficiently create an opportunity for consumers to choose among competing services. Some of the independent grid variables that must be explicitly managed are energy, capacity, location, time, rate of change and quality. Markets can play a major role in the management of these variables. Regulators, owners/operators and consumers need the flexibility to modify the rules of business to suit operating and market conditions
4. Provides the power quality for the range of needs	Not all commercial enterprises, and certainly not all residential customers, need the same quality of power. A smart grid supplies varying grades (and prices) of power. The cost of premium power-quality features can be included in the electrical service contract. Advanced control methods monitor essential components, enabling rapid diagnosis and solutions to events that impact power quality, such as lightning, switching surges, line faults and harmonic sources
5. Optimizes asset utilization and operating efficiency	A smart grid applies the latest technologies to optimize the use of its assets. For example, optimized capacity can be attainable with dynamic ratings, which allow assets to be used at greater loads by continuously sensing and rating their capacities. Maintenance efficiency can be optimized with condition-based maintenance, which signals the need for equipment maintenance at precisely the right time. System-control devices can be adjusted to reduce losses and eliminate congestion. Operating efficiency increases when selecting the least-cost energy-delivery system available through these types of system-control devices
6. Provides resiliency to disturbances, attacks and natural disasters	Resiliency refers to the ability of a system to react to unexpected events by isolating problematic elements while the rest of the system is restored to normal operation. These self-healing actions result in reduced interruption of service to consumers and help service providers better manage the delivery infrastructure

with cheaper power or even their own generated power, which if produced in excess of personal demand could be sold on the open market.

Characteristic 4 (see Table 16.2) refers primarily to centralized power and the pricing of electricity based upon the power quality needs of various customers. What the table fails to illuminate is that power quality can be augmented by consumers of power through devices or even by segmenting sections of their power

Table 16.2 Potential privacy consequences of the smart grid (EPIC, n.d.)

1. Identity theft
2. Determine personal behavior patterns
3. Determine specific appliances used
4. Perform real-time surveillance
5. Reveal activities through residual data
6. Targeted home invasions (latch key children, elderly, etc.)
7. Provide accidental invasions
8. Activity censorship
9. Decisions and actions based upon inaccurate data
10. Profiling
11. Unwanted publicity and embarrassment
12. Tracking behavior of renters/leasers
13. Behavior tracking (possible combination with personal behavior patterns)
14. Public aggregated searches revealing individual behavior

infrastructure or by merely purchasing power from multiple suppliers which guarantee levels of power quality through service level agreements (SLA) (Gustavsson and Ståhl 2010). This is a common ICT practice in many companies for all aspects of the technical infrastructures and the ICT infrastructure which supports them. This blending of responsibility and source of power based upon quality not only allows for competitive pricing among suppliers but also allows the consumer the means to control costs through conditioning their own power when protecting valuable pieces of equipment which are vital economic assets of companies and individuals alike.

Characteristic 5 (see Table 16.2) points to the Smart Grid's ability to manage the grid in a holistic manner (Nampuraja 2011) using an ICT approach known as IT Service Management (ITSM). ITSM is a process-based practice that aligns the delivery of services with the needs of the customer. An important aspect of ITSM is its ability to manage assets of entire systems through a parallel and simultaneous system of Service Support (SS) and Service Delivery (SD). Both SS and SD delicately balance asset management and maintenance while insuring virtually uninterrupted service at agreed upon levels, once again based upon the SLA model. (See ITIL, n.d. for a more detailed discussion of ITSM.)

The traditional grid which we live with today will transform to an "end state" grid which ultimately may look different than currently planned models. As noted by the U.S. Department of Energy (DOE):

> The Smart Grid will consist of millions of pieces and parts – controls, computers, power lines, and new technologies and equipment. It will take some time for all the technologies to be perfected, equipment installed, and systems tested before it comes fully on line. And

> it won't happen all at once – the Smart Grid is evolving, piece by piece, over the next decade or so. Once mature, the Smart Grid will likely bring the same kind of transformation that the Internet has already brought to the way we live, work, play, and learn (DOE n.d.).

While the innovative features of the smart grid hold great potential for improved energy efficiency through better management of consumer demand and improved stewardship of energy resources including greater utilization of renewable generation, they also pose a number of social and ethical challenges including: protecting the privacy of consumer usage information; securing the grid from attacks by foreign nations, terrorists, and malevolent hackers; and ensuring social justice in determining the price of electric power service. As with many new technologies the engineers engaged in developing the smart grid often overlook such issues or only turn to considering them once the technical standards and specifications have been settled. Failure to address these issues in a timely manner, however, may result in delays in establishing the smart grid and undermine its potential. Engineers and others involved in developing the smart grid need to examine ways to address organizational, social, and ethical dimensions that distributed generation and more extensive efforts to influence consumer usage patterns will raise. The cost of doing so would amount to an insignificant fraction of the projected necessary investments.

Preparing engineers to recognize and address such issues presents a significant challenge for engineering education. While several models of curriculum change to incorporate smart grid concepts have been proposed (e.g., Reed and Stanchina 2010; Sluss 2011), most focus solely on the technical aspects of the smart grid to the neglect of privacy, security, equity, and other social and ethical issues.

Privacy

As is the case for many other modern ICT applications such as the Internet and geographical positioning system (GPS), ensuring consumer privacy will be a challenge for the smart grid. Up until now our personal energy usage had been recorded by simple consumption metrics such as kilowatt hours measured using a conventional meter attached to a home or business. In the initial transition to a smart grid, utilities have begun to install "smart meters" that can provide feedback to the utility and customers (as often as every 15 s) on such factors as time of use of electricity; 65 million residential smart meters are expected to be in service in the U.S. by 2020 (Zeller 2010). Since many appliances have a unique "load signature," smart meter data can be analyzed to determine the types of appliances and other equipment consumers are using (Bleicher 2010). In the future, as more demand side technologies are developed, the smart grid could have the capability to monitor and control the usage of every plugged-in electrical device, which would allow the electric utility to turn the device off during times of peak demand to balance load across the grid. For the privilege of acquiring data and controlling consumer electrical devices utility

companies may charge a reduced rate. Alternatively, rate structures that vary by time of day or fuel source (coal vs. wind, for example) may be instituted in order to influence consumer energy usage behaviors.

As we move from theory to design, the emerging smart grid will become a vast ICT network populated with a diverse set of data acquisition devices capable of tracking the source, ownership, performance, and behavioral characteristics of each connected component. The smart grid technologies with the potential to be privacy invasive include "smart" power meters, energy monitoring and control software programs, and monitoring chips built into devices that consume electricity.

In addition to control and monitoring functions, however, the smart grid will have the ability to collect, aggregate, and store individual consumer usage data such as the temporal pattern of electricity usage and the number, type, and usage of electrical appliances and electronic devices. Analysis of this data could reveal such information as home occupation patterns, the number of occupants, and the manufacturer and usage of individual devices – valuable to utility planners but additionally to marketing agencies, insurance companies (property, health, and life) and, potentially, criminals (for example, outsiders may be able to tell when a home is occupied, determine the type of security system, and learn other sensitive information). As Table 16.2 indicates, the list of potential privacy implications of the smart grid is extensive.

Collection and storage of data are only part of the issue. Ultimately, the privacy implications of the smart grid rest upon who *owns* consumer data (Cardenas and Safavi-Naini 2012). Much like the data acquired by supermarket bar-code scanners and loyalty cards, data on specific devices in homes and consumers' patterns of energy use will become a prized resource. Electric utilities or third-party vendors may sell personal data to other organizations to defray costs or simply to increase profits.

Data available through the smart grid will not necessarily be limited to electrical usage data. For example, as noted in an article in *Computerworld*: "GE is even building a smart refrigerator that will be able to read the bar codes of food containers. It'll be able to keep track of what's been bought, what recipes can be made from the food it contains and what should be on next week's grocery list (Cline 2009)."

The PowerMeter application developed by Google is an example of how third-party vendors may become involved in the management of smart grid data. An Internet-based application, PowerMeter received real-time information from utility smart meters and energy management devices and provided customers with access to their home electricity consumption on their personal iGoogle home page. According to McDaniel and McLaughlin (2009): "Although Google has yet to announce the final privacy policy for this service, early versions leave the door open to the company using this information for commercial purposes, such as marketing individual or aggregate usage statistics to third parties." Though Google discontinued the service in 2011, it is only one of many data-hungry organizations racing to develop smart grid monitoring equipment and data systems.

Of course, like supermarket loyalty cards, utility customers may be willing to give up some of their personal data if they think it is being used benignly and if they are getting something in return (such as reduced prices or rates). Up to now, how-

ever, utilities have not had to deal with consumer energy usage data on this scale; they may be unwilling to incur the added expense of protecting consumer data from illegitimate uses or reassuring consumers that this data is protected adequately. The implications have not escaped the privacy watchdogs or even high-ranking U.S. federal government officials. Indeed, former Commerce Secretary Gary Locke warned that privacy concerns might be the "Achilles' heel" of the smart grid. Achieving public acceptance of the smart grid may prove difficult if privacy concerns are not addressed in a proactive manner.

One reflection of consumer concern over the smart grid and privacy is that public controversies, utility commission investigations, and legal cases have already begun to emerge in several places including Nevada, Colorado, Maryland, Illinois and Texas in the United States (Mufson 2011; Cardenas and Safavi-Naini 2012) as well as in other countries including the Netherlands, Australia, and the United Kingdom (Global Smart Grid Federation 2012). Perhaps the best known smart grid case, which involved a class-action lawsuit, is Bakersfield, California where customers of Pacific Gas and Electric Company (PG&E) claimed that their utility bills rose significantly after installation of smart meters (Chediak 2009). In an Illinois court case with privacy implications, compulsory smart meters are being contested on the grounds of violation of 4th Amendment protections against privacy invasion and illegal search (Munkittrick 2012).

There are no federal laws on the books in the U. S. specifically regarding the smart grid (Munkittrick 2012) and existing privacy laws have limited application (McDaniel and McLaughlin 2009). There has, however, been no lack of federal government studies on the smart grid and privacy issues, including reports by the National Institute of Standards and Technology (NIST) (2010), the Department of Energy (DoE) (2010), and the Congressional Research Service (CRS) (Murrill et al. 2012). According to legal blogger David Munkittrick (2012), the reports recommended the following guidelines for smart grid development:

- Appoint personnel responsible for data security and privacy.
- Regularly audit privacy procedures.
- Establish procedures for law enforcement data requests.
- Provide notice to consumers in advance of collection and use of energy use data.
- Aggregate and anonymize data in a way that personal information or activities cannot be determined.
- Keep personal information only as long as necessary to accomplish the purpose for which it was collected.
- Allow individuals access to their personal energy data to correct inaccuracies.

NIST has also established a privacy working group under the framework of its Cyber Security Working Group. Per Cardenas and Safavi-Naini (2012): "The goal of the Privacy group is to identify and clearly describe privacy concerns with energy usage data and to propose ways to mitigate these concerns. In addition, the group strives to clarify privacy expectations, practices, and rights with regard to the Smart Grid."

Utility regulators in the U. S. have been sensitive to the smart grid privacy issue for more than a decade. In 2000, the National Association of Regulatory Utility Commissioners (NARUC) passed a "Resolution Urging the Adoption of General Privacy Principles For State Commission Use in Considering the Privacy Implications of the Use of Utility Customer Information" including provisions relating to the importance of privacy interests, customer determination of the degree of privacy extended to them, required informed consent by consumers for use of non-service or non-billing related data, and provision of data to third parties pursuant only to utility commission approval (NARUC 2000). More recently, NARUC (2011) passed a "Resolution on Smart Grid Principles" which includes sections on protections for vulnerable consumer groups, access to data by consumers and third parties (subject to informed consent of the consumers), and the importance of maintaining consumer privacy.

In 2011, The California Public Utility Commission (CPUC) became the first state commission to promulgate regulations on the privacy and security of consumer usage data that the Center for Democracy and Technology describes as "…a remarkable achievement that merits the attention of not only utility commissions in other states but also of stakeholders in other sectors, for it shows that a comprehensive privacy and data security framework can be crafted that supports both technology innovation and consumer protection" (Dempsey 2011).

The issue of privacy and the emerging Smart Grid is becoming noticed worldwide. In a recent directive the European Commission Data Protection Working Party alerted the public to the potentials of Smart Grid data acquisitions: "The Europe-wide rollout of 'smart metering systems' enables massive collection of personal information from European households, thus far unprecedented in the level of detail and comprehensive coverage: smart metering may enable tracking what members of a household do within the privacy of their own homes and thus building detailed profiles of all individuals based on their domestic activities" (European Commission Article 29 Data Protection Working Party 2013, p. 4).

A number of approaches to smart grid design aimed at protecting consumer privacy have also been proposed including anonymizing sensitive consumer data by distinguishing high-frequency metering data from low frequency data or by data aggregation; power routing to prevent individual appliance data from being detected at the meter; and optimizing sampling frequency to balance data needs and privacy concerns (Cardenas and Safavi-Naini 2012). A more comprehensive approach, involving organizational as well as technical innovation, that was adopted by San Diego Gas and Electric (SDG&E) in 2012, is to apply the "Privacy by Design (PbD)" principles developed by Ann Cavoukian, Information and Privacy Commissioner of Ontario, Canada:

> Privacy by Design (PbD) principles may be integrated right from the start as utilities begin their Smart Grid implementations, thus helping to make sure that customer information is protected. Embracing a positive-sum model whereby privacy, security and energy conservation may be achieved in unison is key to ensuring consumer confidence in electricity providers as Smart Grid projects are initiated. In addition, customer satisfaction with and trust

> of Smart Grid initiatives is an integral factor in the success of energy conservation and other goals of Smart Grid efforts. (Cavoukian and Winn 2012, p. 5).

PbD is based on seven Foundational Principles (Cavoukian and Winn 2012, p. 6):

1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality – Positive-Sum, not Zero-Sum
5. End-to-End Security – Full Lifecycle Protection
6. Visibility and Transparency – Keep it Open
7. Respect for User Privacy – Keep it User-Centric

These principles were adopted for the smart grid context in a collaboration between SDG&E and Ann Cavoukian's group (see Table 16.3).

In addition to providing a roadmap for utilities, PbD provides an excellent framework for educating engineers on the importance of privacy. As Meldal et al. (2008) have shown, privacy and related concerns can and should be incorporated in both general education and engineering curricula:

> With the ever-increasing embedding of interconnected computing platforms at the core of our lives and of society, the successful trust systems issues education of the population in general and of the engineering professionals in particular becomes a matter of critical societal concern.
>
> Educational institutions benefit from taking an holistic approach to teaching security- and trust-related topics. The very ubiquity of the challenge can be made a vehicle for education, allowing for a pervasive injection of the concepts (and underlying technological and political challenges) of the interplay of security, trust, privacy and technology throughout the core as well as the discipline-specific curriculum components. (Meldal et al. 2008, p. 8)

With so much awareness of the importance of privacy on the part of nations, federal agencies, regulators, and smart grid technology designers, one would think

Table 16.3 Smart grid privacy principles (Cavoukian and Winn 2012, p. 13)

1. Smart Grid systems should feature privacy principles in their overall project governance frame work and proactively embed privacy requirements into their designs, in order to prevent privacy-invasive events from occurring
2. Smart Grid systems must ensure that privacy is the default – the "no action required" mode of protecting one's privacy – its presence being assured
3. Smart Grid systems must make privacy a core functionality in the design and architecture of Smart Grid systems and practices – an essential design feature
4. Smart Grid systems must avoid any unnecessary trade-offs between privacy and legitimate objectives of Smart Grid projects
5. Smart Grid systems must embed privacy end-to-end, throughout the entire life cycle of any personal information collected
6. Smart Grid systems must be visible and transparent to consumers – engaging in accountable business practices – to ensure that new Smart Grid systems operate according to stated objectives
7. Smart Grid systems must be designed with respect for consumer privacy, as a core foundational requirement

that privacy concerns will be comprehensively addressed. As seen in other areas of emerging technology, however, legal and ethical responses often lag far behind such issues (Marchant et al. 2011). Ultimately, the problem won't be solved until consumers are convinced their privacy is being preserved. As noted by the Electronic Privacy Information Center (EPIC, n.d.): "The key to privacy protection is to have the user maintain control over the collection, use, reuse, and sharing of personal information including their use of electricity."

Security

Unsurprisingly, many security aspects of the smart grid look like those of the Internet. Although the Internet has not been designated as the primary source of ICT communications, the smart grid will more than likely mature into a system that will utilize the Internet as its backbone. To secure both the informational and power-carrying capacity of the smart grid two important features must be addressed: the physical security of power and ICT networks and equipment and the security of huge databases and computers that analyze the data. The smart grid of the future will integrate both these networks creating the ability for either one to cause disruption to the other. Examples abound where highly automated systems have been brought to a halt or damaged by failures or security breaches in their ICT backbones (e.g., failures in automated securities trading, cyber warfare damage to Iran's centrifuges for nuclear fuel enrichment, and malevolent hacking resulting in infiltration and shutdown of corporate and government Web sites).

As noted by Kosut et al. (2011), "Future smart grids will likely to be more tightly integrated with the cyber infrastructure for sensing, control, scheduling, dispatch, and billing. Already the current power grid relies on computer and communication networks to manage generation and facilitate communications between users and suppliers. While such integration is essential for a future 'smart' grid, it also makes the power grid more vulnerable to cyber-attacks by adversaries around the globe."

Security breaches in the smart grid could lead to brownouts or even blackouts, and could cause serious, long-term damage to power generation, transmission, and distribution equipment. With the integration of power and ICT networks, power delivery components and even everyday power devices (such as appliances) will become nodes on the Internet. In the future, cyber-attacks such as denial-of-service or virus attacks could cause outages in the smart grid and limit electricity supplies, including critical services such as infrastructure and public safety. These attacks could originate anywhere in the world and could start as easily as introducing false data regarding energy usage across many nodes. What do these concerns mean for the development of security mechanisms, policies, and practices to secure the smart grid? There will be pressure to introduce a wider range of surveillance technologies; such technologies are already at the forefront of many heated debates regarding the intrusion of local, state, and federal governments, and also corporations, into the

daily lives of individuals. Security and surveillance systems bring their own data needs, which promise to further erode personal freedoms, including privacy.

One of the most important security concerns of the smart grid is the viability of nation states to protect themselves from having their infrastructures crippled during time of war or as a lead up to hostilities. As the electrical grids of almost all modern societies have become the nerve center for economic, military and vital social systems the attack on these systems could lead to the collapse of entire societies.

As noted by Metke and Ekl (2010), "This vulnerability was considered such a potential risk that the U.S. government identified it as core element of legislation following the New York terrorist attacks of 2011. The need for critical infrastructure protection was first mandated by the Patriot Act of 2001 (Section 1016, the Critical Infrastructure Act of 2001). In 2003, Homeland Security Presidential Directive (HSPD) 7 established the national policy requiring federal departments and agencies to identify and prioritize United States Critical Infrastructure and Key Resources (CIKR) and to protect them from terrorist attacks."

In a 2009 article in the *Wall Street Journal* it was reported that "Cyberspies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former national-security officials. The spies came from China, Russia and other countries, these officials said, and were believed to be on a mission to navigate the U.S. electrical system and its controls. The intruders haven't sought to damage the power grid or other key infrastructure, but officials warned they could try during a crisis or war" (Gorman 2009). Essentially such attacks could bring a country to its knees even before a single shot was fired. For example, recently a cold war has existed between Iran and the U.S. where a manifestation of hostilities has come in the form of the Stuxnet virus, a sophisticated computer virus deployed during the waning days of the Bush administration in an effort to thwart uranium enrichment in the Iranian government's nuclear program. As Sanger (2012) notes, "It appears to be the first time the United States has repeatedly used cyberweapons to cripple another country's infrastructure, achieving, with computer code, what until then could be accomplished only by bombing a country or sending in agents to plant explosives." Sanger also points out that: "President Obama has repeatedly told his aides that there are risks to using – and particularly to overusing – the weapon. In fact, no country's infrastructure is more dependent on computer systems, and thus more vulnerable to attack, than that of the United States. It is only a matter of time, most experts believe, before it becomes the target of the same kind of weapon that the Americans have used, secretly, against Iran."

The vulnerability of key systems and controls that are in widespread use in the developing smart grid is already apparent. As a recent news article noted: "A widely used system for controlling electricity, heating and other systems inside buildings remains vulnerable to attacks over the Internet, despite warnings from U.S. officials.... Poor security in industrial control systems, including those that run manufacturing facilities and power plants, has become an intense focus for security researchers and hackers alike since 2010 when the Stuxnet virus sur-

faced." (Menn 2013). The worrisome issue here is that we have identified widespread vulnerabilities in smart grid technologies at the same time as governments and hacker groups have developed internet viruses specifically designed to exploit those vulnerabilities.

Since the smart grid is predominately an intricate web of ICT networks a fully developed smart grid could in fact be the possible entry point of a devastating cyber-attack. This kind of futuristic war could wreak havoc upon every aspect of a society since literally any and all electrical devices plugged into the smart grid could be comprised and corrupted.

If the security vulnerabilities discussed above can be identified and managed effectively, the smart grid promises to provide significant economic and social benefits. Indeed, balancing the potential economic benefits with privacy and security concerns will be a key challenge in the development of the smart grid. As NARAC (2011) notes in its "Resolution on Smart Grid Principles:"

> As a condition of approving smart grid investments, State commissions should hold utilities responsible for ensuring that smart grid technologies are deployed in a manner consistent with reasonable and effective cyber and physical security best practices. Smart grid systems should be designed to mitigate risks and enhance the resiliency of the power grid and preserve the accuracy, integrity, and privacy of data. State commissions should…recognize that cyber security requires coordination, adaptability and resiliency that goes beyond standards compliance…. Further, State commissions may want to assure that utilities have recovery plans in the event of a successful cyber or physical threat.

Engineering educators have begun to include security-related topics in smart grid courses and curricula (e.g., Schulz 2011; Shireen et al. 2013), though most treatments are limited to "security" as a technical concept; its social and ethical implications are far less recognized. Approaches advocated by Meldal et al. (2008) (discussed above) which locate topics such as security, privacy and trust in a broader socio-technical context are critically needed in engineering education.

Pricing and Equity

Though not as obvious as privacy and security issues, the smart grid also poses potential problems for equitable pricing of electric power service. The nature of these impacts will depend on whether consumer energy usage is left under utility control or consumers are allowed to make their own usage decisions under variable pricing schemes. The former case would limit consumer autonomy. Some utilities, for example, have expressed an interest in controlling customers' thermostats and other appliances (Levinson 2010). Variable pricing, on the other hand, would place an energy management burden on all residential consumers. Those with lower educational levels, limited Internet access or computer skills, medical or cognitive impairments, or those who simply lack time, resources, or motivation to manage their usage patterns could be at a disadvantage. Both cases will require innovative ratemaking and oversight by public utility commissions and greater coordination and standardization within and among retail service areas.

Though smart meter experiments are just in the beginning stages, there have already been regulatory and legal controversies over such issues as required prepaid service plans for low-income consumers (Ailworth 2009) and alleged price gouging under mandatory switches to smart meters. As noted earlier, a highly publicized controversy over higher bills occurred in Bakersfield, California (Chediak 2009), but protests and law suits have occurred elsewhere including Texas. In both the California and Texas cases, independent studies confirmed the accuracy of the smart meters, but utilities have been cautioned to approach the installation of smart meters with a greater concern for consumer needs and attitudes (Zeller 2010). The UK, for example, has developed a draft consumer engagement strategy (Global Smart Grid Federation 2012).

Issues regarding pricing and equity are far from black and white concerns over the cost of energy. The ability of a smart grid to closely monitor and manage the flow of electrical energy has a dramatic impact on almost every other socio- technical system which together have much influence over everyday lives. In a recent whitepaper, a trusted advisor to the Indian government describe the interrelationship of the Smart Grid to other technological systems:

> A smart grid could also interface with other utilities (gas, water, etc.). New services such as home monitoring, healthcare monitoring, etc. could be unleashed, which could provide new revenue streams to utilities as well as enhance consumer convenience. A power utility with its own network could become an Internet Service Provider, either directly or through a partnership or subsidiary. However, such changes are not only resisted (because of the creation of winners and losers) but also because there is vast uncertainty in how these will evolve. (Tongia 2009, p. 7)

Most of the discussion of equity and the smart grid has focused on the issue of dynamic pricing, i.e., variable electric rates that track the actual costs of providing services (in time-of use blocks or as frequently as "real-time'), with many economists and engineers favoring dynamic pricing on the grounds of economic efficiency. As noted by Faraqui (2010), "The pragmatic school of thought argues that rates should reflect time-variation in costs if the societal benefits from so doing exceed the societal costs. Typically, the societal benefits are associated with avoided capacity and energy costs and the societal costs are associated with implementing [smart metering]." According to the IEA (Heffner 2011), the arguments in favor of dynamic pricing include:

- *Traditional flat rates are not economically efficient and hide cross-subsidies*
- *Contrary to conventional wisdom, low-income customers can and will respond to dynamic price signals*

Faraqui (2010) is particularly adamant on the inadequacy of flat rates: "The opponents of dynamic pricing use the unfairness argument to present their case. But the presumption of unfairness in dynamic pricing rests on an assumption of fairness in today's tariffs. A flat rate that charges the same price around the clock essentially creates a cross-subsidy between consumers that have flatter-than-average load profiles and those that have peakier-than-average load profiles. This cross-subsidy is invisible to most consumers but over a period of time, it can run into the billions of dollars."

For their own part, the critics of dynamic pricing argue that it would not benefit the majority of users (Makovich 2011) and indeed could disadvantage small users and help lead to utility control of consumer loads (Levinson 2010). Because of such concerns the movement toward dynamic pricing has slowed in many jurisdictions and it remains unclear as to what extent and how fast it will be implemented.

As Felder (2011) notes, however, there are other factors in the implementation of the smart grid that raise equity concerns, most notably the compulsory installation of smart meters (and subsequent rate increase). Felder also questions the equity of the standard cost-benefit technique applied by supporters of the smart grid: "It would be a mistake to accept implicitly the assumption that a social cost-benefit analysis is the only equity framework and therefore to assume that if smart grid passes such a test, it should be adopted for both efficiency and equity reasons. Proponents of smart grid may, in effect, be making such an assumption by offering a social cost-benefit analysis as the only criterion for evaluation" (p. 95). Other equity issues highlighted by Felder include the distribution of risk and benefits between the utility and its customers (especially in light of the asymmetry of information) and the distribution of benefits between low-income and higher-income customers.

Ultimately, Felder argues, laws and regulations are needed to ensure equity is appropriately considered in rate-making proceedings:

> Although considerations of efficiency are important, they are not dispositive. Regulatory rulemaking commonly appeals to other values such as providing consumers information so they are better informed about decisions that affect them and they are better able to respond. Ratemaking policy also considers environmental issues, monetary and other support for low-income households, and assigning costs to those that cause them. Each of these considerations suggest individually and collectively that larger customers who consume more electricity than smaller customers should pay more for smart grid, that additional costs imposed on low-income consumers should be offset, at least partially, and that the elements of smart grid that directly and materially improve their lives should be prioritized over those elements that do not. (p. 98)

When applied to engineering education, Felder's argument is similar to recent calls for a focus on social justice in engineering education (Lucena 2013). As Leydens notes (2013): "A more socially just engineering profession will necessitate multiple changes to its pipeline – engineering education. If social justice education is to extend across and within the content of the engineering curriculum, it will need to inform and reform multiple educational components: foundational, design and engineering science – as well as humanities and social science – curricula."

Conclusion

Achieving the smart grid potential while tending to privacy, security, and equity concerns should begin with the realization that the smart grid is a complex sociotechnical system that requires solutions that go beyond the engineering of the grid. Solutions

must include thoughtful deliberation by federal and state regulatory agencies, flexible utility responses in addressing consumer concerns and, most importantly, an engineering culture that recognizes and addresses the societal implications of the smart grid upstream in the R&D process and as standards are being developed.

For example, while the National Institute of Standards (NIST) highlighted privacy concerns in a recent report (NIST 2010), the U.S. federal government has yet to enact any smart grid privacy legislation or regulations. By contrast, the California Public Utilities Commission's (CPUC) 2011 decision on protecting privacy and security of consumer data is a landmark ruling that should provide a strong template for other state commissions (CPUC 2011).

One solution for addressing customer concerns regarding the smart grid is to provide opt-out options, such as Pacific Gas and Electric's proposal to permit customers worried about the environment, health, and safety effects of smart meter wireless radio signals to request that the signals be shut off (albeit with a charge for conventional meter reading) (Barringer 2011). More generally, Felder (2010) argues that consumer choice is "the prime benefit that smart grid technologies can provide" (p. 98).

As in the case of the human genome project and nanotechnology, where the U.S. federal funding agencies earmarked a percentage of research funds to examine such issues (Mills and Fleddermann 2005), there is an urgent need to examine the societal implications of the smart grid concurrent with its development. Failure to do so will further threaten civil liberties and social justice in the information age and is likely to pose substantial barriers to public acceptance of the smart grid.

Educating engineers who are prepared to meet the challenges posed by the societal implications of emerging technologies such as the smart grid should be a keystone of efforts to reform engineering curricula for the twenty-first century. Incremental changes such as the linkage of privacy, security and trust advocated by Meldal et al. (2012) are necessary but not sufficient. Ultimately, to prepare engineers for developing a "smart and just grid" (Welsch et al. 2013) will require a revolutionary change in engineering education that places social justice concerns at its core.

Acknowledgments This chapter draws in part on an earlier article (Kostyk and Herkert 2012).

References

Ailworth, E. (2009). Plan for prepaid electricity rejected. *Boston.com*. Retrieved from http://www.boston.com/business/articles/2009/07/23/mass_rejects_utilitys_prepayment_plan_for_low_income_customers/

Amin, M. (2004). Balancing market priorities with security issues. *IEEE Power and Energy Magazine, 2*(4), 30–38.

Amin, M., & Schewe, P. F. (2007). Preventing blackouts. *Scientific American Magazine, 296*(5), 60–67.

Barringer, F. (2011). Pacific gas offers solution to turn off smart meters. *New York Times.* Retrieved from http://www.nytimes.com/2011/03/25/business/energy-environment/25meter.html

Bhanoo, S. N. (2010). Google's energy foray: What's up? *New York Times, Green Blog*. Retrieved from http://green.blogs.nytimes.com/2010/05/05/googles-energy-foray-whats-up/

Bleicher, A. (2010). Privacy on the smart grid. *IEEE Spectrum, online*. Retrieved from http://spectrum.ieee.org/energy/the-smarter-grid/privacy-on-the-smart-grid

Cardenas, A. A., & Safavi-Naini, R. (2012). Security and privacy in the smart grid. In S. K. Das, K. Kant, & N. Zhang (Eds.), *Handbook on securing cyber-physical critical infrastructure* (pp. 637–654). Elsevier/Morgan Kaufman: Burlington, Massachusetts.

Cavoukian, A., & Winn, C. (2012). *Applying privacy by design best practices to SDG&E's smart pricing program*. Information & Privacy Commission, Ontario. Retrieved from http://www.ipc.on.ca/images/Resources/pbd-sdge.pdf

CEN-CENELEC-ETSI Smart Grid Coordination Group. (2012). *CEN-CENELEC-ETSI smart grid coordination group smart grid reference architecture.* Retrieved from http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/xpert_group1_reference_architecture.pdf

Chediak, M. (2009). PG&E faces revolt over smart grid. *BusinessWeek: Technology*. Retrieved from http://www.businessweek.com/technology/content/dec2009/tc20091230_147434.htm

Cline, J. (2009). Will the smart grid protect consumer privacy? Computerworld. Retrieved from http://www.computerworld.com/s/article/9141002/Will_the_smart_grid_protect_consumer_privacy_

CPUC. (2011). Decision adopting rules to protect the privacy and security of the electricity usage data of the customers of Pacific gas and electric company, Southern California Edison Company, and San Diego gas & electric. Decision 11-07-056. California Public Utilities Commission. Retrieved from http://docs.cpuc.ca.gov/PublishedDocs/WORD_PDF/FINAL_DECISION/140369.PDF

Dempsey, J. (2011). California adopts smart grid privacy rule. Center for Democracy & Technology. Retrieved from https://cdt.org/blog/california-adopts-smart-grid-privacy-rule/

DOE. (n.d.). *Building and testing the smart grid.* SmartGrid.Gov, U.S. Department of Energy. Retrieved from http://www.smartgrid.gov/the_smart_grid#smart_grid

DOE. (2010). *Data access and privacy issues related to smart grid technologies.* Department of Energy. Retrieved from http://energy.gov/sites/prod/files/gcprod/documents/Broadband_Report_Data_Privacy_10_5.pdf

EPIC. (n.d.). The smart grid and privacy. EPIC – Electronic Privacy Information Center. Retrieved from http://epic.org/privacy/smartgrid/smartgrid.html

European Commission Article 29 Data Protection Working Party. (2013). *Opinion 04/2013 of the data protection impact assessment template for smart grid and smart metering systems ('DPIA Template'), Prepared by expert group 2 of the commission's smart grid task force.* Retrieved from http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp205_en.pdf

Farhangi, H. (2010). The path of the smart grid. *IEEE Power and Energy Magazine, 8*(1), 18–28.

Faruqui, A. (2010). The ethics of dynamic pricing. *Electricity Journal, 23*(6), 13–27.

Felder, F. A. (2011). The equity implications of smart grid: Questioning the size and distribution of smart grid costs and benefits. In F. P. Sioshansi (Ed.), *Smart grid: Integrating renewable, distributed & efficient energy* (pp. 85–100). Waltham: Academic.

Heffner, G. (2011). Smart grid – smart customer policy needs. In: *Workshop report for the IEA energy efficiency working party,* April, Paris.

Global Smart Grid Federation. (2012). Global smart grid federation report. Retrieved from http://www.globalsmartgridfederation.org/documents/May31GSGF_report_digital_single.pdf

Gorman, S. (2009). Electricity grid in US penetrated by spies. *Wall Street Journal*. Retrieved from http://online.wsj.com/article/SB123914805204099085.html

Gustavsson, R., & Ståhl, B. (2010). The empowered user – the critical interface to critical infrastructures. In: *5th international conference on critical infrastructure (CRIS),* IEEE, 2010, pp. 1–3

IEA. (2011). Technology roadmap: Smart grids. International Energy Agency. Retrieved from http://www.iea.org/publications/freepublications/publication/name,3972,en.html

ITIL. (n.d.). ITIL official website. Retrieved from http://www.itil-officialsite.com/

Kostyk, T., & Herkert, J. (2012). Societal implications of the emerging smart grid. *Communications of the ACM, 55*(11), 34–36.

Kosut, O., Jia, L., Thomas, R. J., & Tong, L. (2011). Malicious data attacks on the smart grid. *IEEE Transactions on Smart Grid, 2*(4), 645–658.

Levinson, M. (2010). Is the smart grid really a smart idea? *Issues in Science and Technology, 27*(1), 39.

Leydens, J. A. (2013). Integrating social justice into engineering education from the margins: Guidelines for addressing sources of faculty resistance to social justice education. In J. Lucena (Ed.), *Engineering education for social justice* (pp. 179–200). Netherlands: Springer.

Lucena, J. (Ed.). (2013). *Engineering education for social justice*. Netherlands: Springer.

Makovich, L. J. (2011). The smart grid: Separating perception from reality. *Issues in Science and Technology, 27*(3), 61–70.

Marchant, G. E., Allenby, B. R., & Herkert, J. R. (Eds.). (2011). *The growing gap between emerging technologies and legal-ethical oversight: The pacing problem*. Dordrecht, Germany: Springer.

McDaniel, P., & McLaughlin, S. (2009). Security and privacy challenges in the smart grid. *IEEE Security & Privacy, 7*(3), 75–77.

Meldal, S., Gates, K., Smith, R., Su, X. (2008). Security, safety and privacy – pervasive themes for engineering education. In Geza Varady (ed.) *ICEE 2008*, iNEER.

Menn, J. (2013). Researchers warn of cyber flaws in Honeywell control systems. Retrieved from http://www.reuters.com/article/2013/02/05/cybersecurity-controls-idUSL1N0B5LG320130205

Metke, A. R., & Ekl, R. L. (2010). Security technology for smart grid networks. *IEEE Transactions on Smart Grid, 1*(1), 99–107.

Mills, K., & Fleddermann, C. (2005). Getting the best from nanotechnology: Approaching social and ethical implications openly and proactively. *IEEE Technology and Society Magazine, 24*(4), 18–26.

Mufson, S. (2011). Growing field of "Smart Grid" technology faces opposition over pricing, Privacy. *Washington Post*. Retrieved from http://articles.washingtonpost.com/2011-11-11/business/35282623_1_smart-grid-smart-meters-renewable-energy-sources

Munkittrick, D. (2012). Smart grid technology implicates new privacy concerns. Privacy Law Blog. Retrieved from http://privacylaw.proskauer.com/2012/03/articles/data-privacy-laws/smart-grid-technology-implicates-new-privacy-concerns/

Murrill, B. J., Liu, E. C., & Thompson, R. M., II. (2012). Smart meter data: Privacy and cybersecurity. Washington, DC: Congressional Research Service.

Nampuraja, E. (2011). A unified management system for smart grid. In *Proceedings of the IEEE ISGT 2011 India,* pp. 328–333.

NARUC. (2000). *Resolution urging the adoption of general privacy principles for state commission use in considering the privacy implications of the use of utility customer information.* Retrieved from http://www.naruc.org/Resolutions/privacy_principles.pdf

NARUC. (2011). Resolution on smart grid principles. Retrieved from http://www.naruc.org/Resolutions/Resolution on Smart Grid Principles.pdf

NIST. (2010). *Guidelines for smart grid cyber security: Vol. 2, privacy and the smart grid.* U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology. NISTIR 7628.

NIST. (2012). *NIST framework and roadmap for smart grid interoperability standards, release 2.0*. U.S. Department of Commerce, National Institute of Standards and Technology. NIST Special Publication 1108R2.

Reed, G. F., & Stanchina, W. E. (2010). Smart grid education models for modern electric power system engineering curriculum. *IEEE power and energy society general meeting, IEEE* (pp. 1–5). IEEE: Piscataway, New Jersey.

Rogers, R. (2013). *Smart grid and energy storage installations rising*. Vital signs, Worldwatch Institute. Retrieved from http://vitalsigns.worldwatch.org/vs-trend/smart-grid-and-energy-storage-installations-rising

Romero, J. J. (2012). Blackouts illuminate India's power problems. *IEEE Spectrum, online*. Retrieved from http://spectrum.ieee.org/energy/the-smarter-grid/blackouts-illuminate-indias-power-problems

Sanger, D. E. (2012). Obama order sped up wave of cyberattacks against Iran. *New York Times*. Retrieved from http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

Schulz, N. N. (2011). Integrating smart grid technologies into an electrical and computer engineering curriculum. In*: Innovative smart grid technologies Asia (ISGT), 2011 IEEE PES* (pp. 1–4). IEEE: Piscataway, New Jersey.

Shireen, W., Kotti, R., & Villanueva, J. A. (2013). *ASEE 2013 Annual Conference*. Retrieved from http://www.asee.org/public/conferences/20/papers/7132/view

Sluss, J. J. (2011). Engineering education activities in electric energy systems. *Computer, 44*(4), 97–98.

Tongia, R. (2009). Smart grids white paper. Center for Study of Science, Technology and Policy. Bangalore. Retrieved from http://www.cstep.in/docs/Smart_Grid_Whitepaper_CSTEP.pdf

Welsch, M., Bazilian, M., Howells, M., Divan, D., Elzinga, D., Strbac, G., Fones, L., Keane, A., Gielen, D., Balijepalli, M., Brew-Hammond, A., & Yumkella, K. (2013). Smart and just grids for sub-Saharan Africa: Exploring options. *Renewable and Sustainable Energy Reviews, 20*, 336–352.

Zeller, Jr., T. (2010). "Smart" electric meters draw complaints of inaccuracy. *New York Times*. Retrieved from http://www.nytimes.com/2010/11/13/business/13meter.html

Joseph Herkert B.S. in Electrical Engineering from Southern Methodist University. D.Sc. in Engineering & Policy from Washington University in St. Louis. Lincoln Associate Professor of Ethics and Technology, College of Letters & Sciences and the Consortium for Science, Policy & Outcomes, Arizona State University, USA. He is Co-Editor of *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: the Pacing Problem* (Springer, 2011), Editor of *Social, Ethical and Policy Implications of Engineering: Selected Readings* (Wiley/IEEE Press, 2000) and has published numerous articles on engineering ethics and societal implications of technology in engineering, law, social science, and applied ethics journals. He previously served as Editor of IEEE *Technology & Society* and an Associate Editor of *Engineering Studies*. He is a Distinguished Life Member of the Executive Board of the National Institute for Engineering Ethics, a former Chair of the Liberal Education/Engineering and Society Division of the American Society for Engineering Education, and a former President of the IEEE Society on Social Implications of Technology.

Timothy Kostyk B.S. in Engineering, University of Louisville, MBA, Bellarmine University. Doctoral student in Arizona State University's Human and Social Dimensions of Science and Technology Program, a researcher and teacher at Arizona State University, where he: teaches classes on the emerging Smart Grid, is a contributor to the Energy Ethics and Policy ongoing seminar, and a member of the Consortium for Science, Policy, and Outcomes. For the past 3 years this field of study has concentrated on the examination of the world wide effort to redesign, rebuild and remodel the existing electrical grid into what is known as the Smart Grid. The dimension of this study incorporates the human, social, and technological aspects of design, particularly the ethical impact of engineered designs including those related to issues concerning privacy, equity and security. For the past 3 years Tim has extensively studied the ongoing efforts of multiple international and national governmental and professional engineering organizations as they together formulate the vision and develop the plans and standards for the development of the Smart Grid.