Securing the Smart Grid

Questions and answers on consumer privacy and threats to the grid – both physical and cyber.

By Massoud Amin

Electricity needs are changing and growing fast. Tweeting, and the myriad devices and infrastructures needed to operate the underpinning communication network, data centers, and storage alone adds thousands of megawatt-hours (MWh) of demand across the globe that did not exist just five years ago. Factor in Internet TV, video streaming, online gaming, and the digitization of medical records, and the world's electricity supply will need to triple by 2050 to keep up. And this basic need for more electric supply will run head on into a host of obstacles.

Getting to adequate levels infrastructure is problematic, notably environmental, policy and financial concerns. To get there, we need to assure we do not increase social, economic, physical and political risks. That invokes questions regarding consumer privacy, cyber security, physical attack, international terrorism, and the role of government.

Naysayers worry that smart grid initiatives, coupled with increased levels of penetration of distributed and intermittent renewable generation resources, contain negative ramifications for some electrical distribution systems, putting stress on devices traditionally used to handle voltage variability. Some have voiced concerns even of potential health impacts from exposure to radio-frequency signals emitted from wireless smart meters.

In fashioning a viable policy on smart grid, no doubt we must address questions such as these:

1. Distributed Resources. How might distributed energy resources, such as solar panels or plug-in vehicles in garages, affect power system operations, markets, and regulations?

2. Business Models. What business models may develop, and how will they successfully serve both upstream electricity market actors and energy consumers?

3. The Utility Enterprise. What effects could these new business models have on incumbent utilities, and what opportunities may exist for other industry sectors to capitalize on these changes?

4. Political Compromise. How should we align an economically viable utility model with state and federal public policy goals?

5. Price Regulation. How do we price services in relation to the value of reliability, power quality, conservation and innovation?

6. Universal Service. Do we continue to provide universal access to electricity services at "just and reasonable" rates, including programs for extending affordable services to low-income customers?

7. Consumer Involvement. What is needed to create positive engagement with stakeholder communities – to incentivize services and choices that customers will value?

8. Technology and Innovation. What policies will facilitate innovation, implementation of new technologies, and delivery of new energy services?

9. Cyber/Physical Security. How should we address issues concerning critical infrastructure protection (CIP) and the security of cyber and physical infrastructure still persist, necessitating vigilance and proactive counter measures?

10. Visions for the Future. What are plausible visions of the future of the power sector, including changes for incumbent utilities, new electricity service providers, regulators, policymakers, and consumers?

The sky is not falling but we are not yet bullet proof.

Last month, in the March 2015 issue of *Public Utilities Fortnightly*, I laid out the case for tackling this challenge through a self-healing smart grid. And though the cost might appear daunting, the benefits might well prove just as remarkable.

On one hand, the cost of a smarter grid would depend on how much instrumentation you actually put in, such as the communications backbone and security. The total price tag ranges around $340 billion to $480 billion, which, over a 20-year period, would be something like $20 billion per year. But right off the bat, the benefits are $70 billion per year in reduced costs from outages, and in a year where there are lots of hurricanes, lots of ice storms, and other disturbances, that benefit goes even further. In addition, it would increase system efficiency by 4.5 percent – that's another $20.4 billion a year.

But this vision is also about job creation and economic benefits. With the actual investment, for every dollar, the return to the broader economy should run from $2.80 to $6.00. And this figure is very conservative. Indeed, in my view, our 21st century digital economy depends on us making these investments,

Massoud Amin is Chairman of the IEEE Smart Grid, an ASME fellow, and a member of two utility industry reliability groups – the Texas Reliability Entity (as board chairman) and the Midwest Reliability Organization (as a board member). At the University of Minnesota he serves as professor of electrical and computer engineering, and as director of the school's Technological Leadership Institute (TLI). Dr. Amin has researched and written on self-healing grid concepts and solutions for two decades. Links to his work are available on the TLE's website at http://massoud-amin.umn.edu/publications.html.

A Decision Template for Utilities

What you'll need to identify and manage the transition.

1. Track and Understand What Is Driving Industry Uncertainty
   - Future demand for electricity supplied by grid resources
   - Future price of natural gas
   - Environmental laws, policy
2. Flexibility and Adaptation
   - Energy efficiency (end-to-end)
   - Long-term operations
   - Near-zero emissions
   - Renewable resources and integration
   - Smart grid
   - Water resource management
3. Connectivity
   - The Tsunami of Data
   - Gaining actionable intelligence from data streams
4. Resiliency
   - Situational intelligence
   - Prevention
   - Recovery
   - Survivability
5. Focus and Vision
   - Organize perceptions about future alternatives
   - Remove biases in visioning
   - Focus debates about technology needs
   - Challenge the view that little will change
   - Enable development of alternative technology portfolios
   - Foster a probabilistic versus a deterministic view of the future

A useful template should address uncertainty about the location, size, and schedule of new power plants coming on line, as well as uncertainties about interregional power transfer patterns, which may change from season to season and year to year. It might also facilitate probabilistic transmission planning methods and pinpoint what additional tools may be needed. Lastly, it could help provide the market signals needed for investors to build new transmission projects. It would be helpful in deciding where they are placed and in placing an online monitoring systems. –***MA***

regardless of the prognosis for more extreme weather to come as our climate changes.

The economic argument is clear: the payback of smart grid technologies in the U.S. is likely to be three to six times greater than the money invested, and will grow with each sequence of grid improvement. For example the 2009 government stimulus plan funding and matching support from utilities and the private sector in the Smart Grid Investment Grant (SGIG) and Smart Grid Demonstration Project (SGDP) programs generated a significant impact on the U.S. economy. Consider the progress that we can document already from that program.

As of March 2012, the total invested value of $2.96 billion to support smart grid projects generated at least $6.8 billion in total economic output. Smart grid deployment positively impacted employment and labor income throughout the economy. Overall, about 47,000 full-time equivalent jobs were supported by investments. Among smart grid vendors – an ecosystem of manufacturers, information technology and technical services providers – about 12,000 direct jobs were supported, with the remaining jobs being in those companies' respective supply chains and induced by the money spent throughout the broader economy.

Investment in core smart-grid industries supports high-paying jobs. Industrial sectors that benefit directly include computer systems design, technical and scientific services and consulting, and electrical/wireless equipment and component manufacturing. Industrial sectors that experience indirect and induced benefits include real estate, wholesale trade, financial services, restaurants, and health care. Smart grid investments made under the American Recovery and Reinvestment Act (ARRA) and associated programs sponsored by the U.S. Department of Energy (DOE) have supported employment in personal service sectors such as health care, financial services, real estate, and food/restaurants, through indirect and induced impacts.

The Metcalf attack in April 2013 reveals several areas that must be and can be remedied.

In fact, the smart grid Gross Domestic Product (GDP) multiplier appears greater than many other forms of government investment. For every $1 million of direct spending, which includes both government ARRA funds and private sector matching, the GDP increased by $2.5 to $2.6 million, depending on the scenario being evaluated, which compares favorably against other potential government investments in general spending or other types of infrastructure.

In short, the most promising way to address the challenges and threats we face lies not in backing away from them, but in developing the kinds of dynamic and self-healing systems that already are known and proven.

As I noted last month, the architecture for the autonomous

microgrids and microgrid assemblies now being modeled are based on multi-agent architecture for operating cellular power networks. In this architecture, each autonomous microgrid, and the resulting cellular power network, is composed of numerous independent and intelligent decision-making agents. These intelligent agents gather and exchange information with each other in real-time or near real-time in order to provide coordinated protection and to optimize system performance.

We have tested microgrids that incorporate a dynamic systems perspective of threat and uncertainty to investigate the performance of the multi-agent architecture for autonomous microgrids and microgrid assemblies as part of cellular power networks. As opposed to the computer science perspective that focuses on securing information, the focus of this work is on analyzing the actions or dynamics of network components and their overall management.

The primary question that is asked and answered becomes something like this: "What is the expected performance of such systems including the effects of failure, repair, contention for resources, attacks, etc.?"

Defining Threats

Question. How serious a problem is physical attack for our electric infrastructure, which has redundancy built in? Is cyber security a more pressing concern?

Answer. In short, the sky is not falling but on the other hand, we are not yet bullet proof.

The National Academy of Engineering classified electrification as the number one engineering achievement of the 20th century. Today, the U.S. electric grid consists of a network of approximately 10,000 power plants, 170,000 miles of high-voltage (>230 kV) transmission lines, over six million miles of lower-voltage distribution lines, and more than 15,000 substations. The transmission system is an interstate grid whose primary purpose is to connect generating plants with electrical load centers like cities and with high demand commercial and industrial facilities. In turn, the local distribution system provides for service to residential, commercial, and small business customers.

The existing power-delivery system is vulnerable to natural disasters and intentional attack. Regarding the latter, a successful terrorist attempt to disrupt the power-delivery system could have adverse effects on national security, the economy, and the lives of every citizen. This category of threat is not new. We've worked for countermeasures since 9/11 and even earlier (*e.g.*, the saboteur in the Pacific Northwest, attacks in South Africa, Brazil, Colombia, Israel, former Yugoslavia, etc.)

Nevertheless, the attack in April 2013 on the Metcalf substation reveals several areas that must be and can be remedied. Without going into details, this damage is not much compared to what can be done without too much organization. Disclosing the information provided in the recent article and any such details can be exploited by criminals, and thus many are disappointed about how it has been disclosed.

As for physical security, the size and complexity of the North American electric power grid makes it impossible both financially and logistically to physically protect the entire end-to-end and interdependent infrastructure. As an increasing amount of electricity is generated from distributed renewable sources, the problem will be only be exacerbated.

As for cyber security, we can see that threats from cyberspace to our electrical grid are rapidly increasing and evolving. While there have been no publicly known major power disruptions due to cyber-attacks, public disclosures of vulnerabilities are making these systems more attractive as targets.

Question. Is there a large difference in the funding by government or industry for addressing physical security for the electric system, as opposed to cyber security? Has there been enough focus given to physical security?

Security cannot be added as an afterthought. We need to start from scratch, at the very beginning.

Answer. The importance and difficulty of protecting power systems against classes of threat have long been recognized.

In 1990, the Office of Technology Assessment (OTA) of the U.S. Congress issued a detailed report, Physical Vulnerability of the Electric System to Natural Disasters and Sabotage, concluding: "Terrorists could emulate acts of sabotage in several other countries and destroy critical [power system] components, incapacitating large segments of a transmission network for months. Some of these components are vulnerable to saboteurs with explosives or just high-powered rifles." The report also documented the potential cost of widespread outages, estimating them to be in the range of $1 to $5/kWh of disrupted service, depending on the length of outage, the types of customers affected, and a variety of other factors. In the New York City outage of 1977, for example, damage from looting and arson alone totaled about $155 million – roughly half of the total cost.

The reality of a coordinated attack has raised the issue of security to be considered along with power systems' reliability, which posits more random and independent failures. The system's vulnerability to natural disasters and physical attacks has long been recognized, but this vulnerability has significantly increased in recent years, in part because the system is operating closer to its capacity and in part because terrorist attacks are no longer hypothetical.

The situation has become even more complex because accounting for all critical assets includes thousands of transformer, line reactors, series capacitors, and transmission lines. Protection of

all the widely diverse and dispersed assets is impractical because there are so many involved.

Assessing Risk

Question. Are there any points that readers should know about an incident like the one at Metcalf Substation in April 2013?

Answer. By taking basic and proactive maintenance and security measures, including compliance with CIP rules ("Critical Infrastructure Protection), we can manage and reduce most categories of risk.

Nevertheless, we still face increased risk due to all types of hazards, from the aging infrastructure, lack of investment in the system, lack of policies that are conducive to modernization, and substantially changed risks due to terrorism and climate weirding. As a recent example, in the months since Hurricane Sandy struck the East Coast with unprecedented fury, much discussion has focused on questions about power restoration in the Northeast.

First, it needs to be understood that a massive, physical assault on the scale of Sandy is bound to overwhelm the power infrastructure, at least temporarily. No amount of money or technology can guarantee uninterrupted electric service under such circumstances.

Second, the power industry in the United States is just beginning to adapt to a wider spectrum of risk. It is noteworthy that both the number and frequency of annual, weather-caused, major outages have increased since the 1950s. Between the 1950s and 1980s, those outages increased from two to five each year. In the period 2008-2012, those outages increased to between 70 percent and 130 per year. In that five-year period, weather-related outages accounted for 66 percent of power disruptions, which affected up to 178 million customers (meters).

This adaptation process continues as we implement strategies, technologies and practices that will harden the grid and improve restoration performance after a physical disturbance. The investments so far in advanced metering infrastructure and the coming wave of investment in distribution automation are but the beginning of a multi-decade, multi-billion-dollar effort to achieve an end-to-end, intelligent, secure, resilient and self-healing system.

Third, cost-effective investments to harden the grid and support resilience will vary by region, by utility, by the legacy equipment involved and even by the function and location of equipment within a utility's service territory.

In Sandy's case, coastal areas were subject to storm surges and flooding, while inland, high winds and lashing rain produced the most damage.

Improved hardening and resilience for distribution systems in those different environments would take different forms. Underground substations along the coasts may have to be rebuilt on the surface, while it might be cost-effective to perform "selective undergrounding" for some overhead lines further inland.

The pursuit of an intelligent, self-healing grid will make the overall network a lot more reliable, especially if it has built-in security protocols. Additional, location-specific steps based on rational risk assessment also can be taken by utilities and customers.

Adding and utilizing existing intelligence – sensors, communications, monitors, optimal controls and computers – to our electric grid with security built-in, can substantially improve its efficiency and reliability through increased situational awareness, reduced outage propagation, and improved response to disturbances and disruptions. This "Smart Grid" can also enable transparent pricing of electricity that will allow consumers to manage their energy costs and facilitate distributed generation and redundancy, opening the door to wider use of variable renewable generation sources and supporting expanded use of electric vehicles.

Regulatory Impediments

One important constraint on regulatory oversight of security protection still appears somewhat problematic: the split jurisdiction over the grid. The bulk electric system falls under federal regulation but the distribution grid, metering, and other aspects of the grid remain regulated by individual states. As a result the oversight of cyber security is split along with other regulatory functions.

A stockpiling authority, be it private or public, could amass inventories of critical components.

With this problem in mind, I recommend a series of steps to facilitate hardening against threats and resiliency to deal with them once they occur:

- **Sensors & Self-Healing**. Take necessary actions to facilitate, encourage, or mandate that secure sensing, "defense in depth," fast reconfiguration, and self-healing be built into the infrastructure.
- **Privacy.** Mandate security for the Advanced Metering Infrastructure, to provide protection against personal profiling, guarantee data privacy for consumers, and to guard against real-time remote surveillance, identify theft, home invasions, activity censorship, and third-party decisions based on inaccurate data.
- **Wireless Vulnerability.** Avoid unnecessary and increased vulnerability that comes with wireless and public Internet connections.
- **Federal-State Coordination.** Bridge the jurisdictional gap between state and federal commissions on cyber security.
- **Disperse the Cost.** Require asset owners to practice due diligence in securing their infrastructure as a cost of doing business.

■ **Local & Regional Centers.** Develop coordinated, hierarchical threat coordination centers – at local, regional, and national levels – that assess precursors and counter cyber attacks.

■ **Security from the Start.** Speed up the development and enforcement of cyber security standards, compliance requirements and their adoption. Facilitate and encourage designs that build in security from the start, and include those designs in standards.

■ **Chip-Level Protections.** Increase investment in the grid and in R&D areas that assure the security of the cyber infrastructure (algorithms, protocols, chip-level and application-level security).

■ **Microgrid Islanding.** Develop methods, such as self-organizing microgrids, to facilitate grid segmentation that limits the effects of cyber and physical attacks.

Documenting best practices on the deployment and integration of new technologies would be especially welcome. So would an increase in federal research and development for emerging technologies to improve the reliability, efficiency and management of the grid that includes new types of generation and energy storage.

On the other hand, overlapping and inconsistent roles and authorities of federal agencies can hinder development of productive, public-private working relationships, thus a new model for these relationships is required for infrastructure security.

For instance, a stockpiling authority, be it private or governmental, could obtain long lead-time equipment based on the power industry's inventory of critical equipment, which must include the number and location of available spares and the level of interchangeability between sites and companies. Clearly, further standardization of equipment will reduce lead times and increase the interchangeability of critical equipment.

A perennial entry in power industry recommendations to the federal government is to provide alternatives for utilities that wish to avoid wireless telecom networks and the public Internet to decrease grid vulnerabilities by, for instance, enabling utilities to obtain private spectrum at a reasonable cost.

Improving the sharing of intelligence and threat information and analysis to develop proactive protection strategies might include the development of threat coordination centers at local, regional and national levels. For that reason, the IEEE Task Force report on priority issues in its most recent (October 2014) Quadrennial Energy Review reported to DOE made recommendations on what role the federal government might play in support of state and local efforts to aid power and integrated utilities in increasing reliability, resilience and security.

Perhaps all these measures (and many more you'll find in the IEEE Task Force report) could be facilitated by more transparent, participatory and collaborative discussion among federal and state agencies, transmission and distribution asset owners, regional transmission operators an independent system operators and their members to improve stakeholders' understanding of mutual interactions, impacts and benefits.

Consumer Privacy

Question. Should consumers be concerned about security and privacy issues with respect to smart grid?

Answer. Privacy of information and cyber security are critical issues at the national level. The Department of Energy, the Department of Homeland Security and utilities are all working to develop guidelines, technologies, best practices, and rules for compliance in this area.

We are continually working on new technologies and approaches to make sure that the grid's control systems are secure. It's a challenge today and it's going to be more of a challenge as we extend those controls deeper into the system and closer to the customer. Privacy is a concern for consumers. We all have decisions to make in terms of the privacy of our data. With smart grid moving into advanced metering and maybe into people's homes to control their appliances and smart grid devices, privacy is a very important issue. It is getting a lot of attention in terms of what people want to enable and who should have access to information associated with smart grid applications. We can put systems in place that maintain the privacy of that data, while still enabling access to provide many valuable applications to customers.

As smart grid evolves, consumers probably won't see sweeping changes, but their voices can serve as a guide.

Question. What will it take to address concerns that communications linked to energy services will invade the privacy of individual consumers?

Answer. The bottom line is that security cannot be added to a system as an afterthought. We need to start from scratch, at the very beginning of any project, and consider privacy and security in all design criteria. Strategic consideration of these issues will make a huge difference in the confidence and protection that the overall system provides. This is necessary whether the design effort is focusing on silicon chips, network components, end-user devices, the architecture, or the system as whole.

Customer concerns are of vital importance. When it comes right down to it, what would the power supply or power grid be without consumers? If there is any compromise of the privacy or security of the service, it will undermine everything. An incident would not only create a breach of confidentiality for the information that has been compromised, but it might also compromise the potential future markets the technology might have been able to create if it the service had been secure.

By taking basic and proactive maintenance and security measures, including compliance with CIP rules ("Critical Infrastructure Protection), we can manage and reduce most categories of risk.

In our work we have proposed and tested several different layers of technologies that monitor and support the privacy of customer information. Security technologies are employed for traffic analyzers, signal analyzers, and agents that monitor voltages, frequency, current (along with their rates of changes), and user behavior. Each component is secured independently and locally so the security precautions cannot be reverse engineered.

This is not a hierarchical system that can be destroyed or taken down. If one or two layers fail, the system does not fail. It's essentially a self-reconfiguring, self-healing architecture. If anybody attacks it or tries to compromise one part of it, the system reconfigures to not only protect itself but to localize and fend off such attacks.

Price, Service and Value

Question. Will smart grid take away consumer choice?

Answer. Smart grid will allow more choices for the consumer. That choice will remain available, whether or not consumers request it from utilities.

Question. Will consumers begin to see sweeping changes, such as significantly lower electricity prices, fewer and less frequent blackouts, and more efficient delivery of power to their homes and businesses? Or, will they simply see "business as usual" in the electrical industry?

Answer. The smart grid evolution will be far from "business as usual" over the next several years. The biggest near-term impact will be on the electrical grid itself, as utilities both large and small further the expansion and implementation of advanced smart grid technologies. Additional developments occurring in parallel with grid expansion, such as Demand Response programs, will have an effect on the average consumer, though these effects will probably be felt more in the mid-term rather than in the near-term.

As the smart grid evolves over the next three to five years, consumers will probably not see sweeping economic differences in their everyday lives. But during that time, their voice can serve as a guide for utilities and regulators in steering smart grid to greater success, and perhaps even accelerate the timetable during the process. By getting involved in two-way educational programs, actively participating in available pilot programs, and embracing smart grid as the long-term solution to our nation's energy and economic challenges, consumers can serve as the vital missing link in the "human smart grid." The window of opportunity is open to make tomorrow's history . . . today.

Question. What policies should the industry adopt to benefit consumers?

Answer. One policy that can be implemented at the state level is dynamic pricing. This will facilitate demand response programs, which give consumers information and tools to manage their own energy use. These approaches can save a consumer 15 percent per month on their electricity bill.

Question. Should the U.S. embark on a comprehensive grid overhaul?

Answer. I hope we do. If you look at a macro picture, whenever we make this type of a big advancement, such as the moon shot or the national highway system, and when we put the American will, know-how, and passion behind any big, hairy, audacious goal, we succeed.

To modernize the whole end-to-end system, the smart grid represents a remaking of the electric power system encompassing all aspects of generation, delivery, and consumption. Benefits will accrue to individuals, societies, and industry: better use of renewable sources, reduction in carbon emissions from fossil plants, improved efficiencies across the power system, broad-based integration of electric and plug-in hybrid vehicles, real-time feedback to consumers on their electricity consumption, improved grid reliability, and more.

The economic benefits of a modernized grid will accrue as investments are made.

But several challenges must first be addressed. Intermittent renewables and greater variability in load profiles will result in high uncertainty in both generation and consumption. Dynamic pricing and demand response will intricately couple economic factors and power flow. With communication technologies providing a system-wide integration infrastructure, the smart grid will represent a prototypical "system of systems." Multiple and often conflicting criteria will need to be coordinated: profits, grid reliability, environmental impacts, equipment constraints, and consumer preferences. Environmental and energy policy need to be supportive of this transformation.

The economic benefits of a modernized grid will accrue as investments are made. Indeed, in my view, our 21st century digital economy depends on us making these investments, in risk-managed and systematic ways.