Smart Grid—Safe, Secure, Self-Healing

Challenges and Opportunities in Power System Security, Resiliency, and Privacy

THE EXISTING POWER DELIVERY system is vulnerable to both natural disasters and intentional attack. 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. Secure and reliable operation of the electric system is fundamental to national and international economic systems, security, and quality of life.

This is not new: both the importance and the difficulty of protecting power systems have long been recognized. In 1990, the U.S. Office of Technology Assessment (OTA) issued a detailed report, *Physical Vulnerability of the Electric System to Natural Disasters and Sabotage*. The report concluded: "Terrorists could emulate acts of sabotage in several other countries and destroy critical [power system] components, incapacitating large

By S. Massoud Amin and Anthony M. Giacomoni

Digital Object Identifier 10.1109/MPE.2011.943112
Date of publication: 13 December 2011

1540-7977/12/$31.00©2012 IEEE

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 costs of widespread outages, estimating them to be in the range of US$1 to US$5 per kWh of disrupted service, depending on the length of the outage, the types of customers affected, and a variety of other factors. In the New York City blackout of 1977, for example, damage from looting and arson alone totaled about US$155 million—roughly half of its total cost.

During the 20 years since the OTA report, the situation has become even more complex. Accounting for all critical assets includes thousands of transformers, line reactors, series capacitors, and transmission lines. Protecting all these diverse and widely dispersed assets is impractical. Moreover, cyber, communication, and control layers add new benefits only if they are designed correctly and securely.

Electricity Infrastructure: Increasing Interdependencies

Energy, telecommunications, transportation, and financial infrastructures are becoming increasingly interconnected, thus posing new challenges for their secure, reliable, and efficient operation. All of these infrastructures are complex networks—geographically dispersed, nonlinear, and interacting both among themselves and with their human owners, operators, and users (see Figure 1).

Virtually every crucial economic and social function depends on the secure and reliable operation of these infrastructures. Indeed, they have provided much of the high standard of living that the more developed countries enjoy. With increased benefit, however, has come increased risk. As these infrastructures have grown more complex in order to handle increasing demands, they have become increasingly interdependent. The Internet, computer networks, and our digital economy have all increased the demand for reliable and disturbance-free electricity; banking and finance depend on the robustness of electric power, cable, and wireless telecommunications infrastructure. Transportation systems, including military and commercial aircraft and land and sea vessels, depend on communication and energy networks. Links between the power grid and telecommunications systems as well as between electrical power lines and oil, water, and gas pipelines continue to be the lynchpins of energy supply networks. This strong interdependence means that an action in one part of an infrastructure network can rapidly create global effects by cascading throughout the same network and even into other networks.

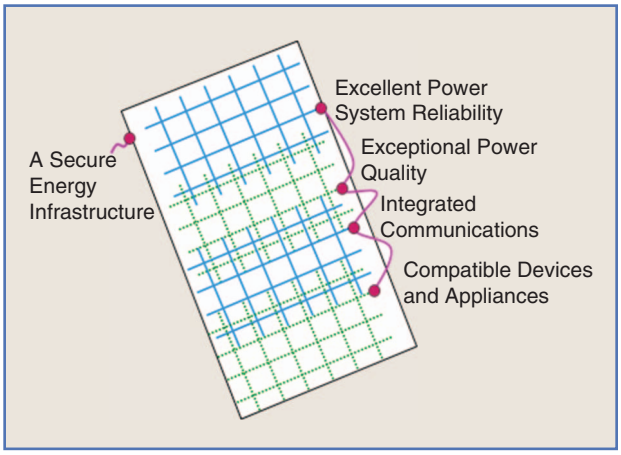

figure 1. A complex set of interconnected webs (source: EPRI, 2002–present).

In the aftermath of the tragic events of 11 September 2001 and recent natural disasters and major power outages, there have been increased national and international concerns expressed about the security, resilience, and robustness of critical infrastructures in response to an evolving spectrum of threats. There is reasonable concern that national and international energy and information infrastructures have reached a level of complexity and interconnection that makes them particularly vulnerable to cascading outages, whether initiated by material failure, natural calamities, intentional attack, or human error. The potential ramifications of network failures have never been greater, as the transportation, telecommunications, oil and gas, banking and finance, and other infrastructures depend on the continental power grid to energize and control their operations. Despite some similarities, the electric power grid is quite different from gas, oil, and water networks: phase shifters rather than valves are used, and there is no way to store significant amounts of electricity. Providing the desired flow on one line often results in "loop flows" on several other lines.

Potential Route Ahead: A Smarter Grid

The key challenge is to enable secure and very high-confidence sensing, communications, and control of a heterogeneous, widely dispersed, yet globally interconnected system. It is even more complex and difficult to control it for optimal efficiency and maximum benefit to the ultimate consumers while still allowing all its business components to compete fairly and freely.

To achieve this goal, a new "megainfrastructure" is emerging from the convergence of energy, telecommunications, transportation, the Internet, and electronic commerce. In the electric power industry and other critical infrastructures, new ways are being sought to improve network efficiency by eliminating congestion problems without seriously diminishing reliability and security. Nevertheless, the goal of transforming the current infrastructures into self-healing energy delivery, computer, and communications networks with unprecedented robustness, reliability, efficiency, and quality for customers and our society is ambitious.

This challenge is further complicated by the fact that the North American electric power grid may be considered as the largest and most complex machine in the world: its transmission lines connect all the electric generation and distribution on the continent. This network represents an

enormous investment, including more than 15,000 generators in 10,000 power plants and hundreds of thousands of miles of transmission and distribution lines. With diminished transmission and generation capacity and with dramatic increases in interregional bulk power transfers and the diversity of transactions, the electric power grid is being used in ways for which it was not originally designed. Grid congestion and atypical power flows have been increasing during the last 25 years, while customer expectations of reliability and cyber and physical security are rising to meet the needs of a pervasively digital world.

Upgrading the control and communication systems for the power grid will present many new security challenges that must be dealt with before extensive deployment and implementation of smart grid technologies can begin. The digitization of such systems may enable remote attacks to grow rapidly, potentially spanning countries or even continents. Moreover, the number of threats against computer systems is rapidly increasing due to the increased availability of highly sophisticated hacker tools on the Internet and the decrease in technical knowledge required to use them to cause damage. While the digitization of such systems will present many new security challenges, it will also provide the grid with increased flexibility to prevent and withstand potential threats.

Key Smart Grid Security Challenges

Physical Challenges

The size and complexity of the North American electric power grid makes it impossible both financially and logistically to physically protect the entire infrastructure. There currently exist more than 450,000 mi of 100-kV or higher transmission lines and many more thousands of miles of lower-voltage lines. As an increasing amount of electricity is generated from distributed renewable sources, the problem will only be exacerbated; the U.S. Department of Energy (DOE) has concluded that generating 20% of all electricity with land-based wind installations will require at least 20,000 square miles. Thus it is probable that a well-organized, determined group of terrorists could take out portions of the grid as they have previously done in the United States, Colombia, and other locations around the globe. Several such incidents in the United States have been publicly reported during the last 30 years, including saboteurs operating in the Pacific Northwest and those using power lines and transformers for target practice on the East Coast. Colombia, for example, has faced up to 200 terrorist attacks per year on its transmission infrastructure over the last 11 years, as reported in a recent *IEEE Power & Energy Magazine* article by Corredor and Ruiz. Such attacks, although troublesome and costly to the local region, affect only a small portion of the overall grid, however. To cause physical damage equivalent to that from a small to moderate-size tornado would be extremely difficult, even for a large, well-organized group of terrorists.

Data on terrorist attacks on the world's electricity sector from 1994–2004 from the Oklahoma-based Memorial Institute for the Prevention of Terrorism show that transmission systems are by far the most common target in terms of the total number of physical attacks. Figure 2 shows the percentage of terrorist attacks aimed at each of the major grid components.

One possible means of increasing the physical security of power lines is to bury them. A 2006 study by the Edison Electric Institute (EEI) calculated that putting power lines underground would cost about US$1 million per mile, compared with US$100,000 per mile for overhead lines, making the idea financially infeasible.

Cyber Challenges

The number of documented cyberattacks and intrusions worldwide has been rising very rapidly in recent years. The results of a 2007 McAfee survey highlight the pervasiveness of such attacks. For example, Figure 3 shows the percentage of IT and security executives from critical infrastructure enterprises located in 14 countries around the world reporting large-scale distributed denial-of-service (DDoS) attacks and their frequency.

DDoS attacks utilize networks of infected computers—whose owners often do not even know that they have been infected—to overwhelm target networks with millions of fake requests for information over the Internet.

Due to the increasingly sophisticated nature and speed of malicious code, intrusions, and DoS attacks, human responses may be inadequate. Figure 4 shows the evolution of cyberthreats over the last two decades and the types of responses that can be used to combat them effectively.

In addition, adversaries often have the potential to initiate attacks from nearly any location in the world. A July 2010 article in *The Economist* quoted one senior American military source as saying, "If any country were found to be planting logic bombs on the grid, it would provoke the equivalent of the Cuban missile crisis." Furthermore, currently

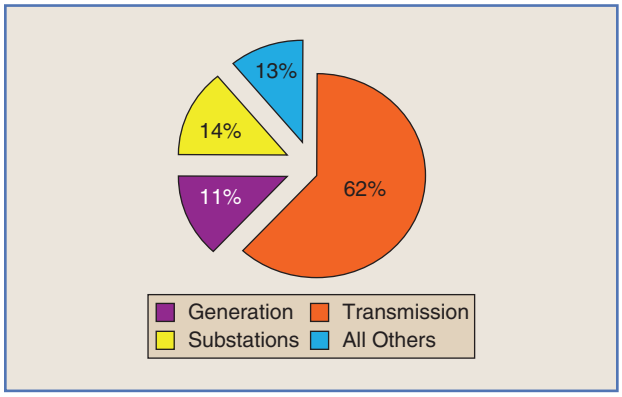

figure 2. Electric terrorism: grid component targets, 1994–2004 (source: *Journal of Energy Security*).

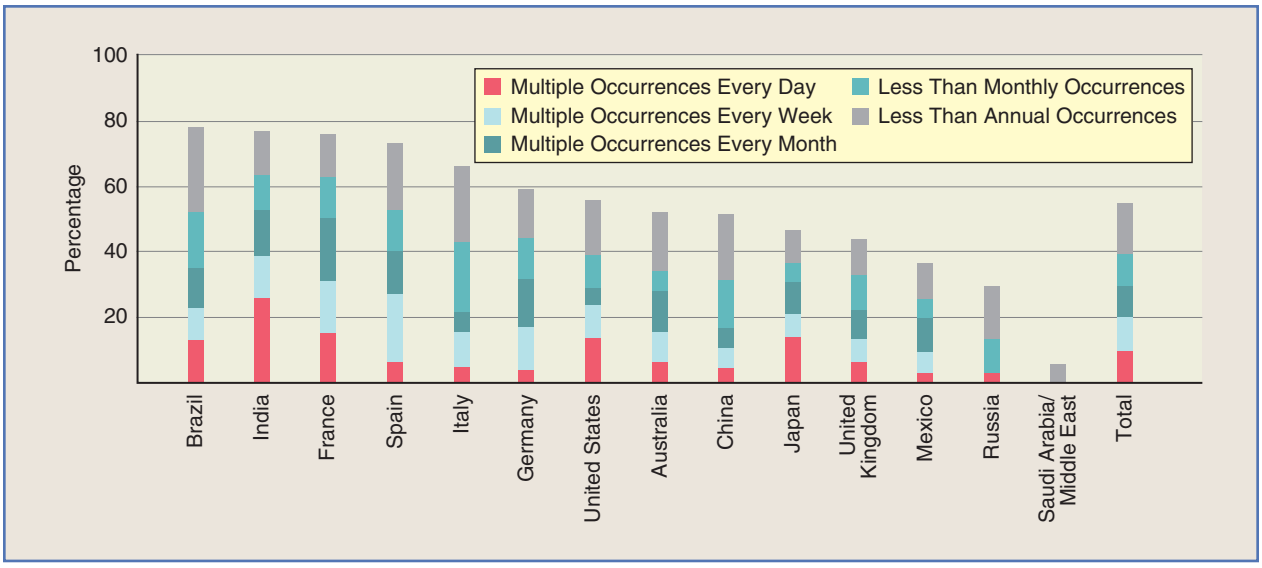

figure 3. Percentage of critical infrastructure enterprise executives reporting large-scale DDoS attacks and their frequency (source: McAfee).

more than 90% of successful cyberattacks take advantage of known vulnerabilities and misconfigured operating systems, servers, and network devices.

The security of cyber and communication networks is fundamental to the reliable operation of the grid. As power systems rely more heavily on computerized communications and control, system security has become increasingly dependent on protecting the integrity of the associated information systems. Part of the problem is that the existing control systems, which were originally designed for use with proprietary, stand-alone communication networks, were later connected to the Internet (because of its productivity advantages and lower costs) but without adding the technology needed to make them secure. Moreover, numerous types of communication media and protocols are used in the communication and control of power systems. Within a substation control network, it is common to find commercial telephone lines as well as wireless, microwave, optical fiber, and Internet connections. The diversity and lack of interoperability among the various communication protocols cause problems for anyone who tries to establish secure communication to and from a substation.

Electric power utilities also typically own and operate at least certain portions of their own telecommunications

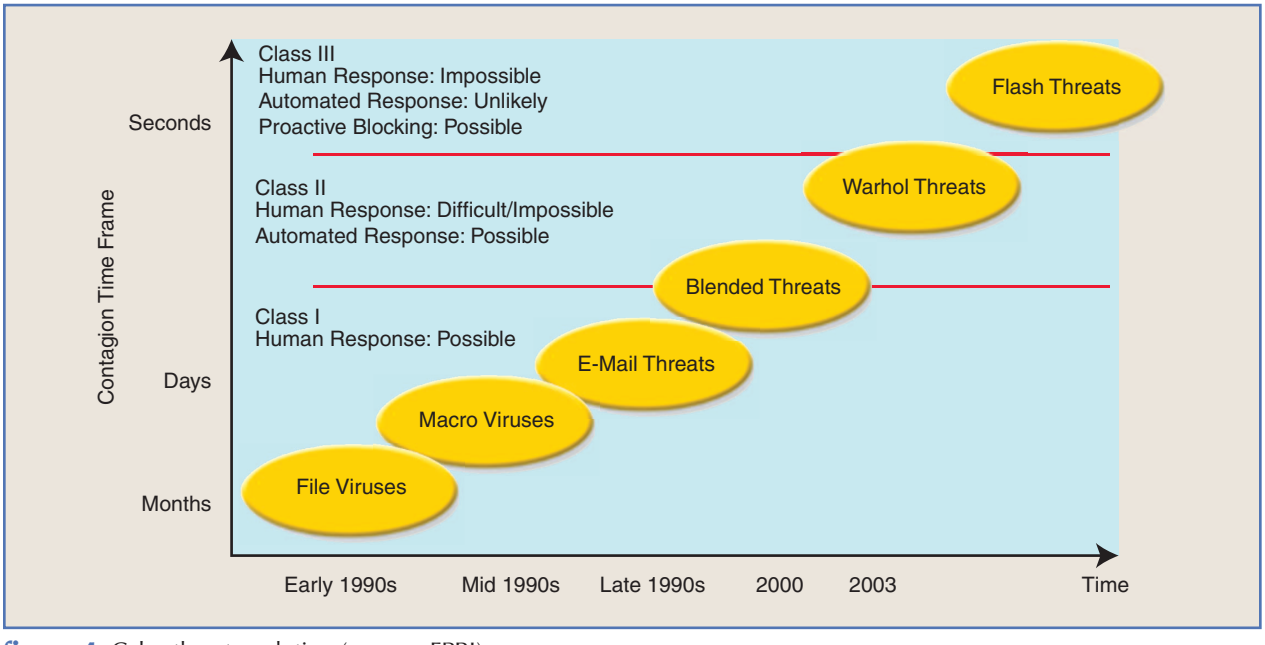

figure 4. Cyberthreat evolution (source: EPRI).

systems, which often consist of a backbone of fiber optic or microwave links connecting major substations with spurs to smaller sites. Increased use of electronic automation raises significant issues regarding the adequacy of operational security, if security provisions are not built in.

More specifically, the operation of a modern power system depends on complex systems of sensors and automated and manual controls, all of which are tied together through communication systems. While the direct physical destruction of generators, substations, or power lines may be the most obvious strategy for causing blackouts, activities that compromise the operation of sensors, communications, and control systems by spoofing, jamming, or sending improper commands could also disrupt the system, cause blackouts, and in some cases result in physical damage to key system components.

Any telecommunication link that is even partially outside the control of the organization that owns and operates power plants, supervisory control and data acquisition (SCADA) systems, or energy management systems (EMSs) represents a potentially insecure pathway into the business operations of the company as well as a threat to the grid itself. The interdependency analyses done by most companies in the last 12–14 years (starting with the preparations for Y2K and continuing after the tragic events of 9/11) have identified these links and the system's vulnerability to their failure. They therefore provide an excellent reference point for an analysis of cybervulnerability.

While some of the operations on the system are automatic, human operators in system control centers ultimately make the decisions and take the actions that control the operations of the system. In addition to the physical threats to such centers and the communication links that flow in and out of them, one must be concerned about two other factors: the reliability of the operators within the centers and the possibility that insecure code has been added to a program in a center computer. The threats posed by "insiders" are real, as is the risk of a "Trojan horse" embedded in the software of one of more of the control centers. A 2008 survey by the Computer Security Institute and the U.S. Federal Bureau of Investigation of data compiled from 522 computer security practitioners and senior executives of U.S. corporations, government agencies, financial and medical institutions, and universities reported that within a 12-month period, 59% of the respondents experienced an attack from a virus, 29% reported unauthorized use of computer services, and 44% reported insider abuse.

The threat of a "Trojan horse" embedded in the control center software can only be addressed by means of careful security measures within the commercial firms that develop and supply this software along with careful security screening of the utility and outside service personnel who perform software maintenance within the centers. Today, security patches often are not supplied to end users, or users are not applying the patches, as they fear they will affect system performance. Current practice is to apply an upgrade or patch only after SCADA vendors thoroughly test and validate it, and this sometimes causes deployment to be delayed by several months.

As a result, cybersecurity is just as important as physical security, if not more so. Due to the gravity of these threats, the Federal Energy Regulatory Commission (FERC) policy statement on the smart grid states that cybersecurity is essential to the operation of the smart grid and that the development of cybersecurity standards is a key priority. The DOE has also stated that the ability to resist attack by identifying and responding to disruptions caused by sabotage is one of the smart grid's seven crucial functions. Much work remains to be done, however, to create standards that, when implemented, will adequately protect the grid from cyberattacks. Emerging standards fall well short of achieving this ultimate goal.

Smart Grid Security Needs

Layered Security

In order to protect electric infrastructure from the threats outlined above, several layers of security are needed to minimize disruptions to system operations. Layered security (or "defense in depth") involves strategically combining multiple security technologies at each layer of a computing system in order to reduce the risk of unauthorized access due to the failure of any single security technology. It exponentially increases the cost and difficulty of compromising a system by creating a much stronger defense than the use of any individual component alone, thus reducing the likelihood of an attack.

The trend of connecting electrical control systems to the Internet exposes all layers of a system to possible attack. Computing layers that must be considered include

- ✔ personnel
- ✔ networks
- ✔ operating systems
- ✔ applications
- ✔ databases.

The security features to be employed at each layer include examination, detection, prevention, and encryption. To protect control systems, well-established information security practices must also be utilized.

Deception

An additional defense mechanism is the use of deception. Deception consists of two possible techniques: dissimulation (hiding the real) and simulation (showing the false). McQueen and Boyer describe several potential dissimulation and simulation techniques that can be used for control systems. Three of the dissimulation techniques described are:

- ✔ *masking* the real by making a relevant object undetectable or blending it into background irrelevance
- ✔ *repackaging*, which hides the real by making a relevant object appear to be something it isn't

Upgrading the control and communication systems for the power grid will present many new security challenges that must be dealt with.

- ✔ *dazzling*, which hides the real by making the identification of a relevant object less certain by confusing the adversary about its true nature.

Likewise, three of the simulation techniques described are:

- ✔ *inventing* the false by creating a perception that a relevant object exists when it doesn't
- ✔ *mimicking*, which invents the false by presenting characteristics of an actual and relevant object
- ✔ *decoying*, which displays the false so as to attract attention away from a more relevant object.

Deception will need to play a key role in smart grid defense mechanisms. Since existing control system architectures are not random and therefore response characteristics are reproducible, the strength of potential adversaries is amplified. Defense mechanisms using deception can greatly increase the difficulty of planning and conducting successful attacks on a system by portraying control system response characteristics as random to attackers. They can also alert operators to possible threats before any systems are harmed.

Additional security needs include rapid containment, restoration, and recovery strategies for times when systems are inevitably compromised. Either software patching or the ability to rapidly identify and isolate the exploited systems must be enabled in order to minimize downtime. This is extremely important, since the consequences of an attack are directly proportional to the length of time the service is disrupted.

Advanced Metering Infrastructure

Vulnerabilities

The implementation of advanced metering infrastructure (AMI) is widely seen as one of the first steps in the digitization of the electric grid's control systems. Despite the increase in the utilization of AMI, there has been very little assessment or R&D effort to identify the security needs for such systems. Smart meters, however, are extremely attractive targets for exploitation, since vulnerabilities can be easily monetized through manipulated energy costs and measurement readings. Currently, in the United States alone it is estimated that US$6 billion is lost by electricity providers to consumer fraud in the electric grid. Possible threats to the electrical grid introduced by the use of AMI include:

- ✔ fabricating generated energy meter readings
- ✔ manipulating energy costs
- ✔ disrupting the load balance of local systems by suddenly increasing or decreasing the demand for power
- ✔ gaining control of millions of meters and simultaneously shutting them down
- ✔ sending false control signals
- ✔ disabling grid control center computer systems and monitors
- ✔ disabling protective relays.

As more utilities move toward using Internet Protocol (IP)–based systems for wide area communications and as the trend of using standardized protocols continues throughout the industry, maintaining the security of such devices will be critical. AMI introduces serious privacy concerns, as immense amounts of energy use information will be stored at the meter. Breaches into this data could expose customer habits and behaviors. Such arguments have led to the recent moratoriums on AMI installations in numerous northern California communities and other areas throughout the country. As a result, several key privacy concerns need to be addressed, including those outlined by the Cyber Security Working Group of the U.S. National Institute of Standards and Technology (NIST). These include:

- ✔ **Personal profiling:** using personal energy data to determine consumer energy behavioral patterns for commercial purposes
- ✔ **Real-time remote surveillance:** using live energy data to determine whether people are in a specific facility or residence and what they are doing
- ✔ **Identity theft and home invasions:** protecting personal energy data from criminals who could use the information to harm consumers
- ✔ **Activity censorship:** preventing the use of energy for certain activities or taxing those activities at a higher rate
- ✔ **Decisions based on inaccurate data:** shutting off power to life-sustaining electrical devices or providing inaccurate information to government and credit-reporting agencies.

In addition, AMI systems will need to be defended against more traditional cyberthreats such as mobile and malicious code, DoS attacks, misuse and malicious insider threats, accidental faults introduced by human error, and the problems associated with software and hardware aging.

Security Needs

In order to defend against the vulnerabilities described above, several security features need to be incorporated into

the development of AMI, along with new privacy laws to protect consumers. Current privacy laws in the United States are fragmented and vague and do not specifically address consumer energy usage. Data stored at the meter and transmitted over communication networks must also meet standard cybersecurity requirements, including confidentiality, integrity, availability, and nonrepudiation.

One security feature alone, such as encryption, will not be able to cover all the possible security threats. Since it is imperative that the industry maintain 100% uptime, both the physical security of the AMI system hardware and multiple standard IT security features like encryption and authentication must be provided for. Furthermore, since it will be impossible to protect against all threats, smart meters must be able to detect even the most subtle unauthorized changes and precursors to tampering or intrusion. Additional consideration must also be given to the cost and impact the security features will have on AMI system operations. Smart meters will need to be cost-effective, since millions will need to be purchased and installed to replace antiquated analog devices. And they must also be robust as they will be deployed in very insecure locations.

Current Security Initiatives

Since the terrorist attacks of 11 September 2001, several steps have been taken and initiatives accomplished to enhance the security and reliability of the nation's current electricity infrastructure. These include the Complex Interactive Networks/Systems Initiative (CIN/SI), a joint program sponsored by the Electric Power Research Institute (EPRI) and the U.S. Department of Defense (DOD); EPRI's Enterprise Information Security (EIS) program; EPRI's post–9/11 Infrastructure Security Initiative (ISI); and various North American Electric Reliability Corporation (NERC) initiatives, such as its information sharing and analysis centers (ISACs), public key infrastructure (PKI), and spare equipment database. Information security frameworks for electric power utilities have also been developed by the International Council on Large Electric Systems (CIGRE). A security framework is considered as the skeleton on which various elements are integrated for the appropriate management of security risk. The various elements considered by CIGRE include security domains, baseline controls, and security processes.

Research and Development Needs

The Smart Infrastructure: A Smarter, More Secure I-35W Bridge

Within less than a year after the August 2007 collapse of the I-35W bridge in Minneapolis, Minnesota, a city of sorts on the south side of the former bridge took shape, complete with a host of heavy-duty equipment pieces, temporary on-site areas for casting and other tasks, and crews constantly at work. The days and months that followed required extraordinary efforts from many, including alumni of the University of Minnesota's infrastructure systems engineering program. They incorporated a sensor network into the new I-35W bridge (at less than 0.5% of total cost) that provides full situational awareness of stressors, fatigue, material, and chemical changes, so as to measure and understand the precursors to failure and to enable proactive and a priori corrective actions.

Analogously, customized and cost-effective advancements are both possible and essential to enable smarter and more secure electric power infrastructures. For example, advanced technology now under development or under consideration holds the promise of meeting the electricity needs of a robust digital economy. The end vision of the smart grid consists of a highly developed electrical platform that engages consumers, enhances efficiency, ensures reliability, and enables integration of renewable energy and electric transportation.

One key money- and power-saving element of the smart grid is its ability to measure how and when consumers use the most power. This information allows consumers to be charged variable rates for energy, based upon supply and demand. This variable rate will incentivize consumers to shift their heavy use of electricity to times of the day when demand is low.

The total cost of a stronger transmission system would be about US$82 billion over the next decade. Additionally, to create a smarter end-to-end power delivery system, we must invest between US$17 and US$24 billion over the next 20 years.

Investment in a smart grid would nearly pay for itself by reducing stupendous outage costs, a savings of US$49 billion per year, and improving energy efficiency, a savings of US$20.4 billion per year. Likewise, through smart grid-enhanced energy efficiency, by 2030 carbon dioxide emissions from the electric sector would be reduced by 58%.

Americans should not accept or learn to cope with increasing blackouts, nor should we rest on the notion that the technical know-how, political will, or money to bring our power grid up to 21st century standards do not exist. The truth is that, as a nation, we must and absolutely can meet the power needs of a pervasively digital society if the United States wishes to maintain its role as a global economic and political leader. The best of American innovation is yet to come, and the smart grid must be part of our future. The potential exists to create an electricity system that provides the same efficiency, precision, and interconnectivity as the billions of microprocessors that it will power.

From a strategic viewpoint, long-term developments and research issues relating to the defense of cyber and physical interdependent infrastructure networks must also be considered. The driving scientific motivation is to further our understanding of adaptive self-healing and self-organizing

mechanisms that can be applied to the development of secure, resilient, and robust overlaid and integrated energy, power, sensing, communication, and control networks.

In addition to the above, further research and development needs include the following areas:

1) **Enabling technologies for an end-to-end secure system of sensing and measurement, leading to improved analysis and visualization and eventually to automation and self-healing systems:**
   - monitoring and analysis, automation and control, materials science, power electronics, and integrated distributed energy resources (DERs)
   - sensing, communication, data management, and mathematical and theoretical foundations to support a better, faster, and higher-confidence understanding of what is going on, leading to improved state and topology estimation and fast look-ahead simulation.
2) **Enabling a stronger and smarter grid by means of complex dynamical systems, systems science, controls, and applied mathematics:**
   - modeling, robust control, dynamic interaction in interdependent layered networks, disturbance propagation in networks, and forecasting and handling uncertainty and risk
   - overall systems science and dynamics (including infrastructure, ecology and environment, markets, and data-driven policy designs).
3) **Strategic R&D:**
   - digital control of the energy infrastructure
   - integrated energy, information, and communications for the end user
   - transformation of the meter into a secure, two-way energy and information portal
   - robust advanced power generation portfolio.

Awareness, education, and pragmatic tool development in this vital area continue to remain challenges. Educating stakeholders and colleagues about the cyber and physical interdependencies has often been difficult, as those who are distinguished members of the community and understand power systems well but are less aware of their cybervulnerabilities routinely minimize the importance of these novel—and persistent—threats.

Conclusion

Cyberconnectivity has increased the complexity of the control systems and facilities it is intended to safely and reliably control. In order to defend electric infrastructure against the impacts of cyber and physical attacks, significant challenges must therefore be overcome before extensive deployment and implementation of smart grid technologies can begin. Cybersecurity and interoperability are two of the key challenges of the smart grid transformation. As for security, it must be built in as part of its design, not glued on as afterthought.

Regarding recent cyberthreat reports, it is fundamental to separate the "hype" from the truth. What is most concerning about such reports is mainly one portion of an early article: "The response to the alert was mixed. An audit of 30 utility companies that received the alert showed that only seven were in full compliance, although all of the audited companies had taken some precautions." This is the reality that needs to be addressed.

Finally, no matter how many layers of security or how much sophistication is used in defense mechanisms, it is essential that the industry hire qualified people. Research findings suggest that human and organizational factors do affect computer and information security performance in a multilayered fashion. Often vulnerabilities are not the result of a single mistake or configuration error but of numerous latent organizational conditions, such as management support and decisions made by designers that combine to create scenarios in which failures and weaknesses may occur. In many complex networks, the human participants themselves are both the most susceptible to failure and the most adaptable in the management of recovery. Thus, staff members must be well trained to respond to a wide variety of emergencies since no amount of technology can replace well-trained personnel.

For Further Reading

J. Clemente, "The security vulnerabilities of smart grid," *J. Energy Security*, June 2009.

P. H. Corredor and M. E. Ruiz, "Against all odds," *IEEE Power Energy Mag.*, vol. 9, no. 2, pp. 59–66, Mar./Apr. 2011.

G. N. Ericsson, "Information security for electric power utilities (EPUs)-CIGRE developments on frameworks, risk assessment, and technology," *IEEE Trans. Power Delivery*, vol. 24, no. 3, pp. 1174–1181, July 2009.

P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security Privacy*, vol. 7, no. 3, pp. 75–77, May/June 2009.

M. A. McQueen and W. F. Boyer, "Deception used for cyber defense of control systems," in *Proc. 2nd Conf. Human System Interactions,* Catania, Italy, 2009, pp. 624–631.

NIST, "Guidelines for smart grid cyber security," The Smart Grid Interoperability Panel—Cyber Security Working Group, NISTIR 7628, Gaithersburg, MD, Aug. 2010.

S. M. Amin, "Securing the electricity grid," *Bridge*, vol. 40, no. 1, pp. 13–20, Spring 2010

S. M. Amin, "Energy infrastructure defense systems," *Proc. IEEE*, vol. 93, no. 5, pp. 861–875, May 2005.

S. M. Amin, "Balancing market priorities with security issues: Interconnected system operations and control under the restructured electricity enterprise," *IEEE Power Energy Mag.*, vol. 2, no. 4, pp. 30–38, Jul./Aug. 2004.

Biographies

S. Massoud Amin is with the University of Minnesota.

Anthony M. Giacomoni is with the University of Minnesota.