Power and Energy Infrastructure

Cyber Security, Defense, and Resilience

S. Massoud Amin

Virtually every crucial economic and social function depends on the secure, reliable operation of power and energy infrastructures. Energy, electric power, telecommunications, transportation and financial infrastructures have become increasingly interdependent, posing new challenges for their resilient and efficient operation. All of these interdependent infrastructures are complex, geographically dispersed, non-linear, and interacting both among themselves and with their human owners, operators and users.

The end-to-end electric power network, grid communications and control systems are often thought to be much more securely protected than is actually the case, especially to malware and intrusions. Over the last two decades, power outages in the United States have increased in size and frequency. This trend is likely to continue as the number of energy consumers increase while infrastructure investment remains stagnant.[1] These circumstances have highlighted the need to update the nation's electric power grid to provide secure and reliable electricity for the future.

Both the importance and difficulty of protecting power systems have long been recognized. In the electricity sector, outages and power quality disturbances cost the economy

S. Massoud Amin is Distinguished Professor of Electrical and Computer Engineering at the University of Minnesota, where he directs the Technological Leadership Institute. Prior to that, he was the Area Manager of Infrastructure Security, Grid Operations, and Energy Markets at the Electric Power Research Institute, where he pioneered research and development in smart grids and self-healing infrastructure. He holds leadership positions on the Texas and Midwest Reliability entities and is the Chairman of IEEE Smart Grid.

more than $80 billion annually on average, and sometimes as much as $188 billion in a single year. Since 1995, the amortization and depreciation rate of old transmission investments has exceeded new construction expenditures. It has been apparent for over a decade that the grid is increasingly stressed, and that the carrying capacity or safety margin to support anticipated demand is in question.[2]

The age of our power infrastructure – particularly underground city networks – is a major issue that should not be viewed in isolation. Instead, the power industry's focus should be on a holistic asset management approach to address grid resilience. That focus should weigh the relative risks and benefits of maintenance, repair and replacement or retirement of the infrastructure's various elements. These elements include thousands of transformers, line reactors, series capacitors, and transmission lines. A holistic approach also requires viewing the utility fleet of capital equipment as critical strategic assets impacted by age and external forces, possessing capabilities and characteristics that can be leveraged to improve reliability.

Cost-effective solutions for holistic asset management depend on rational risk assessment and management. While it is impossible to predict when and where future events will occur, it is possible to identify the substations and lines in the system that pose the greatest risk for large-scale outages. These results can then be used to tailor grid resiliency investments to focus on facilities with the greatest risk for future events. While macro-forces have the potential to impact the nation's power infrastructure, risk is dynamic, local, and specific. National policies that support holistic asset management will be helpful, but achieving hardening and resiliency on the ground will ultimately need to be specific to utility customers' needs, its legacy systems, and its location and technology roadmap. In this manner, this article seeks to provide a state-of-the-art review of non-classified cyber security challenges and opportunities within this framework. By understanding the true breadth of risks and dynamics of complex, interdependent power systems, policymakers, industry leaders, and customers can progress toward smarter, stronger, and more secure networks of energy and commerce.

Reliability. According to data assembled by the U.S. Energy Information Administration (EIA), for most of the decade between 2001-2010, there were 200 outages of 100 megawatts or more during 2001-2005; such outages have increased to 236 during 2006-2010. The number of U.S. power outages affecting 50,000 or more consumers increased from 197 during 2001-2005 to 348 during 2006-2010.[3]

Adjusting conservatively for a 2 percent per year increase in load to 2001 levels, these outages reflect a trend. First, there were 189 outages of 100 megawatts or more during 2001-2005; such outages slightly increased to 206 during 2006-2010. Second, assuming the same 2 percent annual demand growth, the number of U.S. power outages affecting 50,000 or more consumers increased from 186 during 2001-2005 to 303 during 2006-

2010. This trend has persisted at a greater frequency from 2011-2015.[4]

Planning and implementation efforts to replace aging electric infrastructure with digital systems that provide the grid with the capability to reconfigure itself and prevent widespread outages are already underway. This collection of digital overlaid systems is referred to as a 'smart grid.' In 2007, the United States Congress passed the Energy Independence and Security Act (EISA), which outlined specific goals for the development of the nation's smart grid. Those goals include increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid, as well as dynamic optimization of grid operations and resources with full cyber security.[5]

Despite these positive developments, however, the electric power sector is the second-worst of all major U.S. industries in terms of research and development (R&D) spending as a percentage of revenue, bested only by the pulp and paper industry. In fact, R&D represented a meager 0.3 percent of net sales in the period of 1995 to 2000, and declined even further to 0.17 percent between 2001 and 2006 and has continued to hover on the extreme low-end of the spending scale for the past decade.[6] As the digitization of society continues to expand, it becomes increasingly critical that we make investments in development if we want to accommodate the growing need for electricity. In fact, it is projected the world's electricity supply will need to triple by 2050 to keep up with demand.

To achieve the objectives outlined by EISA, the electrical power industry should promote the application of widespread condition monitoring, and integration of real-time operational data. Such applications have been shown to benefit real-time system operations, both in terms of asset utilization and in terms of graceful, planned replacement of stricken assets. Condition-based asset monitoring is preferable to reactive "fix-on-fail" approaches that can be both dangerous and costly.[7]

Incorporating elements of the smart grid will aid in achieving a holistic asset management approach. The addition of centralized and distributed intelligence — via built-in secure sensors, communications, monitors, optimal controls and computers — to our electric grid, can substantially improve its efficiency and reliability through increased situational awareness. This can further provide actionable intelligence, resulting in reduced outage propagation and

It has been apparent for over a decade that the grid is increasingly stressed, **and that the carrying capacity or safety margin to support anticipated demand is in question.**

improved response to disturbances.[8]

Security. 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," which concluded terrorists could "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."[9] In the 25 years since the OTA report, the situation has become even more complex. Accounting for and protecting all critical assets of the electric-power system (which include thousands of transformers, line reactors, series capacitors, and transmission lines dispersed across the continent), is an even harder task using outdated systems. The addition of cyber and automation capabilities have greatly improved grid functionality, but have also introduced new spectra of security threats.[10]

The U.S. Nuclear Regulatory Commission confirmed many of OTA's concerns in January 2003. The commission announced that the Microsoft SQL Server worm known as Slammer had infected a private computer network at the Davis-Besse nuclear power plant in Oak Harbor, Ohio, disabling a safety monitoring system for nearly five hours. Fortunately the plant was offline at the time. Seven months later, however, its offline status was a factor in the big Midwest-Northeast blackout, the bi-national Outage Task Force Report found.[11] Additionally, in January 2008, the CIA reported that the agency knew of four incidents overseas where hackers were able to disrupt, or threaten to disrupt, the power supply of four foreign cities.[12] More recently, the 2011 Stuxnet attack against Iran's Natanz nuclear facilities demonstrated the possibility of uploading malicious code to a power facility's Programmable Logic Controllers (PLCs) to physically damage energy infrastructure without the operators' immediate knowledge.[13]

Types of Vulnerabilities. In order to defend against today's panoply of evolving threats in addition to the insider/human and enterprise-wide security aspects, physical and cyber grid vulnerabilities must be understood.

A. Physical. The size and complexity of the North American electric power grid makes it financially and logistically impossible to physically protect the entire infrastructure sector. There currently exist over 450,000 miles of 100 kV or higher transmission lines, and many more thousands of miles of lower-voltage lines.[14] The Department of Energy (DOE) concluded this problem will only get worse as distributed renewable sources generate a greater share of electricity.[15] Thus, a well-organized determined group of terrorists could likely take out portions of the grid, as they have done previously in the United States, Colombia, and other locations around the globe.[16] Such an attack, although troublesome and costly to the local region, would only be a small portion of the overall grid. To cause physical damage equivalent to that of a small-to moderate-scale tornado would be extremely difficult, though not impossible, for even for a large well-organized group of ter-

rorists to accomplish.[17] As data from the National Memorial Institute for the Prevention of Terrorism confirms, data on terrorist attacks on the world's electricity sector from 1994-2004 shows transmission systems, including lines and substations, are by far the most common target in terms of total number of physical attacks.[18]

B. Cyber. While physical attacks are real and frightening possibilities, cyber attacks have the potential to be just as, if not more, destructive and carry the added threats of stealth and long-distance control.[19] Threats from cyberspace to our electrical grid are rapidly proliferating, and while there have been no publicly known major power disruptions due to cyber attacks, public disclosures of vulnerabilities are making these systems more attractive targets. According to the U.S. Department of Defense, an Al-Qaeda training manual claims, "Using public sources openly and without resorting to illegal means, it is possible to gather at least 80 [percent] of information about the enemy." When it comes to the electric grid, it could be possible to collect relevant vulnerability information from publicly available trade journals, which document the transmission capacity of switching stations and the geographic areas that they are responsible for. Furthermore, the ease of use, anonymity, and access to massive amounts of data makes cyberspace an ideal venue for individuals such as terrorists to plan and coordinate attacks on grid and energy infrastructure.[20]

Along these lines, the cyber risks stem primarily from connecting infrastructure control systems that were originally designed for use with proprietary, stand-alone communications networks to the Internet. This linkage increased productivity and lowered costs, but largely did not include adding the required technology to make the control systems secure.[21] The sheer number of types of equipment and protocols used in the communication and control of power systems exacerbate the problem. The diversity and lack of interoperability in the communication protocols causes problems for anyone who tries to establish secure communication to and from a substation (or among substations in a network of heterogeneous protocols and devices). Furthermore, operators use a wide assortment of communications media to access the control equipment. Within a substation control network, it is common to find commercial telephone lines, wireless, microwave, private fiber, and Internet connections.[22] This adds another layer of complexity and vulnerability to the picture.

As a result, cyber security is just as important if not more so than physical security. In reality, a holistic and all-hazard systems' approach, which includes cyber-physical, the end-to-end enterprise and its human capital, supply chains, along with her primary, secondary, and tertiary interdependencies, is needed. Due to the gravity of these threats, the Federal Energy Regulatory Commission policy statement on smart grid development stated that cyber security is essential to the operation of the smart grid, and the development of cyber security standards is a key priority.[23] However, significant work must still be done to create standards to adequately protect the grid from cyber

attacks. Current standards fall short of achieving this ultimate purpose.[24]

Yet it is important to note that upgrading 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.[25] Reference defines a threat as being a person, thing, event, or idea that poses some danger to an asset and/or organization in terms of that asset's confidentiality, integrity, availability, or legitimate use.[26] An attack is defined as the actual realization of a threat. For example, possible effects of cyber attacks can include the loss of load, the loss of information, harm to human life and the environment, as well as the economic loss, and/or the equipment damage, depending on the severity and objectives of the attack.[27] In this way, the digitalization of the electric grid may paradoxically enable the success of remote attacks.[28] The increased availability of technological means and know-how to compromise computer systems has lowered the threshold for a well-motivated individual or group to impose significant damage.[29] Consequently, while digitization of the electric grid will generate increased flexibility to prevent and withstand potential threats, without adequate security measures, that digitization will present many new security challenges to power infrastructure.

Power Grid Cyber Security. Since the terrorist attacks of September 11, 2001, several steps have been taken to enhance the security and reliability of the nation's 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 Department of Defense (DoD), as well as the North American Electric Reliability Corporation (NERC) initiatives such as the Information Sharing and Analysis Centers (ISACs), public key infrastructure (PKI), and spare equipment databases.[30]

...cyber attacks have the potential to be just as, if not more, destructive [than physical attacks] and carry the added threats of stealth and long-distance control.

Key individuals and institutions are also taking a leading role in developing solutions to cyber vulnerabilities.[31] Researchers at the University of Texas at Austin and the Naval Postgraduate School have developed an analytic technique to prevent disruptions to the grid from physical terrorist attacks.[32] Their method identifies critical sets of a power grid's components, which a terrorist group might target to inflict maximum damage. Carnegie Mellon and the University of Minnesota have been developing a new distributed model of predictive system estimation and distributed control theory to better

analyze the reliability of large-scale infrastructure systems. It is useful and necessary for these systems to have distributed or decentralized control schemes, where local control inputs are computed using local measurements and reduced-order models of the local dynamics.[33]

While these steps are necessary to promote cyber security of grid infrastructure, there are three core security practices that should be considered and implemented:

(1) Layered Security. Several layers of security are necessary to minimize cyber disruptions to system operations. Layered security--or defense-in-depth, according to the DoD--involves strategically combining multiple security technologies at each layer of a computing system to reduce the risk of unauthorized access due to the failure of any single security technology. This strategy exponentially increases the cost and difficulty for an attacker to compromise a system by creating a much stronger defense than that of any individual component alone, thus deterring an attack.[34] Operators should include examination, detection, prevention, and encryption features at each layer of security.[35] To protect control systems, well-established information security practices should be utilized.[36] M. Takano further describes several methods to improve the security of control systems based on a layered security mechanism.[37]

(2) Deception. Deception is an additional defense mechanism. Deception consists of two possible techniques: dissimulation (hiding the real) and simulation (showing the false). McQueen and Boyer describe potential dissimulation and simulation techniques that can be used for control systems.[38] Three potential dissimulation techniques are:

- *Masking* a real system by making a relevant object be undetectable or blend into background irrelevance.
- *Repackaging*, which hides a real system by making a relevant object appear to be something it isn't.
- *Dazzling*, which hides a real system by making the identification of the relevant object less certain by confusing the adversary about its true nature.

Likewise, three potential simulation techniques are:

- *Inventing* a false target by creating a perception that a relevant object exists when it doesn't.
- *Mimicking*, which invents a false target by presenting characteristics of an actual, and relevant object.
- *Decoying*, which uses a false system to attract attention away from more relevant objects.

Deception will play a key role in any smart grid defense mechanism. Under McQueen and Boyer's framework, the

[Layered security] exponentially increases the cost and difficulty for an attacker to compromise a system… **thus deterring an attack.**

individuals directly responsible for system security should be the only ones possessing perfect knowledge of the system's operations. Anyone who is unauthorized to an infrastructure's control system should be prevented from gaining knowledge of the system's design or configuration.[39] This way, deception-based defense mechanisms can portray control system response characteristics as random to attackers, and greatly increase the difficulty of planning and conducting successful attacks upon the system. They can also alert operators to possible threats before any systems are harmed, since attackers will be forced to counter possible deception techniques prior to gaining real access to the system itself.

(3) New Security Features. The security of cyber and communication networks is fundamental to the reliable operations of the grid. Yet cyber has "weakest link" issues. As power systems rely more heavily on computerized communication and control, system security has become increasingly dependent on protecting the integrity of the associated information systems. For instance, any utility system connected directly or indirectly to the public Internet is "disputed territory." That system is vulnerable to cyber intrusions, which can impersonate field devices to spoof bad data into a control center, potentially leading to erroneous decisions impacting the operation and safety of the grid.

In order to defend against potential cyber vulnerabilities, several security features need to be incorporated into the development of Advanced Metering Infrastructure (AMI), which is the integrated system of smart meters, communications networks, and data management systems that smart grids utilize for two-way communication between utilities and consumers.[40] One security feature alone, such as encryption, will not be able to cover all possible security threats.[41] Since it is imperative that the industry maintain 100 percent uptime, both physical security of the AMI system hardware and multiple standard IT security features like encryption and authentication will be needed.[42] 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.[43]

Additional consideration must also be given to both 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. They must also be sufficiently robust since they will be placed in very insecure locations, and they must be certified as "revenue grade" accurate.[44]

New security features must also be accompanied with new privacy laws to protect consumers. Current privacy laws in the United States are fragmented and vague, and they do not specifically address consumer energy usage.[45]

More importantly, developing the tools that increase awareness and education about cyber threats is paramount. Yet it has been an ongoing challenge; educating stakeholders and colleagues in the cyber-physical interdependencies has been difficult, as even distinguished members of the community who understand power

systems well routinely minimize persistent, novel threats. Improving the sharing of intelligence, threat information and analysis to develop proactive protection strategies might improve the situation. This will include the development of threat coordination centers at local, regional and national levels. To that end, the IEEE Task Force Report on priority issues in the 2014 Quadrennial Energy Review made recommendations on what role the U.S. federal government might play in support of state and local efforts to aid power and integrated utilities in increasing reliability, resilience and security.[46]

Difficult Choices. Like any complex, dynamic infrastructure system, the electricity grid has many layers and is vulnerable to many different types of disturbances. While strong centralized control is essential to reliable operations, this requires multiple technologies that are especially vulnerable when they are needed most: during serious system stresses or power disruptions. As security programs are built and protections put into place, difficult choices will have to be made about how to handle a number of trade-offs:

Outdated regulatory frameworks. Split regulatory jurisdiction over the grid is inhibiting investment and modernization efforts. Bulk electric systems are under federal control, but individual states control distribution, metering, and other aspects of the grid. Overlapping and inconsistent roles and authorities of federal agencies can hinder development of productive, public-private working relationships.[47] A new model for these relationships is required for infrastructure security. Additional regulatory reforms, such as the creation of a stockpiling authority, could obtain long lead-time equipment (such as transformers) based on the power industry's inventory of critical equipment, which decrease the probability an attack will substantially reduce grid functionality.

Investments in security. Although hardening some key components—such as power plants and critical substations—is highly desirable, providing comprehensive physical protection for all components is simply not feasible or economical. Dynamic, probabilistic risk assessments have provided strategic guidance on allocating security resources to greatest advantage.[48] However, pathways to cost recovery and making a business case for security investments and upgrades often pose challenges, since the benefits from those investments and upgrades are not always visible.

Security versus efficiency. The specter of future sophisticated terrorist attacks raises a profound dilemma for the electric power industry, which must make the electricity infrastructure more secure, while being careful not to compromise productivity. Resolving this dilemma will require both short- and long-term technology development and deployment. Supportive public policy to aid cost recovery could greatly incentivize development of new business models and strategies.

Centralization versus decentralization of control. For several years, there has been a trend toward centralizing control of electric power systems. Regional transmission organizations were introduced in order to greatly increase effi-

ciency and improve customer service. At the same time, terrorists can exploit the weaknesses of centralized control; therefore, a shift towards developing smaller and local semi-autonomous systems would seem to be preferable. In fact, strength and resilience in the face of attack will increasingly require the ability to bridge simultaneous top-down and bottom-up decision-making in real time—fast-acting and totally distributed at the local level, coordinated at the mid-level and aligned with national objectives.[49]

Wider grid integration and increasing complexity. System integration helps move power more efficiently over long distances and provides redundancy to ensure reliable service, but it also makes the system more complex and harder to operate. The utility industry will need new approaches to simplify the operation of complex power systems and make them more robust in the face of natural or human-made interruptions.

Dependence on Internet communications. Today's power systems could not operate without tightly knit communications capabilities ranging from high-speed data transfer among control centers to the interpretation of intermittent signals from remote sensors. But due to the vulnerability of Internet-linked communications, protecting the electricity supply system will require new technology to improve the security of power-system command, control and communications, including both hardware and software.[50]

Conclusion. This article sought to develop measures to understand and respond to cyber security challenges facing power and energy infrastructure. All these measures and more could be facilitated by more transparent, participatory and collaborative discussion among government agencies, transmission and distribution asset owners, regional transmission and independent system operators and their members to improve stakeholders' understanding of mutual interactions, impacts and benefits.[51] Fortunately, most of the same technologies developed to address other system vulnerabilities can improve power system security as well. But the electricity infrastructure will also require power system-specific advanced technology. Assuming individual utilities are already taking prudent steps to improve their physical security, technology can help by increasing the inherent resilience and flexibility of power systems to withstand a wide range of terrorist attacks, physical or cyber, as well as natural disasters and other unforeseen events. Greater emphasis at the state and federal level for better and innovative security is required to enable economic growth, protect national and global security while still preserving individual privacies, our values, and our way of life. The key question is: Can we build non-intrusive yet high-confidence tools, systems, processes, and laws that increase security and resilience of energy and powerinfrastructure while still preserving civil rights and liberties? Policymakers, industry leaders, and key stakeholders should heed this advice to ensure the security, defense, and resilience of these vital energy and commercial networks.

NOTES

1 S. M. Amin, "For the good of the grid," *IEEE Power and Energy Magazine*, pp. 48-59, November/December 2008.

2 J. D. Bouford and C. A. Warren, "Many states of distribution," *IEEE Power & Energy Magazine*, vol. 5, no. 4, pp. 24-32, July/August 2007.

3 Galvin Electricity Initiative. Fact Sheet: The Electric Power System is Unreliable. [Online]. http://www.galvinpower.org/resources/galvin.php?id=26 *And* "Outages," U.S. Energy Information Administration, http://www.eia.gov/todayinenergy/index.cfm?tg=%20outages.

4 Some regions do better than others. The country's most reliable utilities tend to be located in the Midwest; Minnesota, Iowa, the Dakotas, Missouri, Nebraska, and Kansas lose power on average 92 minutes per year, while customers in New York, Pennsylvania, and New Jersey suffer 214 minutes without electricity. See Galvin Electricity Initiative. The Case for Transformation. [Online]. http://www.galvinpower.org/resources/galvin.php?id=27.

5 NIST, "Smart Grid Cyber Security Strategy and Requirements," *The Smart Grid Interoperability Panel—Cyber Security Working Group*, DRAFT NISTIR 7628, February 2010. *And* Electricity Advisory Committee, "Smart Grid: Enabler of the New Energy Economy," *Electricity Advisory Committee*, 2008. *And* E. Santacana, G. Rackliffe, L. Tang, and X. Feng, "Getting smart," *IEEE Power & Energy Magazine*, vol. 8, no. 2, pp. 41-48, March/April 2010. *And* Z. Jiang et al., "A Vision of smart transmission grids," in *IEEE Power and Energy Society General Meeting*, Calgary, 2009.

6 Galvin Electricity Initiative, Fact Sheet: The Electric Power System is Unreliable. *And* Electric Power Research Institute, "Electricity Sector Framework for the Future Volume I: Achieving the 21st Century Transformation," *Electric Power Research Institute*, Washington, DC, 2003.

7 E. Santacana, G. Rackliffe, L. Tang, and X. Feng 2010.

8 Ibid. *And* R. Davies, "Hydro One's Smart Meter Initiative Paves Way for Defining the Smart Grid of the Future," in *IEEE Power and Energy Society General Meeting*, Calgary, 2009. *And* E. Camponogara, D. Jia, B. Krogh, and S. Talukdar, "Distributed Model Predictive Control," *IEEE Control Systems Magazine*, vol. 22, no. 1, pp. 44-52, February 2002. *And* D. Shirmohammadi and H. W. Hong, "Reconfiguration of electric distribution networks for resistive live losses reduction," *IEEE Transactions on Power Delivery*, vol. 4, no. 2, pp. 1492-1498, April 1989.

9 S. M. Amin, "Security challenges for the electricity infrastructure," *Supplement to Computer*, vol. 35, no. 4, pp. 8-10, April 2002.

10 C.-W. Ten, M. Govindarasu, and C.-C. Liu, "Cybersecurity for electric power control and automation systems," in *IEEE International Conference on Systems, Man and Cybernetics*, Montreal, 2007, pp. 29-34. *And* D. S. Bassett, K. N. Clinard, J. J. Grainger, S. L. Purucker, and D. J. Ward, "Distribution Automation and the Utility System," in *Distribution Automation*. Piscataway, United States of America: IEEE, 1988, ch. 1, pp. 1-6.

11 Defense Science Board (DSB), "Report of the Defense Science Board Task Force on DoD Energy Strategy," *Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics*, Washington, D.C., February 2008.

12 Ibid.

13 Stephen McLaughlin et al., "A Trusted Safety Verifier for Process Controller Code," *NDSS Symposium 2014*, February 2014, pp. 1-3.

14 R. Schainker, J. Douglas, and T. Kropp, "Electric utility responses to grid security issues," *IEEE Power and Energy Magazine*, vol. 4, no. 2, pp. 30-37, March/April 2006.

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

16 Terrorism and the Electric Power Delivery System, declassified on 1 November 2012 (post hurricane Sandy), 146 pp., *NRC press*, particularly chapter 4 on "Vulnerabilities of Systems for Sensing, Communication, and Control," 14 November 2012. *And* J. Salmeron, K. Wood, and R. Baldick, "Analysis of electric grid security under terrorist threat," *IEEE Transactions on Power Systems*, vol. 19, no. 2, pp. 905-912, May 2004.

17 R. Schainker, J. Douglas, and T. Kropp 2006.

18 J. Clemente 2009.

19 R. Schainker, J. Douglas, and T. Kropp 2006.

20 J. Clemente 2009.

21 S. M. Amin, "Securing the electricity grid," *The Bridge*, vol. 40, no. 1, Spring 2010.

22 F. T. Sheldon, S. G. Batsell, S. J. Prowell, and M. A. Langston, "Position Statement: Methodology to Support Dependable Survivable Cyber-Secure Infrastructures," in *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*, 2005, p. 310a.

23 "Smart Grid Policy," Federal Energy Regulatory Commission, *Policy Statement Docket No. PL09-4-000*, July 2009. [Online]. http://www.ferc.gov/whats-new/comm-meet/2009/071609/E-3.pdf.

24 J. E. Dagle, "Cyber Security of the Electric Power Grid," in *IEEE/PES Power Systems Conference and Exposition*, Seattle, 2009, pp. 1-2. *And* I. Winkler, "Opinion: The hackability of the smart grid," *Computerworld*, December 2009.

25 S. M. Amin 2010. And S. M. Amin, "Scoping Study and Survey of Electric Utility Industry Chief Information Officers (CIOs): Trends, challenges, opportunities, and plans regarding future Information Technology Needs for the Electric Power Industry," *Electric Power Research Institute*, White Paper 2007.

26 T. Kropp, "System threats and vulnerabilities," *IEEE Power & Energy Magazine*, vol. 4, no. 2, pp.

46-50, March/April 2006.

27 C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Transactions on Power Systems*, vol. 23, no. 4, pp. 1836-1846, November 2008.

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

29 T. Kropp 2006.

30 D. Watts, "Security & vulnerability in electric power systems," in *35th North American Power Symposium*, Rolla, 2003, pp. 559-566.

31 For more research in this area, see Trustworthy Cyber Infrastructure for the Power Grid (TCIPG), "Publications," https://tcipg.org/publications.

32 J. Salmeron, K. Wood, and R. Baldick 2004.

33 S. Jazebi, S. H. Hosseinian, M. Pooyan, and B. Vahidi, "Performance comparison of GA and DEA in solving distribution system reconfiguration problem," in *11th International Conference on Optimization of Electrical and Electronic Equipment*, Brasov, 2008, pp. 185-190. *And* A. Ahuja, S. Das, and A. Pahwa, "An AIS-ACO hybrid approach for multi-objective distribution system reconfiguration," *IEEE Transactions on Power Systems*, vol. 22, no. 3, pp. 1101-1111, August 2007. *And* S. P. Karthikeyan, V. S. Verma, D. C. Agrawal, R. I. Jacob, and D. P. Kothari, "Assessment of distribution system feeder and its reconfiguration using fuzzy adaptive evolutionary computing," in *Annual IEEE India Conference*, Kanpur, 2008, pp. 240-245. *And* R. E. Brown, "Distribution reliability assessment and reconfiguration optimization," in *IEEE/PES Transmission and Distribution Conference and Exposition*, Atlanta, 2001, pp. 994-999 vol.2. *And* W. H. Kersting, "Radial distribution test feeders," in *IEEE Power Engineering Society Winter Meeting*, Columbus, 2001, pp. 908-912 vol. 2.

34 K. Miller, "Layered security provides superior protection for plant control systems," *Oil & Gas Journal*, October 2005. *And* NIST 2010.

35 P. Helman, G. Liepins, and W. Richards, "Foundations of Intrusion Detection," in *Computer Secuirty Foundations Workshop V*, Franconia, 1992, pp. 114-120. *And* N. Ye, Y. Zhang, and C. M. Borror, "Robustness of the Markov-Chain Model for Cyber-Attack Detection," *IEEE Transactions on Reliability*, vol. 53, no. 1, pp. 116-123, March 2004. *And* M. Shouman, A. Salah, and H. M. Faheem, "Surviving cyber warfare with a hybrid multiagent-based intrusion prevention system," *IEEE Potentials*, vol. 29, no. 1, pp. 32-40, January/February 2010.

36 J. E. Dagle 2009.

37 M. Takano, "Sustainable cyber security for utility facilities control system based on defense-in-depth concept," in *SICE Annual Conference*, Kagawa University, 2007, pp. 2910-2913.

38 M. A. McQueen and W. F. Boyer, "Deception used for cyber defense of control systems," in *2nd Conference on Human System Interactions*, Catania, 2009, pp. 624-631.

39 Ibid.

40 "Advanced Metering Infrastructure and Customer Systems," U.S. Department of Energy: https://www.smartgrid.gov/recovery_act/deployment_status/sdgp_ami_systems.html. And G. Deconinck, "An evaluation of two-way communication means for advanced metering in Flanders (Belgium)," in *IEEE Instrumentation and Measurement Technology Conference Proceedings*, Victoria, 2008, pp. 900-905..

41 F. Cleveland, "Cyber Security Issues for Advanced Metering Infrastructure," in *IEEE T&D Conference*, April 2008, pp. 1-5.

42 S. M. Amin 2007. *And* Defense Science Board 2008.

43 F. Cleveland 2008 And S. T. Mak, "A Synergistic approach to implement demand response, asset management and service reliability using smart metering, AMI and MDM systems," in *IEEE Power and Energy Society General Meeting*, Calgary, 2009.

44 Ibid.

45 P. McDaniel and S. McLaughlin 2009. And J. Cline, "Opinion: will the smart grid protect consumer privacy?," *Computerworld*, November 2009.

46 U.S. President's Quadrennial Energy Review (QER) report, IEEE report to the U.S. Department of Energy and the White House for the nation's first-ever Quadrennial Energy Review (online http://www.ieee-pes.org/component/content/article/158-uncategorised/749-qer), particulaly pages 50-66 on "Asset Management and Security," August 2014. *And* "IEEE Joint Task Force on Quadrennial Energy Report (QER) Submits Final Report to the U.S. Department of Energy," *IEEE Smart Grid News*, October 6, 2014, http://smartgrid.ieee.org/resources/smart-grid-news/1164-ieee-joint-task-force-on-quadrennial-energy-review-qer-submits-final-report-to-the-u-s-department-of-energy.

47 J. D. Bouford and C. A. Warren 2007. *And* FERC 2009.

48 G. N. Ericsson, "Information security for electric power utilities (EPUs)-CIGRE developments on frameworks, risk assessment, and technology," *IEEE Transactions on Power Delivery*, vol. 24, no. 3, pp. 1174-1181, July 2009. *And* T. Sommestad, M. Ekstedt, and P. Johnson, "Cyber security risks assessment with Bayesian Defense graphs and architectural models," in *42nd Hawaii International Conference on System Sciences*, 2009, pp. 1-20.

49 C. G. Rieger, D. I. Gertman, and M. A. McQueen, "Resilient control systems: next generation design research," in *2nd Conference on Human System Interactions*, Catania, 2009, pp. 632-636. And I. Kotenko, "Multi-agent modelling and simulation of cyber-attacks and cyber-defense for homeland

security," in *IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*, Dortmund, 2007, pp. 614-619.

50 A. M. Giacomoni, S. M. Amin, and B. F. Wollenberg, "A control and communications model for a secure and reconfigurable distribution system," in *1st IEEE International Conference on Smart Grid Communications*, Gaithersburg, 2010 (submitted for publication). *And* W. A. Johnson, "A Utility program for enterprise security response," in *IEEE PES WPM*, Columbus, 2001.

51 NRC press 2012. *And* QER 2014.