The threat of terrorism and other attacks raises profound dilemmas for the electric power industry.

Securing the Electricity Grid

S. Massoud Amin holds the Honeywell/H.W. Sweatt Chair in Technological Leadership, directs the Technological Leadership Institute (TLI), and is a University Distinguished Teaching Professor and professor of electrical and computer engineering at the University of Minnesota.

S. Massoud Amin

In the aftermath of the tragic events of 9/11, I became responsible for research and development (R&D) on infrastructure security at the Electric Power Research Institute (EPRI). At first, I was faced with many reports and files claiming either that "we were bullet proof" or that "the sky was falling." It turned out that neither extreme was true of the entire electric-power sector.

The truth depends on the specific preparedness and security measures at each organization for assessing threats and addressing vulnerabilities of the cyber-physical infrastructure. No doubt, however, the existing power-delivery system is vulnerable to natural disasters and to intentional attacks. A successful terrorist attempt to disrupt the power-delivery system could seriously impact national security, the economy, and the life of every American.

The importance and difficulty of protecting power systems 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*. One of the conclusions was: "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 OTA report also documented the potential cost of widespread outages. Estimates ranged from $1/kilowatt hour (kWh) to $5/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 outage of 1977, for example, damage from looting and arson alone totaled about $155 million—roughly half of the total cost (OTA, 1990).

In the 20 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, has become impractical. In addition, the cyber, communication, and control layers that have been added have created new challenges. The focus of this article is on cyber security.

The spectrum of cyber threats continues to evolve.

Recent media reports, in April 2009, for example, highlighted penetrations of the U.S. electricity system by hackers. In November 2009, *60 Minutes* aired a piece confirming rumors of break-ins to the Brazilian energy system in 2005 and 2007. The Nuclear Regulatory Commission confirmed that in January 2003, the Microsoft SQL Server worm known as "Slammer" infected a private computer network at the Davis-Besse nuclear power plant in Oak Harbor, Ohio, and disabled a safety monitoring system for nearly five hours. Fortunately the plant was off-line at the time. In January 2008, the Central Intelligence Agency reported knowledge of four disruptions, or threatened disruptions, by hackers of the power supplies for four cities.

At the Electric Power Research Institute (EPRI),[1] we had been working since 1999 on the modes of penetration and manipulation through intrusion that had been used in the cyber attacks in Brazil. We launched an Infrastructure Security Initiative (ISI), a two-year program funded by the electric power industry, to develop and apply key technologies that could improve overall system security in the face of such threats (EPRI, 2000a, b; 2001; 2002; 2003; 2004; 2005).

Before and after 9/11, utilities members of EPRI-related initiatives, including the ISI, Y2K, and Enterprise Information Security (EIS) programs, put into place extensive information-sharing and vendor action groups so that the results would reach everyone "with a need to know" in the utilities community. We conducted "red-team" studies of cyber attacks on multiple assets (including power plants, transmission and distribution systems, control centers, and communication systems). The focus of these exercises was on responses to attacks (threat and vulnerability assessment, R&D on prevention, mitigation, and restoration) and technology development (secure communication systems, including protocols for communications between control centers, substations, and power plants, and cyber security technologies specifically for control systems). Risk-management frameworks, vulnerability-reduction tools, information-sharing programs, and vendor action groups were also important.

Fortunately, although we found that parts of the system were extremely vulnerable, we were able to put in place several simple programs to raise awareness of security issues and establish cyber-security programs and remedies. We worked with the industry and related organizations (e.g., Edison Electric Institute and the North American Electric Reliability Corporation) to gain the cooperation and compliance of other stakeholders (EPRI, 2001, 2002, 2003, 2004). Yet the spectrum of cyber threats continues to evolve, and much remains to be done.

Interdependencies in Electricity Infrastructure

Secure, reliable operation of the electricity system is fundamental to national and international economies, security, and quality of life; and their interconnectedness makes them increasingly vulnerable to regional and global disruptions initiated locally by material failure, natural calamities, intentional attacks, or human error.

The North American power network, which underpins our economy and quality of life, connects nearly 215,000 miles of transmission lines with all of the electric generation and distribution facilities on the continent; it may be the largest, most complex "machine" in the world. Utilities typically own and operate at least parts of their own telecommunications systems, which often consist of backbone fiber-optic or microwave connections with major substations and spurs to connect to smaller sites. The increasing use of electronic automation raises significant issues for operational security in systems where security provisions have not been built in as design criteria.

[1] A nonprofit energy research consortium organized for the benefit of utility members, their customers, and society at large.

The security of cyber and communication networks is essential for the reliable operation of the grid. The more heavily power systems rely on computerized communications and control, the more dependent system security becomes on protecting the integrity of associated information systems. Unfortunately, existing control systems, which were originally designed for use with proprietary, stand-alone communication networks, were indirectly connected to the Internet without added technologies to ensure their security.

Consider the following "sanitized" conversation showing the lack of awareness of inadvertent connection to the Internet for a power plant (200–250MW, gas-fired turbine, combined cycle, five years old, two operators, and typical multi-screen layout).

A: Do you worry about cyber threats?

Operator: No, we are completely disconnected from the net.

A: That's great! This is a peaking unit, how do you know how much power to make?

Operator: The office receives an order from the ISO, then sends it over to us. We get the message here on this screen.

A: Is that message coming in over the Internet?

Operator: Yes, we can see all the ISO to company traffic. Oh, that's not good, is it?

In addition, as the number of documented attacks and intrusions and their level of sophistication continue to rise (Albert, 2004; Amin, 2002a,b; 2005, 2010; Clemente, 2009; DOE, 2002; EPRI, 2000a,b, 2001, 2002, 2003, 2004; Kropp, 2006; Sandia National Laboratory, 2003; Ten, 2008), human response has become inadequate for countering malicious code or denial-of-service attacks or other recent intrusions (Cleveland, 2008; Ericsson, 2009; EPRI, 2000, 2001, 2002; Schainker et al., 2006). Any telecommunication link that is even partly outside the control of the organization that owns and operates power plants, supervisory control and data acquisition (SCADA) systems, or energy management systems represents a potential pathway into the business operations of the company and a threat to the larger transmission grid.

Interdependency analyses done by most companies in the last 14 years (e.g., in preparation for Y2K and after the events of 9/11) have identified these pathways and the system's vulnerability to their failures. Thus these analyses provide an excellent reference point for a cyber-vulnerability analysis (Amin 2000a,b; 2003, 2005a,b,c; 2007; Darby, 2006; DOE, 2002; EPRI, 2000a, b; 2001, 2002; Ericsson, 2009).

Like all complex, dynamic infrastructure systems, the electric power grid has many layers and is vulnerable to many different types of disturbances. Strong centralized control, which is essential for reliable operations, requires multiple, high-data-rate, two-way communication links, a powerful central computing facility, and an elaborate operation-control center, all of which are vulnerable, especially when they are needed most—during serious system stresses or power disruptions. For greater protection, systems also need intelligent, distributed, secure control that enables parts of the network to remain operational, and even to automatically reconfigure, in the event of local failures or threats of failure.

The specter of future sophisticated terrorist attacks raises a profound dilemma for the electric power industry, which must make the electricity infrastructure more secure, but must also be careful not to compromise productivity. Resolving this dilemma will require both short-term and long-term technology development and deployment that will affect fundamental power system characteristics.

The security of cyber and communication networks is essential to the reliable operation of the grid.

Centralization and Decentralization of Control

For several years, there has been a trend toward centralizing control of electric power systems. The emergence of regional transmission organizations, for example, promises to greatly increase efficiency and improve customer service. But we also know that terrorists can exploit the weaknesses of centralized control. Therefore, smaller, local systems would seem to be the system configuration of choice. 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.

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. We will need new mathematical approaches to simplify the operation of complex power systems and make them more robust in the face of natural or manmade 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. However, because of 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.

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 the greatest advantage.

Despite increasing automation, human operators ultimately make the decisions that control operations.

Fortunately, the same core technologies that were developed to address the vulnerabilities of other systems can also strategically improve electrical system security. These technologies were developed for open access, exponential growth in power transactions and to ensure the reliability necessary for an increasingly digital society.

However, the electricity infrastructure will also require power-system-specific advanced technology. Assuming that 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 terrorist attacks, as well as natural disasters.

As part of our ongoing research at the University of Minnesota, we are designing and assessing control architectures that will enable the power grid to respond quickly to natural and intentional attacks on its cyber-physical infrastructure. We are developing models using various software packages to simulate their effects on system operations. Control architectures are evaluated by simulations and testing on a microgrid, combined with a cost-benefit analysis of options, designs, and policies.

In 2008, we launched a new interdisciplinary Master of Science in Security Technologies (MSST) Program that draws on systems risk analysis, engineering, emerging technologies, economics, human factors, law, food and bio-safety, and public health and policy to teach and investigate security technologies to meet growing demand in government and industry.

The electric power grid includes the entire apparatus of wires and machines that connects the sources of electricity, power plants, and customers. The operation of a modern power system depends on complex systems of sensors and automated and manual controls, all of which are linked through communication systems. Therefore, compromising the operation of sensors or communication and control systems by spoofing, jamming, or sending improper commands could disrupt the entire system, cause blackouts, and in some cases result in physical damage to key system components. That is why the increasing frequency of hacking and cyber attacks is of great concern.

Many elements of the distributed control systems used in power systems are also used in process control in manufacturing, chemical process controls and refineries, transportation, and other critical infrastructure sectors, which are vulnerable to similar modes of attack. Dozens of communication and cyber security intrusions and penetration red-team attacks have revealed a variety of cyber vulnerabilities, such as unauthorized access, penetration, or hijacking of control.

Despite increasing automation, human operators in system control centers ultimately make decisions and take actions to control operations. Thus, in addition to physical threats and threats to the communication links that flow in and out of control centers, we must also

ensure (1) the reliability of operators of control centers and (2) that insecure code has not been added to a program in a control center computer.

Since humans interact with the infrastructure as managers, operators, and users, human performance plays an important role in their efficiency and security. In many complex networks, the human participants themselves are both the most susceptible to failure and the most adaptable in the management of recovery. Modeling and simulating these networks, especially their dynamic security, will require modeling the "insider threat" and the bounded rationality of actual human thinking.

Threats from "insiders," as well as the risk of a "Trojan horse" embedded in the software of one of more control center computers, can only be addressed by careful security measures on the part of commercial firms that develop and supply software, embedded chips, and devices, and by security screening of utility and outside service personnel who perform software and hardware maintenance.

Another problem today is that security patches are sometimes not supplied to end-users, or they are supplied but are not applied for fear of impacting system performance. Current practice is to apply an upgrade/patch only after SCADA vendors have thoroughly tested and validated it, which can sometimes take several months.

It is important to remember that the key elements and principles of operation for interconnected power systems were established in the 1960s prior to the emergence of extensive computer and communication networks. Even though computation is heavily used in all levels of the power network today (e.g., for planning and optimization, local control of equipment, processing of field data), coordination across the network happens at a slower pace. Some coordination is under computer control, but much of it is still based on telephone calls between system operators at utility control centers—even or especially!—during emergencies.

Responses to System Failures

If a large electric network is threatened with a cascading, widespread failure, it is highly desirable that it break into self-sustaining "islands" that can balance generation with demand. With distributed intelligence and components acting as independent agents, each island has the ability to reorganize itself and make efficient use of its remaining local resources to minimize adverse impacts on the overall network and allow some areas to maintain service.

Local controllers guide their islands to operate independently while preparing them to rejoin the network, without creating unacceptable local conditions either during or after the restoration. A network of local controllers acting as a parallel, distributed computer and communicating via microwaves, optical cables, or the power lines per se, can limit messages to information necessary to achieving global optimization and facilitating recovery after a failure.

On any given day, 500,000 customers in the United States are without power for at least two hours.

Advanced technology now under development or under consideration could meet the electricity needs of a robust digital economy. An architecture for this new technology framework is evolving through early research on concepts and enabling platforms to provide an integrated, self-healing, electronically controlled electricity supply system that is extremely resilient and capable of responding in real time to the billions of decisions made by consumers and their increasingly sophisticated agents. We could potentially create an electricity system with the same efficiency, precision, and interconnectivity as the billions of microprocessors it will power.

Long-Term Research

The goals of our long-term research are to further our understanding of adaptive, self-healing, self-organizing mechanisms that can be applied to the development of secure, resilient, robust overlaid/integrated energy, power, sensing, communication, and control networks. Recent advances have been made in complex dynamic systems; bio-inspired defense systems; adaptive and layered security systems; the design of self-healing networks; self/non-self recognition; immunology models; trade-offs between optimization and robustness; dynamic risk assessment; and the stability of large-scale complex networks.

Costs and Benefits of a Secure Electricity Infrastructure

The serious technological challenge facing us is to enable secure, very high-confidence sensing, communication, and control of a heterogeneous, widely dispersed, globally interconnected system. The problem is even more complex than it appears, because we also have to ensure optimal efficiency and maximum benefit to consumers without infringing on the rights of all business components to compete fairly and freely.

In the past 25 years, grid congestion and atypical power flows have been increasing, even as customer expectations of reliability and cyber-physical security have been rising. A major outage (i.e., an outage that affects 7 million customers or more) occurs about once every decade and costs more than $2 billion. Smaller disturbances, which are commonplace, have very high costs for customers and for society as a whole. On any given day, 500,000 customers are without power for two hours or more in the United States. Annual losses to the U.S. economy from power outages and disturbances total $75 billion to $180 billion (Amin and Schewe, 2007).

Compare that to the cost of the programs described above, about $170 million to $200 million per year for R&D and about $400 million per year for more than a decade of fielding, testing, and integrating new technology into the system, with savings of 5- to 7-fold in the prevention and mitigation of disturbances (Amin and Schewe, 2007).

Several reports and studies have estimated that a sustained annual investment of $10 billion to $13 billion will be required for existing technologies to evolve and for innovative technologies to be realized (e.g., NRC, 2009). However, the current level of R&D funding in the electric industry is at an all-time low. In fact, investment rates for the electricity sector are the lowest of any major industrial sector, with the exception of the pulp and paper industry. The electricity sector invests, at most, a few tenths of 1 percent of sales in R&D (0.3 percent of revenues for 1995–2000 and 0.17 percent for 2001–2006), whereas the electronics and pharmaceutical sectors invest 8 to 12 percent of net sales in R&D (Amin and Schewe, 2007).

Even though all industry sectors depend on reliable electricity, our energy systems are clearly underfunded. For utilities, funding and sustaining innovations, such as the smart, self-healing grid, remain a challenge because they must satisfy many competing demands on precious resources while trying to be responsive to their stakeholders, who tend to limit R&D investments to those with immediate applications and short-term financial returns. Investor-owned utilities are also under pressure from Wall Street to increase dividends. In truth, they have little incentive to invest in the longer term.

A balanced, cost-effective approach to investments and to the use of technology could substantially mitigate the risk of investing in R&D. Electricity shall prevail at the level of quality, efficiency, and reliability that customers demand and are willing to pay for. On the one hand, the question is who provides the electricity. On the other hand, achieving grid performance, security, and reliability should not be considered a cost burden to taxpayers but a profitable national investment, because the payback will be three to seven times the money invested, and it will begin with the completion of the first sequence of grid improvements (EPRI, 2005).

The question is not who invests money, because that will ultimately be the public. The question is whether the money will be invested through taxes or raised through consumer payments for electricity usage. Considering the importance and "clout" of regulatory agencies, they should be able to induce electricity producers to plan and fund the process. In my view, this may be the most efficient way to get us moving on the grid.

The absence of a coordinated national decision-making body is a major obstacle. States' rights and state regulators of publicly owned utilities have removed the incentive for supporting a national plan. Thus investor-owned utilities will face either collaboration on a national level or the forced nationalization of the industry.

Given the economic, social, and quality-of-life issues and increasing interdependencies among infrastructures, the key question before us is whether the electricity infrastructure will evolve to become the primary support for the 21st century digital society—a smart grid with self-healing capabilities—or will be left behind as a 20th century industrial relic!

Conclusions

Cyber systems are the "weakest link" in the electricity system. Although vulnerability to attacks has been reduced, much remains to be done. Technology and threats are both evolving quickly, which adds complexity to the current cyber-physical system; in addition, there is often a lack of training and awareness by organizations

(e.g., forgetting/ignoring the human factor in the equation). Installing modern communications and control equipment (elements of the smart grid) can help, but security must be designed into the system from the start, not glued on as an afterthought.

Acknowledgments

Support from the National Science Foundation and Electric Power Research Institute for research by Ph.D. students is gratefully acknowledged.

References

Albert, R., I. Albert, and G. Nakarado. 2004. "Structural Vulnerability of the North American Power Grid," Physical Review E, 69, 023103(R).

Amin, M. 2002a. Security Challenges for the Electricity Infrastructure. Special issue of the IEEE Computer Magazine on Security and Privacy, April.

Amin, M. 2002b. Special issues of IEEE Control Systems Magazine on Control of Complex Networks 21(6) and 22(1).

Amin, M. 2003. North American electricity infrastructure: are we ready for more perfect storms? IEEE Security and Privacy 1(5): 19–25.

Amin, M. 2005a. Powering the 21st century: we can—and must—modernize the grid. IEEE Power and Energy Magazine (March/April): 93–95.

Amin, M. (guest editor). 2005b. Special issue of IEEE Security & Privacy Magazine on Infrastructure Security 3(3).

Amin, M. (guest editor). 2005c. Special Issue of Proceedings of the IEEE on Energy Infrastructure Defense Systems 93(5): 855–1059.

Amin, M. 2007. Electricity Infrastructure Security. Pp. 9-41 to 9-57 in CRC Handbook of Energy Conservation and Renewable Energy, edited by Y.D. Goswami and F. Kreith. New York: CRC Press.

Amin, M. 2010a. Countermeasures: Robustness, Resilience, and Security. In Wiley Handbook of Science and Technology for Homeland Security. New York: Wiley and Sons. Forthcoming.

Amin, M. 2010b. Self-healing, Resilient, Robust and Smart Infrastructure Systems. In Handbook of Science and Technology for Homeland Security. New York: Wiley and Sons. Forthcoming.

Amin, M., and P. Schewe. 2007. Preventing blackouts. Scientific American (May): 60–67.

Clemente, J. 2009. The security vulnerabilities of smart grid. Journal of Energy Security (June): 3.

Cleveland, F. 2008. Cyber Security Issues for Advanced Metering Infrastructure. Pp. 1–5 in IEEE T&D Conference, April 2008.

Darby J., J. Phelan, P. Sholander, B. Smith, A. Walter, and G. Wyss. 2006. Evidence-Based Techniques for Evaluating Cyber Protection Systems for Critical Infrastructure. Pp. 1–10 in IEEE Military Communications Conference. DOI 10.1109/MILCOM.2006.302504. New York: IEEE.

DOE (Department of Energy). 2002. Vulnerability Assessment Methodology: Electric Power Infrastructure. September. Available online at *http://www.esisac.com/publicdocs/assessment_methods/VA.pdf*.

EPRI (Electric Power Research Institute). 2000a. Communication Security Assessment for the United States Electric Utility Infrastructure. Palo Alto, Calif.: EPRI.

EPRI. 2000b. Information Security Primer for the Power Industry. Palo Alto, Calif.: EPRI.

EPRI. 2001. Electricity Infrastructure Security Assessment, Vol. I-II. Palo Alto, Calif.: EPRI.

EPRI. 2002. Security Vulnerability Self-Assessment Guidelines for the Electric Power Industry. Palo Alto, Calif.: EPRI.

EPRI. 2003. Infrastructure Security Initiative (ISI): Promoting Security for the Electric Power Grid. Palo Alto, Calif.: EPRI.

EPRI. 2004. Complex Interactive Networks/Systems Initiative (CIN/SI): Final Summary Report. Overview and Summary Final Report for Joint EPRI/U.S. Department of Defense University Research Initiative, 155 pp. Palo Alto, Calif.: EPRI.

EPRI. 2005. Strategic Insights into Security, Quality, Reliability, and Availability. EPRI Report 1008566, 128 pp. Palo Alto, Calif.: EPRI.

Ericsson, G.N. 2009. Information security for electric power utilities (EPUs)-CIGRE developments on frameworks, risk assessment, and technology. IEEE Transactions on Power Delivery 24(3): 1174–1181.

Kropp, T. 2006. System threats and vulnerabilities. IEEE Power & Energy Magazine 4(2): 46–50.

NRC (National Research Council). 2009. America's Energy Future: Technology and Transformation. Washington, D.C.: National Academies Press.

OTA (Office of Technology Assessment). 1990. Physical Vulnerability of the Electric System to Natural Disasters and Sabotage. OTA-E-453. Washington, D.C.: U.S. Government Printing Office.

Sandia National Laboratory. 2003. Common Vulnerabilities in Critical Infrastructure Control Systems. Albuquerque, N.M.: Sandia National Laboratory.

Schainker, R., J. Douglas, and T. Kropp. 2006. Electric utility

responses to grid security issues. IEEE Power and Energy Magazine 4(2): 30–37.

Ten, C.-W., C.-C. Liu, and G. Manimaran. 2008. Vulnerability assessment of cybersecurity for SCADA systems. IEEE Transactions on Power Systems 23(4): 1836–1846.

Additional Readings

Amin, M. 2000. National Infrastructures as Complex Interactive Networks. Pp. 263–286 in Automation, Control, and Complexity: An Integrated Approach, edited by T. Samad and J. Weyrauch. New York: John Wiley and Sons Ltd.

Amin, M. 2008. For the good of the grid: toward increased efficiencies and integration of renewable resources for future electric power networks. IEEE Power & Energy 6(6): 48–59.

Deconinck, G. 2008. An Evaluation of Two-Way Communication Means for Advanced Metering in Flanders (Belgium). Pp. 900–905 in IEEE International Instrumentation and Measurement Technology Conference Proceedings, Victoria, Canada, May 12–15, 2008. New York: IEEE.

Defense Science Board. 2008. Report of the Defense Science Board Task Force on DOD Energy Strategy: "More Fight—Less Fuel." Available online at *http://www.acq.osd.mil/dsb/reports/ADA477619.pdf*.

FERC (Federal Energy Regulatory Commission). 2009. Smart Grid Policy. Federal Energy Regulatory Commission, Policy Statement Docket No. PL09-4-000, July 2009. Available online at *http://www.ferc.gov/whats-new/comm-meet/2009/071609/E-3.pdf*.

GAO (U.S. Government Accountability Office). 2004. Critical Infrastructure Protection Challenges and Efforts to Secure Control Systems. Washington, D.C.: GAO.

Helman, P., G. Liepins, and W. Richards. 1992. Foundations of Intrusion Detection. Pp. 114–120 in Computer Security Foundations Workshop V, Franconia, New Hampshire, June 16–19, 1992. New York: IEEE.

Kotenko, I.V. 2007. Multi-agent modelling and simulation of cyber-attacks and cyber-defense for homeland security. Pp. 614–619 in IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Dortmund, Germany. New York: IEEE.

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

NIST (National Institute of Standards and Technology). 2010. Smart Grid Cyber Security Strategy and Requirements, The Smart Grid Interoperability Panel–Cyber Security Working Group, DRAFT NISTIR 7628, February 2010. Available online at *http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/NISTIR7628Feb2010/draft-nistir-7628_2nd-public-draft.pdf*.

Sommestad, T., M. Ekstedt, and P. Johnson. 2009. Cyber Security Risks Assessment with Bayesian Defense Graphs and Architectural Models. Pp. 1–20 in 42nd Hawaii International Conference on System Sciences. New York: IEEE.

Ten, C.-W., M. Govindarasu, and C.-C. Liu. 2007. Cybersecurity for Electric Power Control and Automation Systems. Pp. 29–34 in IEEE International Conference on Systems, Man and Cybernetics, Montreal, 2007. New York: IEEE.

Ye, N., Y. Zhang, and C.M. Borror. 2004. Robustness of the Markov-chain model for cyber-attack detection. IEEE Transactions on Reliability 53(1): 116–123.