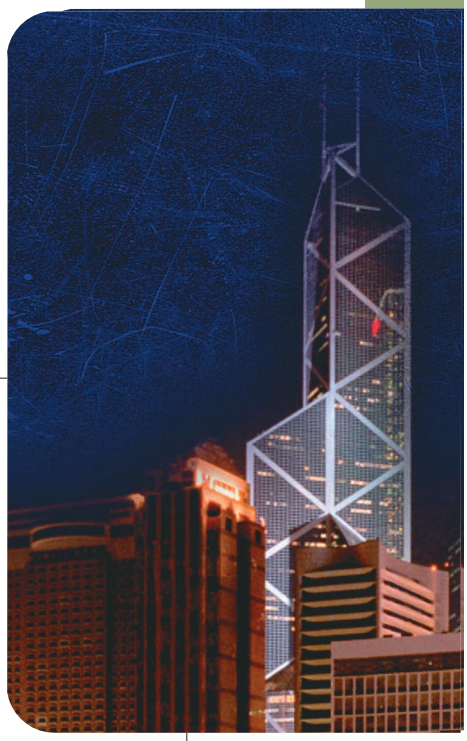
North America's Electricity Infrastructure:

Are we ready for more perfect storms?



Massoud Amin
University of Minnesota

With the tragic events of 9/11 permanently etched in our minds, the massive 14 August power outage evoked eerie reminders of what shook our world 2 years ago. While preliminary reports indicate that there was no apparent evidence of terrorism, the cascading blackouts were a sudden illumination of our electricity infrastructure's vulnerable condition. This infrastructure affects us all—are we prepared for future storms?

Our massive power network

The North American power network represents an enormous investment, including more than 15,000 generators in 10,000 power plants, and hundreds of thousands of miles of transmission lines and distribution networks. Analysts estimate it to be worth over US$800 billion. In 2000, they valued the transmission and distribution at US$358 billion.[1]

With its millions of relays, controls, and other components, our power network is the most complex machine ever invented. The National Academy of Engineering hailed the North American power-delivery system as the supreme engineering achievement of the 20th century because of its ingenious engineering, catalytic role for other technologies, and impact on improving quality of life down to the household level.[1] Possibly the largest machine in the world, its transmission lines connect all generation and distribution on the continent to form a vertically integrated hierarchical network consisting of the generation layer (as just mentioned), and the following three basic levels:[2]

- *Transmission*. Meshed networks combining extra-high voltage (above 300 kV) and high voltage (100-300 kV), connected to large generation units and very large customers and, via tie-lines, to neighboring transmission networks and to the sub-transmission level.
- *Sub-transmission*. A radial or weakly coupled network including some high voltage (100-300 kV) but typically 5-15 kV, connected to large customers and medium-size generators.
- *Distribution*. Typically a tree network including low voltage (110-115 or 220-240 V) and medium voltage (1-100 kV), connected to small generators, medium-size customers, and local low-voltage networks for small customers.

Unfortunately, over the past 100 years, the network has evolved without formal analysis of the system-wide implications of this evolution, including its diminished transmission and generation shock-absorber capacity under the forces of deregulation, the digital economy, and interaction with other infrastructures.

Only recently, with the advent of deregulation, unbundling, and competition in the electric power industry, has the possibility of power delivery beyond neighboring areas become a key design and engineering consideration, yet we still expect the existing grid to handle a growing volume and variety of long-distance, bulk-power transfers. To meet the needs of a pervasively digital world that relies on microprocessor-based devices in vehicles, homes, offices, and industrial facilities, grid congestion and atypical power flows are increasing, as are customer reliability expectations.

Reliability issues

Several cascading failures during the past 40 years spotlighted our need to understand the complex phenomena associated with power network systems and the development of emergency controls and restoration (see the "North American power-grid vulnerabilities" sidebar.). Widespread outages and huge price spikes during the past few years raised public concern about grid reliability at the national level.[3]

According to data from the North American Electric Reliability Council (NERC) and analyses

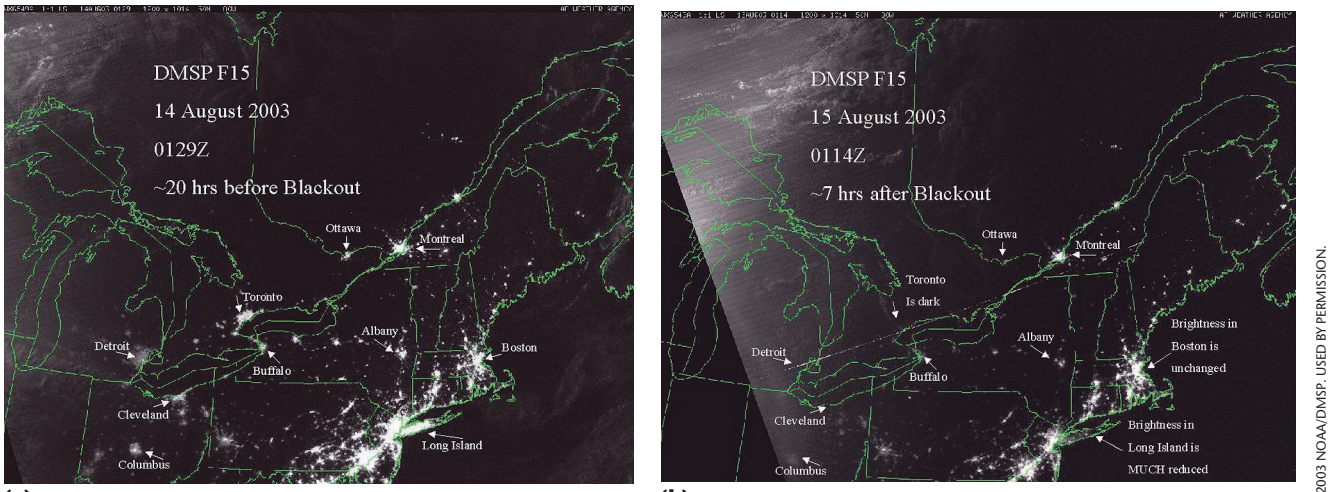


Figure 1. Cascading failures of 14 August 2003. (a) 20 hours before blackout and (b) 7 hours after.

from the Electric Power Research Institute (EPRI), average outages from 1984 to the present have affected nearly 700,000 customers annually. Smaller outages occur much more frequently and affect tens to hundreds of thousands of customers every few weeks or months, while larger outages occur every two to nine years and affect millions. Much larger outages affect seven million customers per decade. This rare event has much higher consequences. These analyses are based on data collected for the US Department of Energy (DOE), which requires electric utilities to report system emergencies that include electric service interruptions, voltage reductions, acts of sabotage, unusual occurrences that can affect the reliability of bulk power delivery systems, and fuel problems.[4-6]

Furthermore, today's electric power delivery system is

North American powergrid vulnerabilities

Attention to the grid has gradually increased after several cascading failures.

- November 1965—A cascaded system collapse blackout in 10 states in the Northeast US affected about 30 million people
- 1967—The Pennsylvania-New Jersey-Maryland (PJM) blackout occurred.
- May 1977—15,000 square miles and 1 million customers in Miami lost electricity.
- July 1978—In New York's suburbs, lightning caused over voltages and faulty protection devices, which caused 10 million people to lose power for over 24 hours, resulting in wide-spread looting, over 4,000 arrests, and ultimately, the ouster of New York City's mayor.
- December 1978—Blackout in part of France due to voltage collapse.
- January 1981—1.5 million customers in Idaho, Utah, and Wyoming were without power for 7 hours.
- March 1982—Over 900,000 lost power for 1.5 hours due to high-voltage line failure in Oregon.
- December 1994—2 million customers from Arizona to Washington state lost power.
- July 1996—A high-voltage line touched a tree branch in Idaho and fell. The resulting short circuit caused blackouts for 2 million customers in 14 states for approximately 6 hours
- August 1996—Following the 2 July blackout, two high-voltage lines fell in Oregon and caused cascading outages affecting over 7 million customers in 11 Western states and two Canadian provinces.
- January 1998—Ice storms caused over 3 million people to lose power in Canada, New York, and New England.
- December 1998—San Francisco, California Bay Area blackout.
- July 1999—New York City blackout caused 300,000 people to be without power for 19 hours.
- 1998–2001—Summer price spikes affect customers (infrastructure's inadequacy affecting markets).
- Industry-wide Y2K readiness program identified telecommunication failure as the biggest source of risk of the lights going out on rollover to 2000.
- Western states' suffered power crises in summer 2001 and its aftermath.
- Eastern United States and Canada face cascading outages on 14 August 2003.

based largely on technology developed in the 1950s or earlier, and installed over the last 30 to 50 years. The strain on this aging system is beginning to show. Figure 2 shows how system outages have affected electricity consumers. Generally, a relatively small number of US consumers experience a large number of outages; conversely, outages that affect a large number of consumers are quite rare. For example, in Figure 2, the data point in the lower right-hand corner represents the widespread outage of 10 August 1996, which affected approximately seven million consumers in 11 western US states and two Canadian provinces. However, this plot could also indicate that the number of larger outages might be rising.

Based on EPRI's analyses[6] of data in NERC's Disturbance Analysis Working Group (DAWG) database, 41 percent more outages affected 50,000 or more consumers in the second half of the 1990s than in the first half (58 versus 41). The average outage affected 15 percent more consumers from 1996 to 2000 than from 1991 to 1995 (409,854 versus 355,204).

Figure 3 presents the data in another way. It shows that 76 outages led to a loss of 100 megawatts (MW) of power or more in the second half of the decade, compared to 66 such occurrences in the first half. During the same period, the average lost load caused by an outage increased by 34 percent, from 798 MW from 1991 to 1995 to 1067 MW from 1996 to 2000.

Another dimension of the vulnerability to major blackouts is that local actions can create global effects by cascading through a power network and even into other interdependent infrastructures, making them vulnerable to failures with widespread consequences.[4,7-9] Competition and deregulation have created multiple energy producers that must share the same regulated energy distribution network, one that now lacks the carrying capacity or safety margin to support anticipated demand. Investments in maintenance and research and development continue to decline in the North American electrical grid.

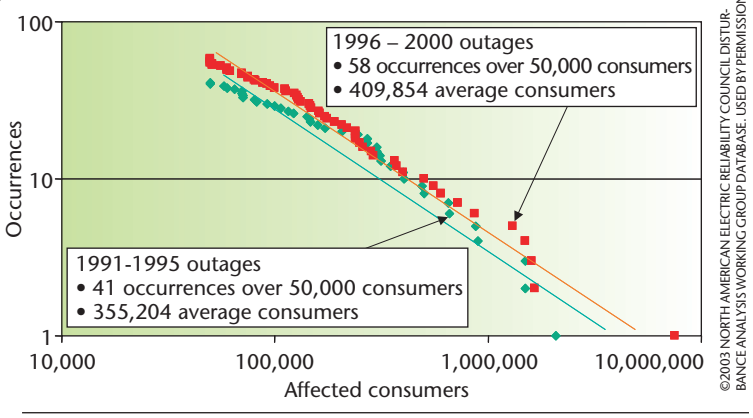


Figure 2. Number of US power outages versus the number of consumers affected (1991 to 2000). A logarithm-logarithm plot of outages and their impact on customers. The reliability goal is to move these curves down toward the origin; that is, to make outages less frequent and with smaller impact on customers.

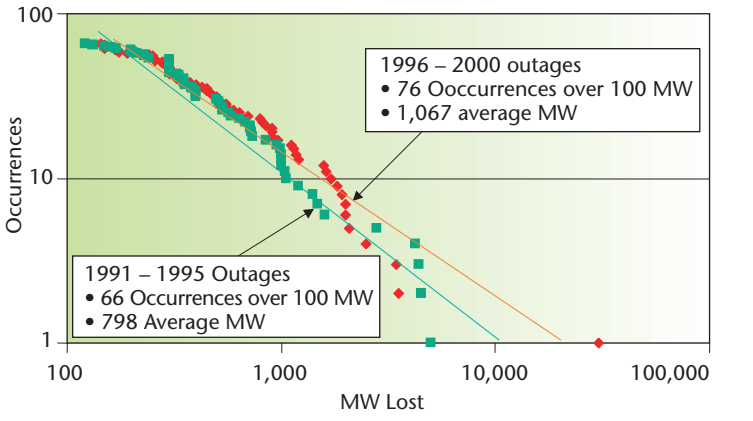


Figure 3. Number of US power outages versus the amount of electric load lost (1991 to 2000). Log-log plot of outages and their size in megawatts (MW).

A stressed infrastructure

The major outage on 14 August in the Eastern US and the earlier California power crisis in 2000 are only the most visible parts of a larger and growing US energy crisis that is the result of years of inadequate investments in the infrastructure. For example, at the root of the California crisis was declining investment in infrastructure components that led to a fundamental imbalance between growing demand for power and an almost stagnant supply. The imbalance had been brewing for many years and is prevalent throughout the nation (see EPRI's Western States Power Crises white paper; www.epri.com/WesternStatesPowerCrisisSynthesis.pdf).

From a broader view, the North American electricity infrastructure is vulnerable to increasing stresses from several sources. One stress is caused by an imbalance between growth in the demand for electric power and enhancement of the power delivery system to support this growth. From 1988 to 1998, the US's total electricity demand rose by nearly 30 percent, but its transmission network's capacity grew by only 15 percent. This disparity will likely increase from 1999 to 2009: analysts expect demand to grow by 20 percent, while planned transmission systems grow by only 3.5 percent. Along with that imbalance, today's power system has several other sources of stress.

- *Demand is outpacing infrastructure expansion and maintenance investments.* Generation and transmission capacity margins are shrinking and unable to meet peak condi-

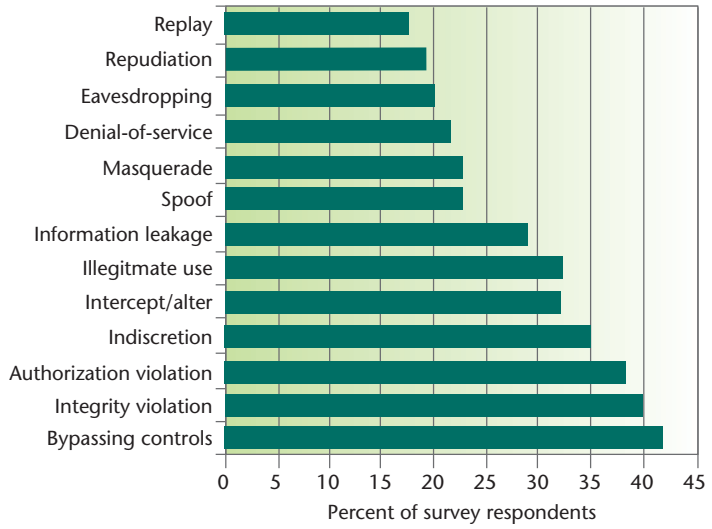


Figure 4. Perceived threats to power supply control.[12]

tions, particularly when multiple failures occur while electricity demand continues to grow.

- *The transition to deregulation is creating new demands that are not being met.* Power transactions are growing exponentially while grid capacity is severely limited. The infrastructure is not being expanded or enhanced to meet the demands of wholesale competition in the industry. As a result, connectivity between consumers and markets is at a gridlock.
- *The current power-delivery infrastructure cannot adequately handle the new demands of high-end digital customers and the 21st century economy.* It cannot support levels of security, quality, reliability, and availability needed for economic prosperity under continued stress. The existing infrastructure is vulnerable to human error, natural disasters, and intentional physical and cyber attack. It does not adequately accommodate emerging beneficial technologies, including distributed energy resources and energy storage, or facilitate enormous business opportunities in retail electricity or information services.
- *The infrastructure has not kept up with new technology*. Many distribution systems have not been updated with current technology.
- *Proliferation of distributed energy resources (DERs) but little are connected to the grid and the overall system integration and reliablility effects are to be determined*. DER includes a variety of energy sources—such as micro turbines, fuel cells, photovoltaics, and energy storage devices—with capacities ranging from approximately 1 kilowatt (kW) to 10 MW, DER can play an important role in strengthening the energy infrastructure. Currently, DER accounts for about 7 percent of total capacity in the United States, mostly in the form of backup generation, yet very little is connected to the power-delivery system. By 2020, DER could account for as much as 25 percent of total US capacity, with most of the DER devices connected to the power-delivery system.
- *Return-on-investment (ROI) uncertainties discourage investments in infrastructure upgrades.* Investing new technology in the infrastructure can meet these aforementioned demands. More specifically, according to a June 2003 report by the US National Science Foundation, research and development spending in the US as a percent of net sales was about 10 percent in the computer and electronic products industry and 12 percent for the communication equipment industry in 1999. Conversely, electric utilities' R&D investment was more than an order of magnitude lower—less than 0.5 percent during the same period. R&D investment in most other industries is also significantly greater than that in the electric power industry.[10]
- *Concern about the national infrastructure's security.*[7,11] A successful terrorist attempt to disrupt electricity supplies could have devastating effects on national security, the economy, and every citizen's life. Yet power systems have widely dispersed assets that can never be absolutely defended against a determined attack.

In addition to human error, economic effects, and power-market impacts, the existing power system is vulnerable to natural disasters and intentional attack. Regarding the latter, a November 2001 EPRI assessment developed in response to the 9/11 attacks highlights three kinds of potential threats to the US electricity infrastructure:[7,11]

- *Attacks on the power system*, in which the infrastructure itself is the primary target.
- *Attacks by power system*, in which components are used as weapons to attack the population.
- *Attacks through the power system*, in which attackers take advantage of power system networks to affect other infrastructure systems, such as telecommunications.

The dispersed nature of the power delivery system's equipment and facilities complicates the protection of the system from a determined attack. Furthermore, both physical vulnerabilities and susceptibility of power-delivery systems to disruptions in computer networks and communication systems must be considered.

Threats to the power supply

A survey of electric utilities revealed real concerns about grid and communications security. Figure 4 ranks the perceived threats to utility control centers. The most likely threats were bypassing controls, integrity violations, and authorization violations, with four in 10 com-

panies rating each as either a 5, or 4 out of 5, with a rating of 5 being the highest vulnerability. Concern about the potential threats generally increased as the size of the utility (peak load) increased.[12]

The system's equipment and facilities are dispersed throughout the North American continent, which complicates protection of the system from a determined terrorist attack. In addition, we must consider another complexity—the power-delivery systems' physical vulnerabilities and susceptibility to disruptions in computer networks and communication systems. For example, terrorists might exploit the increasingly centralized control of the power delivery system to magnify the effects of a localized attack. Because many consumers have become more dependent on electronic systems that are sensitive to power disturbances, an attack that leads to even a momentary interruption of power can be costly. A 20-minute outage at an integrated circuit fabrication plant, for example, could cost US$30 million.

Toward the future

Advanced technology will necessarily play an important role in ongoing efforts to provide enhanced security because of the electricity infrastructure's unique attributes. Fortunately, these core technologies will also resolve other system vulnerabilities.

The asset-intensive utility systems, that underpin our economy and quality of life, are tempting targets. The complex systems used to relieve bottlenecks and clear disturbances during periods of peak demand are also now at great risk of serious disruption.

Cyber attacks are very probable as intruders are becoming increasingly tech-savvy; furthermore, not all digital and communication conduits have been sealed off. Preliminary reports have raised questions linking the Blaster worm to potentially worsening the 14 August blackout's severity. While it is too soon to confidently verify root causes, several testimonies during a Congressional hearing held 3 and 4 September have pointed to potential problems with critical control, communication and IT infrastructure connected to energy management systems (EMS) as well as to supervisory control and data acquisition (SCADA) systems (see the "Additional technology and policy resources" sidebar for more).

Detailed vulnerability tests and analyses carried out by the private industry, as well as those conducted by the state and federal governments, have shown specific local and end-to-end vulnerabilities. Consequently, we know what we need to do to prevent and mitigate attack but much more remains to be done. As a nation, our tactical response is adequate, but strategic response is lacking. We need a supportive public-policy umbrella because the public doesn't appreciate the latent threat to the power system.

Additional technology and policy resources

Several pertinent strategic plans and roadmapping activities for electric delivery technologies are in the works, including:

- A binational US–Canada Joint Task Force on the Power Outage of 14 August, whose team members include the US DOE, NERC, EPRI, and other stakeholders, are investigating the blackout and its root causes. Just one week prior to the blackout, EPRI released a report on the challenges facing the US's electricity sector, outlining a framework for action. The report, the Electricity Sector Framework for the Future (ESFF), was completed prior to the outage, and provides several recommendations to enable a complete transformation of the electricity enterprise; www.epri.com/corporate/esff/viewpdfs.asp.
- The House Committee on Energy and Commerce report, "Blackout 2003: How Did It Happen and Why?" http://energycommerce.house.gov.
- Critical Foundations: Protecting America's Infrastructures, The report of the President's Commission on Critical Infrastructure Protection, October 1997, www.ciao.ncr.gov.
- US Department of Energy, "National Transmission Grid Study," 15 May 2002; http://tis.eh.doe.gov/ntgs/gridstudy/main_screen.pdf.
- EPRI's electricity technology roadmap (1999) and subsequent reports (2003): www.epri.com
- NRECA's roadmap at www.crnweb.org/crnweb/news/DV/9/00/000007z.pdf?uri=2073
- California Energy Commission's report: www.energy.ca.gov/pier/strat/strat_reports.html.

The key elements and principles of operation for interconnected power systems were established prior to the emergence of extensive computer and communication networks. Computation is now heavily used in planning, design, simulation and optimization at all levels of the power network, and computers are widely used for fast local control of equipment as well as to process large amounts of sensor data from the field. Coordination across the network happens on slower timescales via the system operators. Some coordination occurs under computer control, but much of it is still based on telephone calls between system operators at the utility control centers (even—or especially!—during an emergency). There is not yet a significant and intimate interaction of an extensive computer/communication network layer with the primary physical layer in the operation and control of a power system.

To address these and other vulnerabilities to destabilizers, the electric power industry and all pertinent public and private sectors must work together with other critical infrastructure stakeholders (see the "Additional technology and policy resources" sidebar). Specifically, we should consider carrying out a recommendation in the US National Re-

search Council 2002 report, "Making the Nation Safer: The Role of Science and Technology in Countering Terrorism" (http://books.nap.edu/html/stct/):

> "A coordinating council should be formed to ensure that the necessary research on electric power systems is carried out, that the resulting technologies have a route to market, that implementation is done expeditiously, and that the costs are recovered through appropriate incentives, fees, rate adjustments, or other funding mechanisms. The council should include, but not be limited to, representation from the North American Electric Reliability Council, DOE, the Office of Homeland Security, NARUC, EPRI and other utility industry groups, manufacturers, and ISOs and RTOs."

Another concern in electric utility organizations is the loss of knowledge and trained human capital, which is the result of reduction in work forces, downsizing, and new business focus. As we plan for a secure future, we must remember that our knowledge base is ebbing away—the average power engineer's age has increased significantly over the past two decades. Currently, a serious shortage of power engineers is developing, and this trend will continue for several decades as many engineers reach retirement age. To fill the vacancies in the power-engineering workforce, we must expand efforts beyond traditional methods to proactively recruit engineering students at earlier points in their educational program.

While there is some disagreement in the industry about the cause of decreasing numbers of those entering the power energy field, most experts agree on several factors that contribute to the lack of student interest. These include, but are not necessarily limited to, the perception of the power-engineering field as technologically mature, a decade of depressed hiring, and lower salaries for entry-level engineers.

Unfortunately, this decline in interest comes at a difficult time for the US. Recent events and blackouts have illuminated the need for engineers in the industry. However, changes in electric power operation as a result of political regulatory restructuring have highlighted the shifting requirements of today's power engineer. The trends in many utilities, energy-research organizations, and university power-engineering programs have been toward reduction, downsizing, "right sizing," and eventual capsizing. We must reverse this trend.

Technology can make a vital contribution to security by enhancing power systems' inherent resilience and flexibility to withstand terrorist attacks and natural disasters. Creating a smart grid with self-healing capabilities is no longer a distant dream; we've made considerable progress.

Achieving and sustaining infrastructure reliability, robustness, security, and efficiency requires strategic investments in research and development. Although the immediate and critical goal is to avoid widespread network failure, the longer-term vision is to enable adaptive and robust infrastructures. From a broader view, science and technology help expand upper bounds to our quality of life. During the past 10 millennia, fundamental understandings gained through scientific discovery and enabled by innovative technologies have provided humans the tools to ascend from savagery to civilization. Engineers and scientists have played a central role in shaping our world and building everlasting "monuments of our civilization" through science and technology. What lasting monuments are we building now for future generations?

Given economic, societal, and quality-of-life issues and the ever-increasing interdependencies among infrastructures, this objective offers timely challenges to all of us: Will the electricity infrastructure evolve to become the primary support for the 21st century's digital society—a smart grid—or be left behind as a 20th century industrial relic? □

Acknowledgments

I developed most of the material and findings presented here while I was at the Electric Power Research Institute (EPRI) in Palo Alto, California. I gratefully acknowledge EPRI's support and feedback from numerous colleagues at EPRI, universities, industry, and government agencies.

References

1. *Electricity Technology Roadmap: 1999 Summary and Synthesis,* tech. report CI-112677-V1, EPRI, Palo Alto, Calif., July 1999; www.epri.com/corporate/discover_epri/roadmap/.
2. P. Kundur, *Power System Stability and Control*, EPRI Power System Engineering Series, McGraw-Hill, 1994.
3. J.F. Hauer and J.E. Dagle, *Review of Recent Reliability Issues and System Events*, US Dept. of Energy, 30 Aug. 1999; www.eere.energy.gov/der.transmission/pdfs/reliabilityevents.pdf.
4. M. Amin, "Toward Self-Healing Energy Infrastructure Systems," *IEEE Computer Applications in Power*, vol. 14, no. 1, Jan. 2001, pp. 20–28.
5. M.Amin, "Energy Infrastructure Defense Systems," *Proc. IEEE*, to be published 2005.
6. *Electricity Technology Roadmap: Synthesis Module on Power Delivery System and Electricity Markets of the Future*; tech. report, EPRI, www.epri.com.
7. M. Amin, "Security Challenges for the Electricity Infrastructure," *Computer*, April 2002, pp. 8–10.
8. M. Amin, "Toward Self-Healing Infrastructure Systems,"

Computer, vol. 33, no. 8, Aug. 2000, pp. 44–53.
9. M. Amin, "Modeling and Control of Complex Interactive Networks," *IEEE Control Systems Magazine*, vol. 22, no. 1, Feb. 2002, pp. 22–27.
10. US Nat'l Science Foundation, "Research and Development in Industry: 2000," tech. report, NSF 03-318, US Nat'l Science Foundation, Arlington,Va., June 2003; www.nsf. gov/sbe/srs/nsf03318/pdf/taba19.pdf.
11. *Electricity Infrastructure Security Assessment*, vols. 1 and 2, EPRI, Palo Alto, Calif., 2001.
12. "Communication Security Assessment for the United States Electric Utility Infrastructure," tech. report 1001174, EPRI, Palo Alto, Calif., Dec. 2000, pp. 4–11.

Massoud Amin *is professor of electrical and computer engineering, holds the H.W. Sweatt Chair in Technological Leadership, and is the director of the Center for the Development of Technological Leadership at the University of Minnesota. His research focuses on global transition dynamics to enhance resilience and security of national critical infrastructures. He has BS and MS degrees in electrical and computer engineering from the University of Massachusetts-Amherst, and MS and D.Sc. degrees in systems science and mathematics from Washington University. He previously worked for the Electric Power Research Institute (EPRI) as area manager of infrastructure security, grid operations/planning, and electricity markets, and, after 9/11, he directed all security-related research and development. He is a member of the Board on Infrastructure and the Constructed Environment (BICE) at the US National Academy of Engineering. He is a member of* IEEE Security & Privacy*'s editorial board. Contact him at amin@cdtl.umn.edu.*