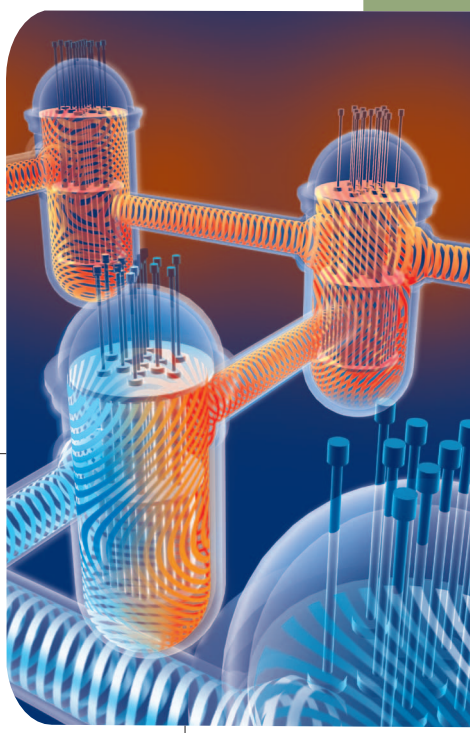
Infrastructure Security: Reliability and Dependability of Critical Systems



Massoud Amin
University of Minnesota

A new mega-infrastructure is emerging from the convergence of energy, telecommunications, transportation, the Internet, markets, and e-commerce. Moreover, some of these critical infrastructures are seeking new ways to improve network efficiency and eliminate congestion problems without seriously diminishing reliability and security.

This special issue of *IEEE Security & Privacy* focuses on the security, agility, and robustness of large-scale critical infrastructure. Specifically, it examines the challenges associated with infrastructure protection for enhanced system security, reliability, efficiency, and quality.

Network failures

The potential ramifications of network failures have never been greater: most of our critical infrastructures depend on national power grids to energize and control their operations. Secure and reliable operation of these networks is fundamental to national and international economy, security, and our quality of life.

Electrical

Of particular importance is the reliable availability of inexpensive, secure, high-quality electrical power and high-performance communication networks. The Northeast/Canadian blackout of August 2003, European outages in summer 2003, the Western US states' power crisis from 2000 to 2001, and the growing prevalence of Internet hacker attacks and email viruses demonstrate that these key infrastructures are highly vulnerable to either accidental or intentional failure.

The North American power network could realistically be considered the largest and most complex machine in the world—its transmission lines connect all electric generation and distribution on the continent. In that respect, it exemplifies many of the complexities of electric power infrastructure and how technological innovation, combined with efficient markets and enabling policies, can address them. The US National Academy of Engineering has declared the North American electrical grid to be the supreme achievement of the 20th century.

However, the interconnected nature of networks means that single, isolated disturbances can cascade through and between networks with potentially disastrous consequences. Because the electric power infrastructure underpins all other critical infrastructures, it's particularly vulnerable to deliberate as well as accidental disturbances.

Both the importance and difficulty of protecting power systems has long been recognized. In 1990, the Office of Technology Assessment (OTA) of the US Congress issued a detailed report, *Physical Vulnerability of the Electric System to Natural Disasters and Sabotage*, concluding, "Terrorists could emulate acts of sabotage in several other countries and destroy critical [power system] components, incapacitating large segments of a transmission network for months. Some of these components are vulnerable to saboteurs with explosives or just high-power rifles."[1] The report also documented the potential cost of widespread electrical outages; in the New York City outage of 1977, for example, damage from looting and arson alone cost near US$155 million—roughly half of the outage's total cost.

During the 15 years since the OTA report, the situation has become even more complex. In addition to physical vulnerability, we must also consider power systems' increased susceptibility to disruptions in computer networks and communications systems. To improve operating efficiency, power system control has become more centralized, which

makes it a tempting terrorist target. Moreover, many customers have become dependent on electronic systems that are sensitive to power disturbances. A 20-minute outage at an integrated circuit fabrication plant, for example, can cost US$30 million.

Approximately 25 years ago, our electrical system had more built-in "shock absorbers" to meet peak demand; however, in recent years, these shock absorbers have steadily decreased. Years ago, the generation capacity margin, a "cushion" that could handle unexpected events or increased electricity demand, was between 25 to 30 percent—that cushion has now shrunk to less than half that, currently hovering around 10 to 15 percent. During the 1990s, actual demand for electricity in the US increased some 35 percent, whereas transmission capacity increased by only 18 percent. The demand is expected to grow by 20 percent in the current decade, with new transmission capacity lagging behind at less than 4 percent. This added capacity serves as a risk-managed plan in case equipment fails, or in case there is an unusually high demand for power, such as on very hot or cold days. As a result, the average outage affected 15 percent more consumers from 1996 to 2000 than from 1991 to 1995.[2,3]

For the past quarter of a century, the condition of our national infrastructure has been stagnate or deteriorating. In March 2001, September 2003, and March 2005, the American Society of Civil Engineers (ASCE) released its Report Cards for America's Infrastructure (www.asce.org/reportcard), an assessment of the trends affecting 12 infrastructure areas, including roads, bridges, transit, aviation, drinking water, wastewater, dams, hazardous waste, navigable waterways, and energy.

An ASCE report card scores includes evaluations based on a multitude of categories; each category is evaluated on condition and performance, capacity versus need, and funding versus need. The grades range from A for exceptional to F for failing. The overall scores for 2001, 2003, and 2005 were D+, D+, and D, respectively. In 2001, the ASCE estimated that it would take US$1.3 trillion over the next five years to fix the problems. This amount increased to $1.6 trillion by 2003, and again in 2005.

Information technology is emerging as a notable force of change in power delivery. High-speed powerline networks, automated real-time meters, and other "gateway to the home" devices, along with the ubiquitous Internet, have enabled new types of entities to enter the electric power industry. Power marketers and providers of electricity and related services are no longer the sole providers of electrons. Competition is likely to spur further demand for information technologies, which will in turn stimulate the development of advanced control, computing, and metering technologies.

Science and technology responses to these challenges include advances in mathematical foundations of complex systems and other emerging computational, control, and communication systems that provide an attractive bottom-up paradigm for modeling, simulation, control, optimization, and adaptive protection of operations—both financial and physical—in complex networks. Practical methods, tools, and technologies based on advances in these fields are beginning to allow power grids and other infrastructures to locally self-regulate, including automatic reconfiguration in the event of failures, threats, or disturbances.[4–6]

Communication risk

Recognizing the increased interdependence between IT and electricity infrastructures, the energy industry is tightening its hold on its networks, even in the face of deregulation and the resulting commercial competition. But in today's environment, traditional external entities such as suppliers, consumers, regulators, and even competitors must now have access to segments of the network. This access greatly increases the security risk to other functional segments of the internal network.

Security for the cyber and communication networks used by a growing variety of businesses is fundamental to the reliable operation of the grid connecting all these networks together. As power systems rely more heavily on computerized communications and control, system security has become increasingly dependent on protecting the integrity of the associated information systems. Part of the problem is that existing control systems, which were originally designed for proprietary, stand-alone communications networks, were later connected to the Internet (because of its productivity advantages and lower costs), but without systematically adding the technology to make them secure.[7,8]

Like any complex dynamic infrastructure system, the electricity grid has many layers and is vulnerable to many different types of disturbances. Although strong centralized control is essential to reliable operations, it requires multiple, high-data-rate, two-way communication links, a powerful central computing facility, and an elaborate operations control center, all of which are especially vulnerable when they are needed most—during serious system stresses or power disruptions. For deeper protection, intelligent distributed control is also required to keep parts of the network operational.[4–6]

Secure communications

Although most organizations attempt to protect their business systems and control centers from cyberattacks, plant control systems and substations might not be adequately protected, allowing the penetration of mission-critical operational systems via unsecured access points.

Potential risks span the spectrum from having data stolen (industrial espionage) to total loss of power flow control to substantial physical damage (sabotage). [7,8]

As a first step, information security provisions such as authorization, authentication, and encryption must be added to current communications protocols. To accomplish this, each protocol must be reexamined to determine the impact on performance of adding such security features. Eventually, however, a secure, private communications system must be adopted as an effective alternative to Internet-based systems. Advanced cybersecurity technologies are particularly needed for power system control and monitoring.

The next step is a comprehensive assessment to determine which communications technologies and security options are appropriate for utility operations and where they should be implemented first. Utilities have unique requirements for communications performance, including timing, redundancy, substation control and protection, and equipment control and diagnostics, which must be preserved in spite of security constraints. In particular, security adds data "overhead" and timing delays that could disrupt real-time operations, which means that issues of time and bandwidth will also have to be solved.

Next, efficacy of designing a new private communications network must be considered; such a system can be built from the ground up to provide the required levels of security, including authorization, authentication, encryption, intrusion detection, and redundancy. New networks must impart sufficient bandwidth and improved efficiency to provide real-time data to meet the requirements of control center operations.

From a strategic research and development viewpoint, the lack of a unified framework with robust tools poses several policy and technological challenges.

The Articles

The articles in this special issue go a long way toward addressing two key issues in distributed denial-of-service (DDoS) attacks and the development of a pragmatic approach to quantifying security and calculating risk.

Large-scale worm outbreaks that lead to DDoS flooding attacks can cause many different kinds of Internet catastrophes. In "Collaborative Internet Worm Containment," Min Cai et al., suggest a new WormShield system for automated worm signature detection and dissemination to stop worms from spreading. The authors' large-scale worm simulation shows that collaborative WormShield monitors can detect worm signatures approximately 10 times faster than using independent monitors.

Mehmet Sahinoglu, in his article, "Security Meter: A Practical Decision-Tree Model to Quantify Risk," describes Security Meter, which provides a quantitative technique with an updated repository on vulnerabilities, threats, and countermeasures to calculate risk.

Digital technology can make a vital contribution to reliability and security by enhancing infrastructure systems' resilience and flexibility to withstand terrorist attacks and natural disasters. But considerable technical challenges and several economic and policy issues remain to be addressed: What threat level is the industry responsible for? Will market-based priorities support a strategically secure power system? Who will pay for the economic incentives for such investments? What overall system architecture is most conducive to maintaining security?

Advanced technology now under development holds the promise of meeting the electricity needs of a robust digital economy. The potential exists to create an electricity system that provides the same efficiency, precision, and interconnectivity as the billions of microprocessors that it will power. ▢

References

1. US Office of Technology Assessment, *Physical Vulnerability of the Electric System to Natural Disasters and Sabotage*, tech. report OTA-E-453, US Government Printing Office, June 1990.
2. M. Amin, "North America's Electricity Infrastructure: Are We Ready for More Perfect Storms?," *IEEE Security & Privacy*, vol. 1, no. 5, 2003, pp. 19–25.
3. M. Amin, "Balancing Market Priorities with Security Issues: Interconnected System Operations and Control under the Restructured Electricity Enterprise," *IEEE Power and Energy Magazine*, vol. 2, no. 4, 2004, pp. 30–38.
4. M. Amin, "Toward Self-Healing Energy Infrastructure Systems," *IEEE Computer Applications in Power*, vol. 14, no. 1, 2001, pp. 20–28.
5. M. Amin, "Toward Self-Healing Infrastructure Systems," *Computer*, vol. 33, no. 8, 2000, pp. 44–53.
6. *Proc. IEEE on Energy Infrastructure Defense Systems*, special issue, vol. 93, no. 5, 2005.
7. EPRI, *Communication Security Assessment for the United States Electric Utility Infrastructure*, EPRI Report 1001174, Dec. 2000, pp. 4–11.
9. M. Amin, "Security Challenges for the Electricity Infrastructure," supplement to *Computer*, Apr. 2002, pp. 8–10.

Massoud Amin *is a professor of electrical and computer engineering and holds the H.W. Sweatt Chair in Technological Leadership at the University of Minnesota. His research focuses on global transition dynamics to enhance resilience and security of national critical infrastructure. Amin received a BS and an MS in electrical and computer engineering from the University of Massachusetts-Amherst, and an MS and a DSc in systems science and mathematics from Washington University. He is a senior member of the IEEE. Contact him at amin@umn.edu.*