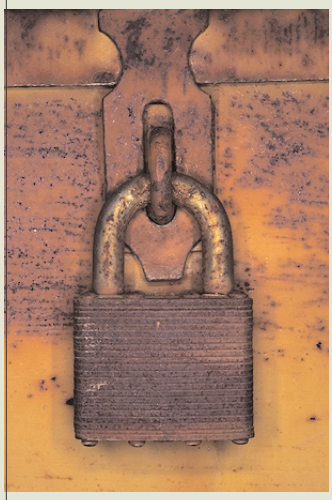

Secure and reliable operation of our energy and information infrastructures is fundamental to national and international economy, security, and quality of life.

Security Challenges for the Electricity Infrastructure

Massoud Amin, Electric Power Research Institute (EPRI)

Because critical infrastructures touch us all, the growing potential for infrastructure problems stems from multiple sources, including system complexity, economic growth, deregulation, terrorism, and even the weather. Electric power systems constitute the fundamental infrastructure of modern society. 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.

Indeed, because of the intimate connections between power systems and society's other infrastructures, we need to consider three different kinds of threats:

- *Attacks upon the power system*. In this case, the electricity infrastructure itself is the primary target—with outages rippling into the customer base. The point of attack could be a single component—a critical substation or a transmission tower. Or there could be a simultaneous, multipronged attack intended to bring down an entire regional grid. Similarly, the attack could target electricity markets, highly vulnerable because of their transitional status.
- *Attacks by the power system*. Here, the ultimate target is the population, using parts of the electricity infrastructure as a weapon. Terrorists could use power plant cooling towers, for example, to disperse chemical or biological agents.
- *Attacks through the power system*. The target is the civil infrastructure in this case. Utility networks include multiple conduits for attack, including lines, pipes, underground cables, tunnels, and sewers. For example, terrorists could couple an electromagnetic pulse through the grid to damage computer or telecommunications infrastructure.

The dilemma

The terrorist attacks of 11 September have exposed critical vulnerabilities in America's essential infrastructures: Never again can the security of these fundamental systems be taken for granted. In particular, the electric power industry must quickly rethink its basic approach to system security—identifying the most important vulnerabilities and implementing programs to address the terrorist threat through improved prevention, mitigation, and recovery. These lessons apply as well to the infrastructures of countries around the world.

The specter of terrorism raises a profound dilemma for the electric power industry: How to make the electricity infrastructure more secure without compromising the productivity advantages inherent in today's complex, highly interconnected electric networks? Resolving this dilemma will require both short- and long-term technology development and deployment, affecting some of the fundamental characteristics of today's power systems:

- *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 greatly increased efficiency and improved customer service. But if terrorists can exploit the weaknesses of centralized control, security would seem to demand that smaller, local systems become the system configuration of choice. In fact, strength and resilience in the face of attack will increasingly rely upon the ability to bridge simultaneous top-down and bottom-up decision-making in real time.
- *Increasing complexity*. The North American electric power system might be the most complex machine ever built. 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. In response, we 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 capability—ranging from high-speed data transfer among control centers to interpretation of intermittent signals from remote sensors. Because of the vulnerability of Internet communications, however, protecting the electricity supply system will require new technology to enhance the security of power system command, control, and communications, including both hardware and software.

- *Assessing the most effective security investments.* . Although hardening of some key components, such as power plants and critical substations, is certainly desirable, providing comprehensive physical protection to all components is simply not feasible or economic. Probabilistic assessments can offer strategic guidance on where and how to deploy security resources to greatest advantage.

Fortunately, the core technologies needed to strategically enhance system security are the same as those needed to resolve other areas of system vulnerability. These result from open access, exponential growth in power transactions, and the reliability needed to serve an increasingly digital society.

Security and quality needs

The North American electric power system needs a comprehensive strategy to prepare for the diverse threats posed by terrorism. Such a strategy should both increase protection of vital industry assets and ensure the public that they are well protected. We'll need to consider a number of actions in formulating an overall security strategy, including securing the grid from cascading damage; sealing off pathways for environmental attack; monitoring conduits for attack, then sealing them off and "sectionalizing" them under attack conditions; securing critical controls and communications from penetration by hackers and terrorists; building greater intelligence into the grid for flexibility and adaptability under attack conditions, including automatic reconfiguration; and providing ongoing security assessments, including the use of game theory to develop potential attack scenarios, to ensure that the power industry can stay ahead of changing vulnerabilities.

Advanced technology will necessarily play an important role in efforts to provide enhanced security because of the electricity infrastructure's unique attributes. Assuming that individual utilities are already undertaking prudent steps to improve physical security wherever possible, technology can make a vital contribution by enhancing the inherent resilience and flexibility of power systems to withstand terrorist attacks, as well as natural disasters.

At the Electric Power Research Institute (EPRI)—a nonprofit energy research consortium organized for the benefit of utility members, their customers, and society at large—we are responding to this need by launching an Infrastructure Security Initiative, a two-year program funded by the electric power industry to develop and apply key technologies that could greatly improve overall system security.[1]

What we seek is a new standard of performance. Many in our industry have called for an increase in reliability from today's average of about 99.9% (approximately 8 hours of outage per year) to 99.9999% (about 32 seconds outage per year) or even 99.9999999% (one outage lasting less than a single ac cycle per year).

Such near-perfect power is needed for error-free operation of the microprocessor chips finding their way into just about everything, including billions of embedded applications, these days. The future digital society will be built on microprocessors—in smart refrigerators that automatically keep themselves stocked, in smart door locks that know who to let in and when, smart shoes that monitor your daily exercise and physical condition, smart wallets, smart curtains, smart toothbrushes, and smart cereal boxes.

Adequate microprocessors now cost just a few dollars; before long the price will be a few cents or less. The catch is the quality of electricity service: unprotected microprocessors demand perfect power to function properly. A similar need of perfection exists for other infrastructures, where future advanced systems are predicated on the perfect functioning of today's communications, transportation, and financial services.

Human performance

Because humans interact with these infrastructures 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 economic and financial aspects, will require modeling the bounded rationality of actual human thinking, unlike that of a hypothetical "expert" human as in most applications of artificial intelligence. Even more directly, most of these networks require some human intervention for their routine control, especially when they are exhibiting anomalous behavior that might suggest actual or incipient failure.

In many complex networks, the human participants themselves are both the most susceptible to failure and the most adaptable in the management of recovery.

Operators and maintenance personnel are obviously "inside" these networks and can have direct, real-time effects on them. But the users of a telecommunication, transportation, electric power, or pipeline system also affect the behavior of those systems, often without conscious intent. The amounts, and often the nature, of the demands put on the network can be the immediate cause of conflict, diminished performance, and even collapse. Reflected harmonics from one user's machinery degrade power quality for all. Long transmissions from a few users create Internet congestion. Simultaneous lawn watering drops the water pressure for everyone. In a very real sense, no one is "outside" the infrastructure.

Given that there is some automatic way to detect actual or imminent local failures, the obvious next step is to warn the operators. Unfortunately, the operators are usually busy with other tasks, sometimes even responding to previous warnings. In the worst case, the detected failure sets off a multitude of almost simultaneous alarms as it begins to cascade through the system, and, before the operators can determine the real source of the problem, the whole network has shut itself down automatically.

Unfortunately, humans have cognitive limitations that can cause them to make serious mistakes when they are inter-

rupted. In recent years, a number of systems have been designed that let users delegate tasks to intelligent software assistants (softbots) that operate in the background, handling routine tasks and informing the operators in accordance with some protocol that establishes the level of their delegated authority to act independently. In this arrangement, the operator becomes a supervisor, who must either cede almost all authority to subordinates or be subject to interruption by them.

Meeting the challenge

In the electric power industry and other critical infrastructures, technologists are seeking new ways to improve network efficiency and eliminate congestion problems without seriously diminishing reliability and security. Achieving these objectives in light of their vulnerability to cascading outages—initiated by material failure, natural calamities, intentional attack, or human error, as well as demands posed by economic, societal, and quality-of-life considerations and the ever-increasing interdependencies between interconnected infrastructures—offers new and exciting scientific and technological challenges.

Recently, the US Department of Defense and EPRI jointly funded the Complex Interactive Networks/Systems Initiative to produce a significant, strategic advancement in the robustness, reliability, and efficiency of the interdependent energy, communications, financial, and transportation infrastructures.[2] Six consortia, consisting of 107 professors and numerous researchers and graduate students in 26 US universities, focused on advancing basic knowledge and developing breakthrough concepts in modeling and simulation; measurement, sensing, and visualization; control systems; and operations and management.

To date, these results include over 350 papers published or submitted for publication, with 19 promising technologies extracted and transferring to the industry. As an example, a key high-priority technology is *adaptive intelligent islanding*: When major disruptions occur on a power system today, the transmission network automatically responds by breaking into self-contained islands, according to fixed procedures established well in advance. Such procedures have not generally been updated since the onset of deregulation and will not be adequate for dealing with a terrorist attack on multiple carefully chosen targets. Rather, we need a more flexible islanding method that can react instantaneously to attack conditions, taking into account the location and severity of damage, load status, and available generation.

Another pertinent area involves security of the cyber and communication network; 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. But existing control systems, which were originally designed for use with proprietary, standalone communications networks, were later connected to the Internet, but without adding the technology needed to make them secure.

Information is a critical business resource for nearly every modern industry. Communication of critical business information and controlled sharing of that information are essential parts of all business operations and processes. As the deregulation of the energy industry unfolds, information security will become more important. For the energy-related industries, the need to balance the apparently mutually exclusive goals of operating system flexibility with the need for security will need to be addressed from a business perspective.

Key electric energy operational systems depend on real-time communication links both internal and external to the enterprise. The functional diversity of these organizations means that these key systems must be designed with a focus on open systems that users can configure for integrating with other external and internal systems. In many cases, these systems can be reconfigured using telecommunication technologies; in nearly all cases, the systems dynamically exchange data in real time. This results in a need for highly reliable, secure control and information management systems.

From a broader view, the various areas of interactive infrastructure networks present numerous theoretical and practical challenges. Modeling, prediction, simulation, cause and effect relationships, analysis, optimization and control of coupled systems comprised of a heterogeneous mixture of dynamic, interactive, and often nonlinear entities, unscheduled discontinuities, and numerous other significant effects all must be addressed. Furthermore, a pertinent question is at what resolution should sensing, modeling, and control be started to achieve the overall objectives of efficiency, robustness and reliability?

Our immediate and critical goal is to avoid widespread network failure, but the longer-term vision is to enable adaptive and robust infrastructure; as expressed in the July 2001 issue of *Wired*: "The best minds in electricity R&D have a plan: Every node in the power network of the future will be awake, responsive, adaptive, price-smart, eco-sensitive, real-time, flexible, humming—and interconnected with everything else."[3]

Achieving this vision and sustaining infrastructure reliability, robustness, and efficiency are critical long-term issues that require strategic investments in research and development. Given economic, security, societal, and quality-of-life issues and the ever-increasing interactions and interdependencies among infrastructures, this objective offers exciting scientific and technological challenges.

References

1. EPRI, *Electricity Infrastructure Security Assessment*, Vol. I-II, EPRI, Palo Alto, Calif., Nov. and Dec. 2001.
2. A. Amin, "EPRI/DoD Complex Interactive Networks/Systems Initiative: Self-Healing Infrastructures," *Proc. 2nd DARPA-JFACC Symp. Advances in Enterprise Control*, IEEE Computer Soc. Press, Los Alamitos, Calif., 2000.
3. S.Silberman, "The Energy Web," *Wired*, vol. 9, no. 7, July 2001.

Massoud Amin is area manager, Infrastructure Security, and serves as lead, Mathematics and Information Science at the Electric Power Research Institute (EPRI). Contact him at EPRI, 3412 Hillview Ave., Palo Alto, CA 94304-1395; mamin@epri.com.