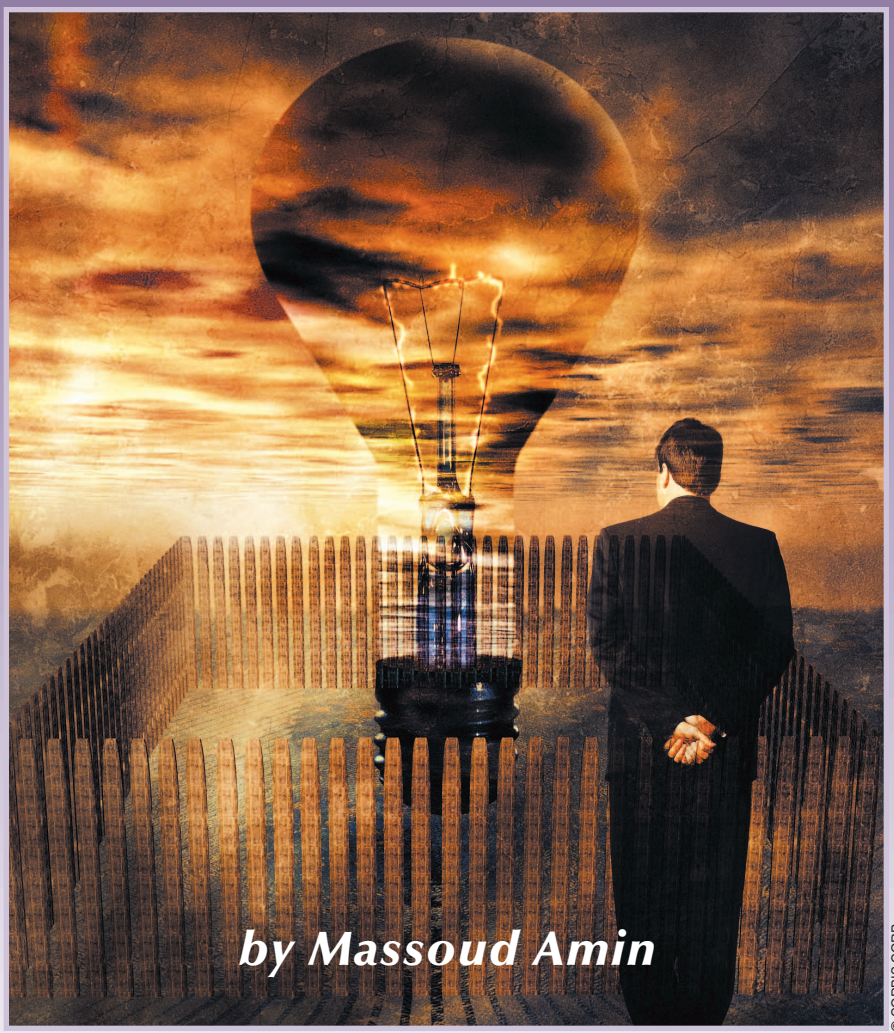
Balancing Market Priorities with Security Issues



by Massoud Amin

1540-7977/04/$20.00©2004 IEEE

Interconnected System Operations and Control under the Restructured Electricity Enterprise

OUR NATIONAL SECURITY AND DIGITAL ECONOMY PLACE INCREASED DEMAND for reliable and disturbance-free electricity. The massive power outages in the United States, Canada, United Kingdom, and Italy in 2003 underscored electricity infrastructure's vulnerabilities. This vital yet complex infrastructure underpins our society and quality of life—what role can enabling technologies, business/economic analyses, and judicious policies play in predicting, averting, and/or managing future crises?

From a broader perspective, during the past ten 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 to shape our world and built everlasting "monuments of our civilization" through science and technology. The key challenge before us is what lasting monuments are we building now for future generations?

All economic and societal progress depends on a reliable and efficient energy infrastructure; for instance, banking and finance depend on the robustness of electric power, cable, and wireless telecommunications. Transportation systems including military and commercial aircraft and land and sea vessels depend on communication and energy networks. The linkages between electric power grid, telecommunications, and couplings of electric generation with oil, water, and gas pipelines are ever increasing and continue to be a lynchpin of energy supply networks.

These characteristics, in turn, present unique challenges in modeling, prediction, simulation, cause and effect relationships, analysis, optimization, and control. What set of theories can capture a mix of dynamic, interactive, and often nonlinear entities with unscheduled discontinuities? Another important dimension is the effect of deregulation and economic factors on a particular infrastructure and the impact of policies and human performance. Complex network research shows that although the people who are part of the complex system are the most susceptible to failure, they are also the most adaptable in managing its recovery. To successfully model infrastructure systems, especially through economic and financial market simulations, then, we must model the bounded rationality of human thinking.

The North American power network may realistically be considered to be the largest and most complex machine in the world—its transmission lines connect all the 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. This network represents an enormous investment, including over 15,000 generators in 10,000 power plants, and hundreds of thousands of miles of transmission lines and distribution networks, whose estimated worth is over US$800 billion. In 2000, transmission and distribution was valued at US$358 billion.

Through the North American electricity infrastructure, every user, producer, distributor and broker of electricity buys and sells, competes and cooperates in an "ElectricityEnterprise." Every industry, every business, every store and every home is a participant, active or passive, in this continent-scale conglomerate. Over the last decade and during the next few years, the electric enterprise will undergo dramatic transformation as its key participants—the traditional electric utilities—respond to deregulation, competition, tightening environmental/land-use restrictions, and other global trends.

However, this 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

Fortunately, the core technologies needed to strategically enhance system security are the same as those needed to resolve other areas of system vulnerability.

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.

Secure and reliable operation of these systems is fundamental to national and international economy, security, and quality of life. Their very interconnectedness makes them more vulnerable to global disruption, initiated locally by material failure, natural calamities, intentional attack, or human error.

The Electricity Enterprise: Today and Tomorrow

Possibly the largest machine in the world, North American power network's transmission lines connect all generation and distribution on the continent to form a vertically integrated hierarchical network. The question is raised as to whether there is a unifying paradigm for the simulation, analysis, and optimization of time-critical operations (both financial transactions and actual physical control) in these multiscale, multicomponent, and distributed systems. In addition, mathematical models of interactive networks are typically vague (or may not even exist); moreover, existing and classical methods of solution are either unavailable, or are not sufficiently powerful. For the most part, no present methodologies are suitable for understanding their behavior.

Another important dimension is the effect of deregulation and economic factors on a particular infrastructure. While other and more populous countries, such as China and India, will have greater potential electricity markets and demands, the United States is presently the largest national market for electric power. Its electric utilities have been mostly privately owned, vertically integrated, and locally regulated. National regulations in areas of safety, pollution, and network reliability also constrain their operations to a degree, but local regulatory bodies, mostly at the state level, have set their prices and their return on investment, and have controlled their investment decisions while protecting them from outside competition. That situation is now rapidly changing, as state regulators are moving toward permitting and encouraging a competitive market in electric power.

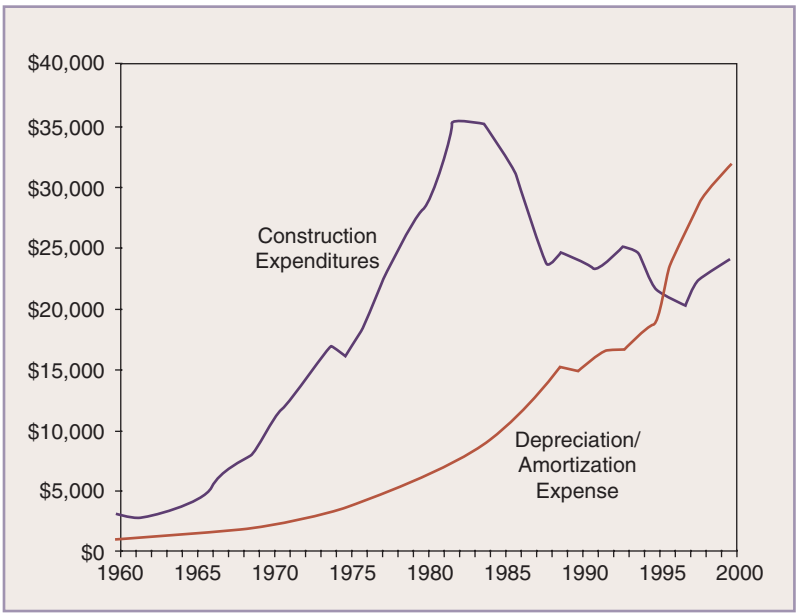


figure 1. Since the "cross over" point in about 1995 utility construction expenditures have lagged behind asset depreciation. This has resulted in a mode of operation of the system analogous to "harvesting the farm far more rapidly than planting new seeds" (data provided by EEI and graph courtesy of EPRI).

The electric power grid was historically operated by separate utilities; each independent in its own control area and regulated by local bodies, to deliver bulk power from generation to load areas reliably and economically—as a noncompetitive, regulated monopoly, emphasis was on reliability (and security) at the expense of economy. Competition and deregulation have created multiple energy producers that must share the same regulated energy delivery network. Traditionally, new delivery capacity would be added to handle load increases, but because of the current difficulty in obtaining permits and the uncertainty about achieving an adequate rate of return on investment, total circuit miles added annually are declining while total demand for delivery resources continues to grow. In recent years, the "shock absorbers" have been shrinking; e.g., during the 1990s actual demand in the United States increased some 35%, while capacity has increased only 18%, the most visible parts of a larger and grow-

ing U.S. energy crisis that is the result of years of inadequate investments in the infrastructure. According to EPRI analyses, since 1995 to the present the amortization/depreciation rate exceeds utility construction expenditures (Figure 1).

As a result of these "diminished shock absorbers," the network is becoming increasingly stressed, and whether the carrying capacity or safety margin will exist to support anticipated demand is in question. The complex systems used to relieve bottlenecks and clear disturbances during periods of peak demand are at great risk to serious disruption, creating a critical need for technological improvements.

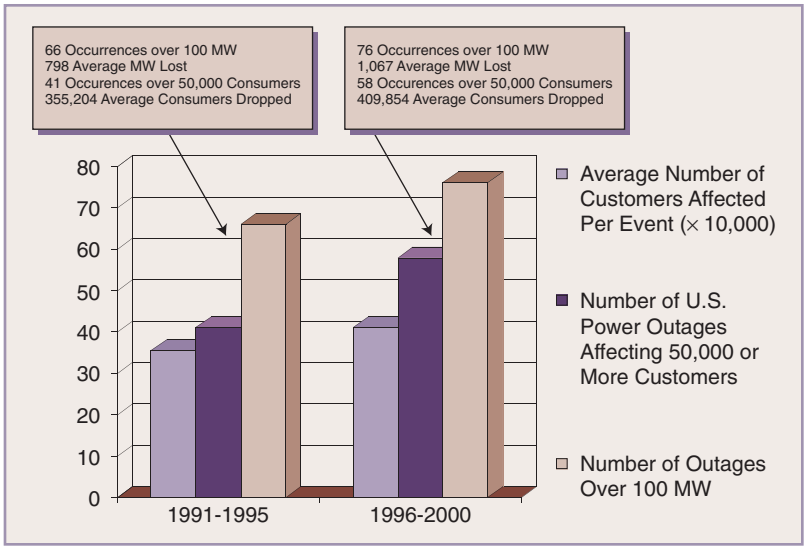


figure 2. Increasing frequency and size of U.S. power outages 100 MW or more (1991–1995 versus 1996–2000), affecting 50,000 or more consumers per event. Generally, a relatively small number of U.S. consumers experience a large number of outages; conversely, outages that affect a large number of consumers are quite rare; however, this plot could also indicate that the number of larger outages could be rising (data courtesy NERC's disturbance analysis working group database).

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. Widespread outages and huge price spikes during the past few years raised public concern about grid reliability at the national level. According to data from the North American Electric Reliability Council (NERC) and analyses from the Electric Power Research Institute (EPRI), average outages from 1984 to the present have affected nearly 700,000 customers per event 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 or more customers per event each decade. These analyses are based on data collected for the U.S. 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.

Coupling these analyses with diminished infrastructure investments, and noting that the cross-over point for the utility construction investment versus depreciation occurred in 1995 (Figure 1), we analyzed the number and frequency of major outages along with the number of customers affected during the decade 1991–2000; splitting it into the two time periods 1991–1995 and 1996–2000 (Figure 2). Based on EPRI's analyses of data in NERC's Disturbance Analysis Working Group (DAWG) database, 41% more outages affected 50,000 or more consumers in the second half of the 1990s than in the first half (58 outages in 1996–2000 versus 41 outages in 1991–1995). The average outage affected 15% more consumers from 1996 to 2000 than from 1991 to 1995 (average size per event was 409,854 customers affected in the second half of the decade versus 355,204 in the first half of the decade). In addition, there were 76 outages of 100 MW 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%, from 798 MW from 1991 to 1995 to 1067 MW from 1996 to 2000 (Figure 2).

Electricity Infrastructure: Interdependencies with Cyber and Digital Infrastructures

Electric power utilities typically own and operate at least parts of their own telecommunications systems, which often consist of backbone fiber-optic or microwave connecting major substations, with spurs to smaller sites. Increased use of electronic automation raises significant issues regarding the adequacy of operational security. As is true of other critical infrastructures, increased use of automated technologies raises significant security issues, however:

- ✔ reduced personnel at remote sites makes the sites more vulnerable to hostile threats
- ✔ interconnecting automation and control systems with public data networks makes them accessible to individuals and organizations, from any worldwide location using an inexpensive computer and a modem
- ✔ use of networked electronic systems for metering, scheduling, trading, or e-commerce imposes numerous financial risks associated with network failures.

In what follows we shall provide a brief overview of some key areas and present selected security aspects of operational systems, without discussing potentially sensitive material; these aspects include:

- ✔ operational systems rely very heavily on the exchange of information amongst disparate systems
- ✔ utilities rely on very extensive private and leased telecommunication systems
- ✔ networking of these systems is expanding rapidly
- ✔ networking is expanding beyond utility doors, to encompass other utilities, corporations, and customers
- ✔ standard communication protocols and integration techniques are a MUST, despite the increased security risks
- ✔ increased security concerns in the aftermath of tragic events of 11 September 2001
- ✔ deregulation is increasing the incentives for unauthorized access to information.

Infrastructures under Threat

The terrorist attacks of September 11 have exposed critical vulnerabilities in America's essential infrastructures: Never again can the security of these fundamental systems be taken for granted. 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 the lives of every citizen. Yet power systems have widely dispersed assets that can never be absolutely defended against a determined attack.

Because critical infrastructures touch us all, the growing potential for infrastructure problems stems from multiple sources. These sources include system complexity, deregulation, economic effects, power-market impacts, terrorism, and human error. The existing power system is also vulnerable to natural disasters and intentional attacks. Regarding the latter, a November 2001 EPRI assessment developed in response to the September 11, 2001, attacks highlights three different kinds of potential threats to the U.S. electricity infrastructure:

- ✔ **Attacks *upon* the power system.** In this case, the electricity infrastructure itself is the primary target—with ripple effects, in terms of outages, extending into the customer base. The point of attack could be a single component, such as a critical substation, or a transmission tower. However, there could also be a simultaneous, multipronged attack intended to bring down the entire grid in a region of the United States. Similarly, the attack could target electricity markets, which because of their transitional status is highly vulnerable.
- ✔ **Attacks *by* the power system.** In this case, the ultimate target is the population, using parts of the electricity infrastructure as a weapon. Power plant cooling towers, for example, could be used to disperse chemical or biological agents.
- ✔ **Attacks *through* the power system.** In this case, the target is the civil infrastructure. Utility networks include multiple conduits for attack, including lines, pipes, underground cables, tunnels, and sewers. An electromagnetic pulse, for example, could be coupled through the grid with the intention of damaging computer and/or telecommunications infrastructure.

The Dilemma: Security and Quality Needs

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-term and long-term technology development and deployment, affecting some of the fundamental characteristics of today's power systems:

- ✔ **Centralization/decentralization of control.** For several years, there has been a trend toward centralizing control of electric power systems. Emergence of regional transmission organizations (RTOs) as agents of wide-area control, for example, offers the promise of 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 has been called 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, new mathematical approaches are needed to simplify the operation of complex power systems and to 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, protection of the electricity supply system requires new technology to enhance the security of power system command, control, and communications, including both hardware and software.
- ✔ **Accessibility and vulnerability.** Because power systems are so widely dispersed and relatively accessible, they are particularly vulnerable to attack. Although "hardening" of some key components, such as power plants and critical substations, is certainly desirable, it is simply not feasible or economic to provide comprehensive physical protection to all components. 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, as identified in the *Electricity Technology Roadmap*. These result from open

The dilemma is to make the electricity infrastructure more secure without compromising the productivity advantages inherent in today's complex, highly interconnected electric networks.

access, exponential growth in power transactions, and the reliability needed to serve a digital society.

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. A number of actions will need to be considered in formulating an overall security strategy.

- ✔ The grid must be made secure from cascading damage.
- ✔ Pathways for environmental attack must be sealed off.
- ✔ Conduits for attack must be monitored, sealed off, and "sectionalized" under attack conditions.
- ✔ Critical controls and communications must be made secure from penetration by hackers and terrorists.
- ✔ Greater intelligence must be built into the grid to provide flexibility and adaptability under attack conditions, including automatic reconfiguration.
- ✔ Ongoing security assessments, including the use of game theory to develop potential attack scenarios, will be needed to ensure that the power industry can stay ahead of changing vulnerabilities.

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. 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.

Human Performance

Since 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 (AI). Even more directly, most of these networks require some human intervention for their routine control and especially when they are exhibiting anomalous behavior that may suggest actual or incipient failure.

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 immanent 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 interrupted. In recent years, a number of systems have been designed that allow users to 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. At present, we have very limited understanding of how to design user interfaces to accommodate interruption.

Broader Technical Issues

In response to the above challenges, several enabling technologies and advances are/will be available that can provide necessary capabilities when combined in an overall system design. Among them are the following:

- ✔ Flexible AC transmission system (FACTS) devices, which are high-voltage thyristor-based electronic controllers that increase the power capacity of transmission

lines and have already been deployed in several high-value applications. At peak demand, up to 50% more power can be controlled through existing lines.

- ✔ Fault current limiters (FCLs), which absorb the shock of short circuits for a few cycles to provide adequate time for a breaker to trip. It is noteworthy that preliminary results of the post 14 August outage show that FCLs could have served as large electrical "shock absorbers" to limit the size of blackouts.
- ✔ Wide-area measurement systems (WAMS), which integrate advanced sensors with satellite communication and time stamping using global positioning systems (GPS) to detect and report angle swings and other transmission system changes.
- ✔ Innovations in materials science and processing, including high-temperature superconducting (HTS) cables, oxide-power-in-tube technology for HTS wire, and advanced silicon devices and wide-bandgap semiconductors for power electronics.
- ✔ Distributed resources such as small combustion turbines, solid oxide and other fuel cells, photovoltaics, superconducting magnetic energy storage (SMES), transportable battery energy storage systems (TBESS), etc.
- ✔ Information systems and online data processing tools such as the Open Access Same-time Information System (OASIS); and Transfer Capability Evaluation (TRACE) software, which determines the total transfer capability for each transmission path posted on the OASIS network, while taking into account the thermal, voltage, and interface limits.
- ✔ Monitoring and use of IT: Wide-Area Measurement/Management Systems (WAMS), Open-access Same-time Information System (OASIS), Supervisory Control and Data Acquisisiton (SCADA) Systems, Energy Management Systems (EMS).
- ✔ Analysis tools: Several software systems for dynamic security assessment of large/wide-area networks augmented with market/risk assessment.
- ✔ Control: FACTS and fault current limiters (FCLs)
- ✔ Intelligent electronic devices with security provisions built-in combining sensors, computers, telecommunications units, and actuators; integrated sensor; two-way communication; "intelligent agent" functions: assessment, decision, learning; actuation, enabled by advances in several areas including semiconductors, and resource-constrained encryption.

However, if most of the above technologies are developed, still the overall systems' control will remain a major challenge. This is a rich area for research and development of such tools, as well as to address systems and infrastructure integration issues of their deployment in the overall network—especially now because of increased competition, the demand for advanced technology to gain an advantage, and the challenge of providing the reliability and quality consumers demand.

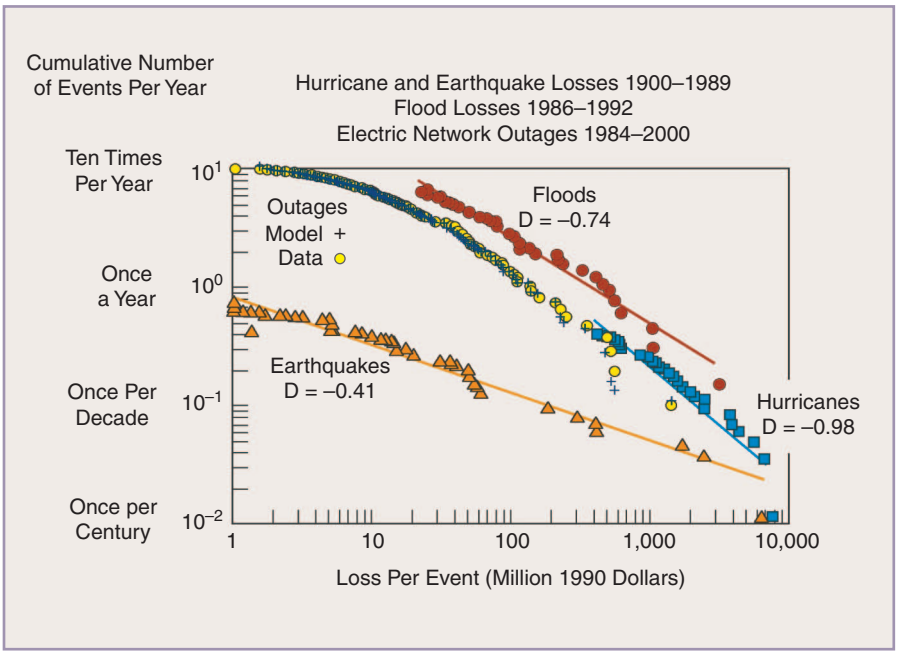


figure 3. Understanding complex systems and global dynamics. Economic losses from disasters were found to follow a power law distribution—for hurricanes, floods, earthquakes, and even electrical outages. Fundamental power law distributions also were found for forest fires, internet congestion, and other systems. CIN/SI results such as these translate into new approaches for optimizing complex systems in terms of productivity and robustness to disaster. Our goal is to move the power outage curve down toward the origin; i.e., to make outages less frequent and with smaller impact on customers. [Source: the EPRI/DoD complex interactive networks/systems initiative (CIN/SI).]

Complex System Failure

Beyond the human dimension, there is a strategic need to understand the societal consequences of infrastructure failure risks along with benefits of various tiers of increased reliability. From an infrastructure interdependency perspective, power, telecommunications, banking and finance, transportation and distribution, and other infrastructures are becoming more and more congested and are increasingly vulnerable to failures cascading through and between them. A key concern is the avoidance of widespread network failure due to cascading

To address the vulnerabilities, the electric power industry and all pertinent public and private sectors must work together with other critical infrastructure stakeholders.

and interactive effects. Moreover, interdependence is only one of several characteristics that challenge the control and reliable operation of these networks. Other factors that place increased stress on the power grid include dependencies on adjacent power grids (increasing because of deregulation), telecommunications, markets, and computer networks. Furthermore, reliable electric service is critically dependent on the whole grid's ability to respond to changed conditions instantaneously.

Prior to the tragic events of September 11, the U.S. President's Commission on Critical Infrastructure Protection in 1997 highlighted the growing concern. It noted the damaging and dangerous ways that cascading failures could unpredictably affect the economy, security, and health of citizens. Secure and reliable operation of these systems is fundamental to our economy, security, and quality of life, as was noted by the President's Commission on Critical Infrastructure Protection Report published in October 1997 and the subsequent Presidential Directive 63 on Critical Infrastructure protection, issued on 22 May 1998.

More specifically, secure and reliable operation of critical infrastructures poses significant theoretical and practical challenges in analysis, modeling, simulation, prediction, control, and optimization. To address these challenges, a research initiative—the EPRI/DOD Complex Interactive Networks/Systems Initiative (CIN/SI)—was undertaken during 1998–2001 to enable critical infrastructures to adapt to a broad array of potential disturbances, including terrorist attacks, natural disasters, and equipment failures.

The CIN/SI overcame the longstanding problems of complexity, analysis, and management for large interconnected systems—and systems of systems—by opening up new concepts and techniques. Dynamical systems, statistical physics, information and communication science, and computational complexity were extended to provide practical tools for measuring and modeling the power grid, cell phone networks, Internet, and other complex systems. For the first time, global dynamics for such systems can be understood fundamentally (Figure 3).

Funded effort included six consortia, consisting of 107 professors and numerous researchers and graduate students in 26 U.S. universities, focused on advancing basic knowledge and developing breakthrough concepts in modeling and simulation, measurement sensing and visualization, control systems, and operations and management. A key concern was the avoidance of widespread network failure due to cascading and interactive effects—to achieve this goal, technical objectives were defined in three broad areas:

- ✔ modeling: understanding the "true" dynamics—to develop techniques and simulation tools that help build a basic understanding of the dynamics of complex infrastructures
- ✔ measurement: knowing what is or will be happening—to develop measurement techniques for visualizing and analyzing large-scale emergent behavior in complex infrastructures
- ✔ management: deciding what to do—to develop distributed systems of management and control to keep infrastructures robust and operational

In all, more than 300 technical papers have been published to date, and 19 promising technologies have been extracted from CIN/SI findings for commercial development. These results address diverse areas, including electricity grid analysis and control, Internet communications and security, manufacturing process control, command and control networks, traffic flow over highway nets, long-term design of critical infrastructures, and integrated assessment of design and policies in a global context. CIN/SI results also addressed the difficult qualitative aspects of modeling the bounded rationality of the human participants in complex systems. Such analysis is critical because humans are the components in any system most susceptible to failure and the most adaptable in managing recovery. Together, these results provide an initial technical foundation for projecting key dynamics on a global scale.

CIN/SI has developed, among other things, a new vision for the integrated sensing, communications, and control of the power grid. Some of the pertinent issues are why/how to develop controllers for centralized versus decentralized control and issues involving adaptive operation and robustness to disturbances that include various types of failures. As expressed in the July 2001 issue of *Wired* magazine: "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." The technologies included, for example, the concept of self-healing electricity infrastructure that is now part of CEIDS, and the methodologies for fast look-ahead simulation and modeling, adaptive intelligent islanding, and strategic power infrastructure protection systems are of special interest for improving grid security from terrorist attack.

Conclusions: Toward a Secure and Efficient Infrastructure

How to control a heterogeneous, widely dispersed, yet globally interconnected system is a serious technological problem in any case. It is even more complex and difficult to control it for optimal efficiency and maximum benefit to the ultimate consumers while still allowing all its business components to compete fairly and freely. A similar need exists for other infrastructures, where future advanced systems are predicated on the near perfect functioning of today's electricity, communications, transportation, and financial services.

Creating a smart grid with self-healing capabilities is no longer a distant dream; we've made considerable progress. But considerable technical challenges as well as several economic and policy issues remain to be addressed; these include:

- ✔ What threat level is the industry responsible for? And what does government need to address?
- ✔ Will market-based priorities support a strategically secure power system? Who will pay for it and what are the economic incentives for such investments?
- ✔ What overall system architecture is most conducive to maintaining security?
- ✔ Our society has a short attention span and shifting memory in response to energy crises because, typically, we put out the "biggest fires" of the day as they occur. Energy policy and technology development require long-term commitments as well as sustained and patient investments in technology creation and development of human capital.

To address these and other vulnerabilities, the electric power industry and all pertinent public and private sectors must work together with other critical infrastructure stakeholders. Given economic, societal, and quality-of-life issues and the ever-increasing interdependencies among infrastructures, a key challenge before us is whether the electricity infrastructure will evolve to become the primary support for the 21st century's digital society—a smart grid with self-healing capabilities—or be left behind as a 20th century industrial relic?

Acknowledgments

I express my gratitude to the guest editor of this special issue, Prof. Mohammad Shahidehpour, for his encouragement and continued interest in this subject. 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.

For Further Reading

M. Amin, "North America's electricity infrastructure: Are we ready for more perfect storms?," *IEEE Security Privacy Mag.*, vol. 1, no. 5, pp. 19–25, Sept./Oct. 2003.

M. Amin, "Toward self-healing energy infrastructure systems," *IEEE Computer Applicat. Power Mag.*, vol. 14, no. 1, pp. 20–28, Jan. 2001.

Committee hearing of the House Committee on Energy and Commerce, "Blackout 2003, How did it happen and why?" Sept. 3–4, 2003 [Online]. Available: http://energycommerce.house.gov

DOE, "National transmission grid study," U.S. Department of Energy, May 2002 [Online]. Available: http://tis.eh.doe.gov/ntgs/gridstudy/main_screen.pdf.

EPRI, "Complex Interactive Networks/Systems Initiative: Final summary report: Overview and summary final report for joint EPRI and U.S. Department of Defense University Research Initiative, EPRI. Palo Alto, August 2004.

EPRI, Electricity Infrastructure Security Assessment, vol. I-II, EPRI, Palo Alto, CA, Nov. /Dec. 2001.

EPRI, Electricity Technology Roadmap: Synthesis Module on Power Delivery System and Electricity Markets of the Future. EPRI, Palo Alto, July 2003

F.F. Hauer and J.E. Dagle, *Review of Recent Reliability Issues and System Events*, Consortium for Electric Reliability Technology Solutions, Transmission Reliability Program, Office of Power Technologies, U.S. DOE, Aug. 30, 1999.

National Science Foundation, Division of Science Resources Statistics, "Research and Development in Industry: 2000," Arlington, VA (NSF 03-318), June 2003, http://www.nsf.gov/sbe/srs/nsf03318/pdf/taba19.pdf.

Biography

Massoud Amin is professor of electrical and computer engineering, directs the Center for the Development of Technological Leadership (CDTL), and holds the HW Sweatt Chair in Technological Leadership at the University of Minnesota. Before joining the University of Minnesota in March 2003, he was with the Electric Power Research Institute (EPRI), where he coined the term "self-healing grid," and led the development of more than 19 technologies being transferred to industry. After September 11 he directed all security-related research and development and twice received Chauncey Awards at EPRI, the institute's highest honor. Dr. Amin has worked with military, governmental, universities, companies and private agencies, focusing on theoretical and practical aspects of reconfigurable and self-repairing controls, infrastructure security, risk-based decision making, system optimization, and differential game theory for aerospace, energy, and transportation applications. He is a member of the Board on Infrastructure and the Constructed Environment (BICE) at the U.S. National Academy of Engineering and a senior member of IEEE. Dr. Amin received his B.S. (cum laude) and M.S. degrees in electrical and computer engineering from the University of Massachusetts, Amherst, and M.S. and D.Sc. degrees in systems science and mathematics from Washington University. For additional publications see http://cdtlnet.cdtl.umn.edu/amin.html