Scanning the Technology

Energy Infrastructure Defense Systems

MASSOUD AMIN, SENIOR MEMBER, IEEE

Energy infrastructure faced with deregulation and coupled with interdependencies with other critical infrastructures and increased demand for high-quality and reliable electricity for our digital economy is becoming more and more stressed. The occurrence of several cascading failures in the past 40 years has helped focus attention on the need to understand the complex phenomena associated with these interconnected systems and to develop defense plans to protect the network against extreme contingencies caused by natural disasters, equipment failures, human errors, or deliberate sabotage and attacks.

With dramatic increases in interregional bulk power transfers and accelerating diversity of transactions among parties, the electric power grid is being used in ways for which it was not originally designed. As the power grids become heavily loaded with long-distance transfers, the already complex system dynamics become even more important. The potential for rare events but high-impact cascading phenomena represent just a few of many new science and technology challenges. We focus on the lessons learned as well as challenges associated with accomplishing these missions, including recent hardware, software, applications, and algorithmic developments.

Keywords*—Critical infrastructure protection, electric power grid, emergency control, infrastructure defense plans, protection against rare events and extreme contingencies.*

I. INTRODUCTION

Secure and reliable operation of the energy infrastructure and other critical systems are 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 massive power outages in the United States, Canada, the United Kingdom, and Italy in 2003 underscored electricity infrastructure's vulnerabilities [1]–[16]. 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?

In the aftermath of the tragic events of 11 September 2001, there are increased national and international concerns about the security and robustness of critical infrastructures in response to evolving spectra of threats. The sources of vulnerability include natural disasters (e.g., earthquakes, hurricanes, winter storms), equipment failures, human errors, or deliberate sabotage and attacks. In addition, "dual use" technologies will be addressed, including improvements to the system that would improve the overall security/resilience to other modes of failures and disasters, such as floods, ice storms, earthquakes, etc.

Virtually every crucial economic and social function depends on the secure, reliable operation of energy, telecommunications, transportation, financial, and other infrastructures. The Internet, computer networks, and our digital economy have increased the demand for reliable and disturbance-free electricity; banking and finance depends 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. Links between the power grid and telecommunications and between electrical power and oil, water, and gas pipelines continue to be a linchpin of energy supply networks. This strong interdependence means that an action in one part of one infrastructure network can rapidly create global effects by cascading throughout the same network and even into other networks.

The potential ramifications of network failures have never been greater, as the transportation, telecommunications, oil and gas, banking and finance, and other infrastructures depend on the continental power grid to energize and control their operations.

Over the last century, various thrusts of power systems have continued to present numerous theoretical and practical challenges to the electrical engineering community ranging from control of electric motors to operation of electric

Manuscript received April 30, 2002; revised February 27, 2005.

The author is with the Center for the Development of Technological Leadership and the Department of Electrical and Computer Engineering, University of Minnesota, Minneapolis, MN 55454 USA (e-mail: amin@umn.edu).

Digital Object Identifier 10.1109/JPROC.2005.847257

power grid. Challenges persist, including modeling, prediction, simulation, cause and effect relationships, analysis, optimization, control and restoration of a large-scale multilayered system composed of a heterogeneous mixture of dynamic, interactive, and often nonlinear entities, unscheduled discontinuities, and numerous other significant effects.

The occurrence of several cascading failures in the past 40 years has helped focus attention on the need to understand the complex phenomena associated with these interconnected systems and to develop defense plans to protect the network against extreme contingencies. With dramatic increases in interregional bulk power transfers and accelerating diversity of transactions among parties, the electric power grid is being asked to respond in ways for which it was not originally designed. Grid congestion and atypical power flows are increasing, while customer expectations of reliability are rising to meet the needs of a pervasively digital world.

Furthermore, as the power grids become heavily loaded with long-distance transfers, the already complex system dynamics become even more important. The potential for rare events but high-impact cascading phenomena represent just a few of many new science and technology concepts that are under development. Analysis and modeling of interdependent infrastructures (e.g., the electric power, together with protection systems, telecommunications, oil/gas pipelines, and energy markets) is especially pertinent.

The North American power 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 [10]–[17].

Through the North American electricity infrastructure, every user, producer, distributor, and broker of electricity buys and sells, competes and cooperates in an "electric enterprise." Every industry, every business, every store, and every home is a participant, active or passive, in this continent-scale conglomerate. 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 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. An upcoming special issue of the PROCEEDINGS OF THE IEEE, guest edited by Prof. M. Ilic, will focus on policy and market issues. In this issue, we shall focus mainly on defense system challenges and their application.

II. THE ELECTRICITY ENTERPRISE: TODAY AND TOMORROW

Possibly the largest machine in the world, the 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 either are 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 currently 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, state regulators are moving toward permitting and encouraging a competitive market in electric power.

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%. These are the most visible parts of a larger and growing U.S. energy crisis, which is the result of years of inadequate investments in the infrastructure. According to Electric Power Research Institute (EPRI) analyses, from 1995 to the present, the amortization/depreciation rate exceeds utility construction expenditures (Fig. 1).

A. North American Electricity Infrastructure Vulnerabilities and Cost of Cascading Failures

Attention to the grid has gradually increased after several cascading failures. The 10 August 1996 blackout cost was

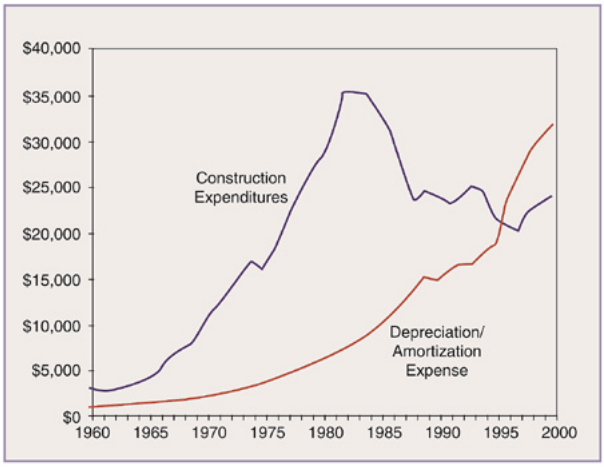

Fig. 1. Since the "crossover" point in about 1995, utility construction expenditures have lagged behind asset depreciation. This has resulted in a mode of operation of the system analogous to "harvesting far more rapidly than planting new seeds" while demand (load) continues to increase at about 2% per year (data provided by Edison Electric Institute (EEI); graph courtesy of EPRI).

over $1.5 billion and included all aspects of interconnected infrastructures and even the environment. Most recently, the 14 August 2003 outage is estimated to have a cost in the range of $6 billion–$10 billion. Past disturbances provide some idea of how cascading failures work.

- November 1965—A cascaded system collapse blackout in ten states in the northeastern United States 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, FL, lost electricity.
- July 1977—In New York's suburbs, lightning caused overvoltages and faulty protection devices, which caused 10 million people to lose power for over 24 h, resulting in widespread looting, over 4000 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 h.
- March 1982—Over 900 000 lost power for 1.5 h 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. The resulting short circuit caused blackouts for 2 million customers in 14 states for approximately 6 h.
- 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 U.S. 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, CA, Bay Area blackout.
- July 1999—New York City blackout caused 300 000 people to be without power for 19 h.
- 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.
- Northeastern United States and Canada cascading outages on 14 August 2003.

III. 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 [7]–[11], [17]. According to data from the North American Electric Reliability Council (NERC) and analyses from the 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 7 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 [1], [3]–[6], [10], [11], [17], [23].

Coupling these analyses with diminished infrastructure investments, and noting that the crossover point for the utility construction investment versus depreciation occurred in 1995 (Fig. 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 periods 1991–1995 and 1996–2000 (Fig. 2). Based on the EPRI's analyses [1], [15] of data in the NERC's Disturbance Analysis Working Group (DAWG) database [1], [10], [11], 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 size 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

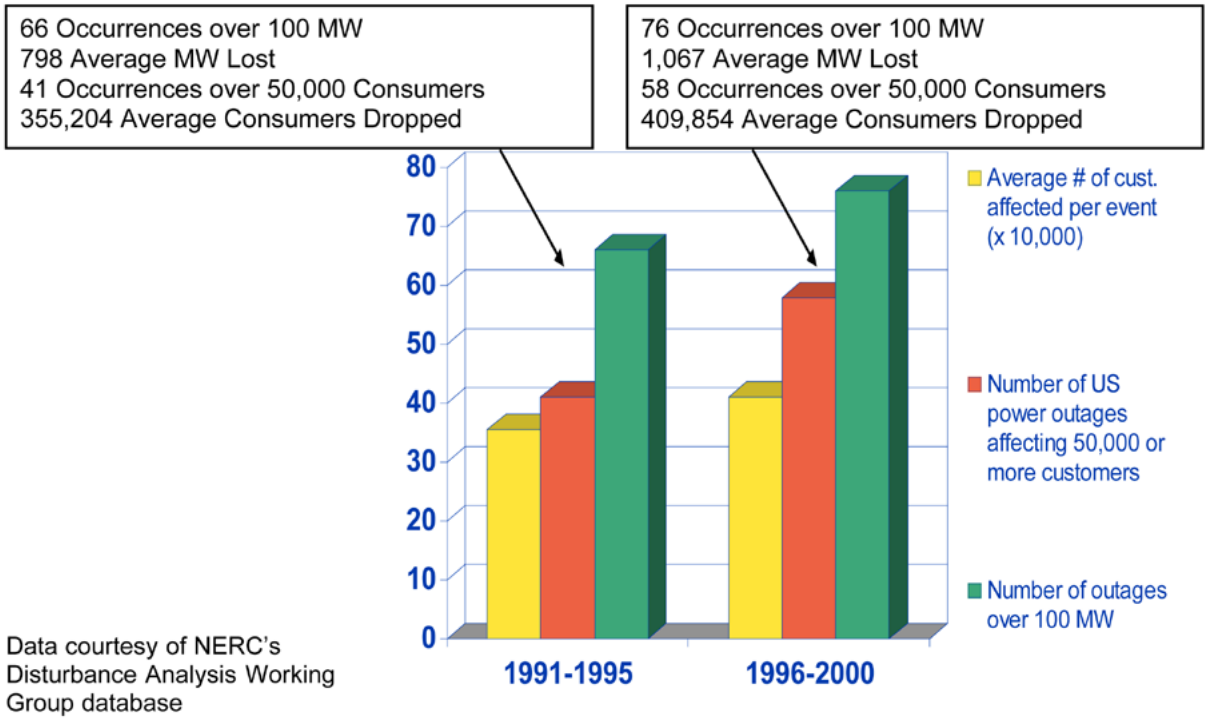

Fig. 2. Increasing frequency and size of U.S. power outages 100 MW or more (1991–1995 versus 1996–2000), affecting 50 000 or more consumers per event. Generally, a relatively small number of U.S. consumers experience a large number of outages; conversely, outages that affect a large number of consumers 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).

1991 to 1995 to 1067 MW from 1996 to 2000 (Fig. 2) [1], [10], [11], [15]–[17].

IV. Brief Overview of System Operation

At its most fundamental level, the electricity infrastructure form a vertically integrated hierarchical network consisting of the generation layer (noted above) and then three network levels [18]. The first is the *transmission* network, which is 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 subtransmission level. The second level is *subtransmission*, which consists of 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. Finally, the third network level is *distribution*, which is 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.

In a large interconnected power system, security is primarily focused on transient and dynamic stability considerations. As such, the main concerns are on the loss of generation or power import, the loss of transmission lines in heavily loaded power transfer interfaces, and the possibility of undamped or growing oscillations. These events have time scales of 0.1–10 s.

Several utilities and energy companies have installed dynamic recording devices capable of storing measured voltage, current, and frequency data at typically 6–30 samples per second. Based on the recorded data, an event analyzer has been developed that is able to classify the disturbances. The scheme identifies single-event disturbances very reliably. More investigation is required to develop a reliable identification scheme for multiple-event disturbances.

Several pertinent theories on power system operating conditions have been provided in the literature; these contributions not only provide mathematical foundations but also include some guidance on how to measure and adapt to disturbances. A power system can be characterized as having multiple states, or "modes," during which specific operational and control actions and reactions are taking place:

- *normal mode:* economic dispatch, load frequency control, maintenance, forecasting, etc.;
- *disturbance mode:* faults, instability, load shedding, etc.;
- *restorative mode:* rescheduling, resynchronization, load restoration, etc.

In the normal mode, the priority is on economic dispatch, load frequency control, maintenance, and forecasting. In the disturbance mode, attention shifts to faults, instability, and load shedding. In the restorative mode, priorities include rescheduling, resynchronization, and load restoration. Some authors include an alert mode before the disturbance actually

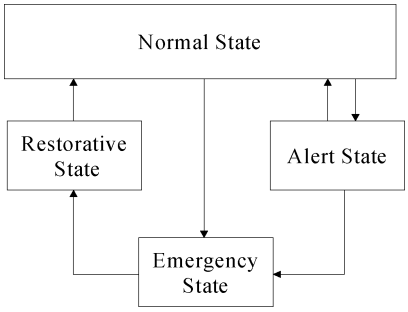

Fig. 3. Four states of a power system.

affects the system; DyLiacco [19] classified power system operating states into normal, emergency and restorative. The concept was extended by Cihlar *et al.* [31] by adding an alert state (see Fig. 3).

Others add a system failure mode before restoration is attempted [20]; Fink and Carlsen further extended the classification by dividing the emergency state into two separate states, emergency and *in extremis*, based on system integrity and balance between generation and load. Another contribution was provided by Zaborszky *et al.* [52], who subdivided the emergency state into three crises (stability, viability, and integrity) to bring dynamics and time-frame characteristics into consideration. Stability emergencies include transient and oscillatory instability, which occur in time frames of a few to tens of seconds. Viability emergencies are longer term operation contingencies, such as voltage instability which may last for several minutes to even hours such as the precursor signatures in the reactive power during the August 2003 northeastern United States–Canada blackout.

Schulz and Price [46] first addressed the issue of emergency identification by proposing emergency classification schemes with four dimensions: system integrity, branch loading, active power balance, and reactive power balance. An emergency detector was proposed that sensed local variables (such as voltages, power, and frequency), processed the data, compared them to *a priori* analysis results, and would initiate appropriate control actions if necessary. Besides these many operational, spatial, and energy levels, power systems are also multiscaled in the time domain, from nanoseconds to decades, as shown in Table 1. The relative time of action for different types of events, from normal to extreme, varies depending on the nature and speed of the disturbance and the need for coordination.

There are a number of other contributing factors that undermine system security and exacerbate blackouts; these include interconnection mismatches, unavailability of reactive support, and lack of coordinated response among control areas. Each region focuses primarily on its own transmission system. Each of the individual parts can be very reliable, yet the total connected system may not be as reliable. While accounting systems have boundaries, electric power and critical communications do not obey these boundaries. Very often, intertie separations are not preplanned for severe emergencies, leaving the decision and system stabilization response to the operators at the time that the operators have many other responsibilities, including coordination with neighboring system operators, verification of equipment rating and status, identifying corrective measures, etc.

With advances in satellite, communications, and computers technologies several utilities have installed or are in the process of installing phasor measurement units (PMU). These devices are also known by other names, such as digital frequency recorders (DFR) and dynamic swing recorders (DSR). Some older units do not have global positioning system (GPS) clocks; therefore, their data is not synchronized with other monitors. PMUs have been installed at the AEP service area [49], in the Western Electricity Coordinating Council (WECC) under the Wide-Area Measurement Systems (WAMS) project [39], and in the New York area; at New England Independent System Operator (ISO-NE) has installed DSR devices.

As a subset, disturbance classification lends itself to the ability to be able to react quickly or even predict events. At the very least, a "snapshot" of the event will have been taken. This will mean that no event will go unnoticed. In the past, events have gone by unnoticed. Furthermore, the ability to predict and react would indicate that problems could be detected and mitigated much sooner. A system operator could be trained accordingly while taking into account both communication delays and computer server status.

To develop an integrated security analysis, metric, and the corresponding states, it is necessary to understand, measure and model each security monitoring "agent's" context. In particular, we need to know how each agent can and should affect monitoring and operations. The above state transition diagram—including its modes—is not sufficient unless we incorporate the above metrics and map the above into a unique state. In doing so, we need higher resolution views of the electric grid, its communication and computer network, etc., from each agent's perspective. This will not only benefit the system operation and its security but will also provide a framework for understanding, describing, and operating a distributed system in the restructured environment.

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.

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. 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. Increased use of electronic automation raises significant issues regarding the adequacy of operational security: 1) reduced personnel at remote sites makes them more vulnerable to hostile threats; 2) interconnection of 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; 3) use of networked

Table 1
Time Hierarchy of Power Systems

ACTION / OPERATION	TIME FRAME
Wave effects (fast dynamics, lightning caused overvoltages)	Microseconds to milliseconds
Switching overvoltages	Milliseconds
Fault protection	100 milliseconds or a few cycles
Electromagnetic effects in machine windings	Milliseconds to seconds
Stability	60 cycles or 1 second
Stability Augmentation	Seconds
Electromechanical effects of oscillations in motors & generators	Milliseconds to minutes
Tie line load frequency control	1 to 10 seconds; ongoing
Economic load dispatch	10 seconds to 1 hour; ongoing
Thermodynamic changes from boiler control action (slow dynamics)	Seconds to hours
System structure monitoring (what is energized & what is not)	Steady state; on-going
System state measurement and estimation	Steady state; on-going
System security monitoring	Steady state; on-going
Load Management, load forecasting, generation scheduling	1 hour to 1 day or longer; ongoing.
Maintenance scheduling	Months to 1 year; ongoing.
Expansion planning	Years; ongoing
Power plant site selection, design, construction, environmental impact, etc.	2 years or longer

electronic systems for metering, scheduling, trading, or e-commerce imposes numerous financial risks implied by use of this technology.

Any complex dynamic infrastructure network typically has many layers and decision-making units and is vulnerable to various types of disturbances. Effective, intelligent, distributed control is required that would enable parts of the networks to remain operational and even automatically reconfigure in the event of local failures or threats of failure. The paper in this issue by Shahidehpour and Wiedman, "Natural Gas Infrastructure Protection for Supplying the Electric Power Plants," focuses on the interdependencies with markets and gas pipelines. The restructuring of electricity has introduced new risks associated with the security of natural gas infrastructure on a significantly large scale, which entails changes in physical capabilities of pipelines, operational procedures, sensors and communications, contracting (supply and transportation), and tariffs. The authors discuss the essence of protecting the natural gas infrastructure for supplying the ever-increasing number of gas-powered units and its impact on the reliability of the electricity infrastructure.

To extend this further to the larger interconnected systems incorporating the power system, protective system, fuel supply infrastructure, and the communications system, methods are needed to overcome the computational complexity introduced by the massive size and interconnectedness of these complex systems.

V. 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 11 September 2001 attacks highlights three different kinds of potential threats to the U.S. electricity infrastructure [1]–[3], [13].

- **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 are 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.

VI. The Dilemma: Security and Quality Needs

The specter of terrorism raises a profound dilemma for the electric power industry: How to make the electricity in-

frastructure 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 man-made 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* [15], [16]. These result from open 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.

VII. 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 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 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.

VIII. 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.
- WAMS, which integrate advanced sensors with satellite communication and time stamping using 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: WAMS, OASIS, Supervisory Control and Data Acquisition (SCADA) systems, and 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; FCLs; sensing and coordinated control of multiple FACTS.
- Intelligent electronic devices with security provisions built in—combining sensors, computers, telecommunications units, and actuators; integrated sensors; 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.

IX. Western States Power Crises: A Brief Overview of Lessons Learned

An example of "urgent" opportunities is within the now seemingly calm California energy markets; the undercurrents that led to huge price spikes and considerable customer pain in recent years are yet to be fully addressed and alleviated. Such "perfect storms" may appear once again during another cycle of California economic recovery and growth. The California power crisis in 2000 was only the most visible part of a larger and growing U.S. 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.[1]

California is a good downside example of a societal testbed for the ways that seemingly "good" theories can fail in the real world. For example, inefficient markets provide inadequate incentives for infrastructure investment:

- boom–bust cycle may be taking shape in generation investment;
- transmission investment running at one-half of 1975 level;

[1]See EPRI's Western States Power Crises white paper [Online]. Available: http://www.epri.com/WesternStatesPowerCrisisSynthesis.pdf

- congestion in transmission network is rising, as indicated by increase of number of transmission loading reliefs (TLRs) during the last three years.

Cost of market failure can be also very high; as indicated by the exercise of market power in California during summer of 2000, which cost consumers $4 billion initially, while the ongoing intermediate loss to businesses may well be considerably higher. For a pertinent analysis/survey, please see the May 1st 2004 issue of the *Economist* magazine:[2]

> To add to their woes, Californian business leaders now have to face up to a problem for which they share some of the blame: infrastructure. A business has to have access to electricity, water, transport and decent staff. Yet the entrepreneurial classes have been extremely reluctant to let the state spend money on any of these items. Most of the state's physical infrastructure dates back to the 1960s …

More specifically regarding the electricity underinvestment and persisting undercurrents, very specific "investments" by the state were made, on the order of $10 billion, paid to subsidize (hold down) electricity prices, and to bail out bankrupt companies through long-term noncompetitive contracts which did not address the undercurrents and shortcomings of the earlier policies. As the *Economist* points out:

> As for energy, when Californians suffered repeated blackouts three years ago, Mr. Davis blamed out-of-state companies for defrauding consumers. There was a grain of truth in that, but the main causes were, first, the state's adamant refusal to let anybody build power plants and, second, a botched attempt at "deregulation": ingeniously, California had devised a system that held consumer prices stable but allowed wholesale prices to fluctuate. Mr. Davis eventually managed to "solve" the crisis by partially nationalizing the industry and signing expensive long-term contracts with the power companies, but neither of the underlying causes of the energy crisis have been tackled. Mr. Schwarzenegger wants to renegotiate the contracts; if he does not get his way, another such crisis is likely to blow up in the next few years (and it takes at least two years to build a power station). The longer you look at the energy crisis, the more amazing it seems. It brought the state to a halt, enraged consumers and arguably cost Mr. Davis his job (his reputation never really recovered). Yet nothing much has been done to stop the same thing happening all over again. It makes you wonder how the state will cope with the far greater challenges posed to its human infrastructure by the arrival of 10 million people over the past decade, most of them poor and uneducated, and the transformation of its demographic make-up.

To address these issues there are both tactical as well as strategic needs; for example, the so-called low-hanging fruits to improve transmission networks include the following.

- Deploy existing technologies to improve use of already in place transmission assets (e.g., FACTS, dynamic thermal circuit rating, and energy storage-peak shaving technologies). For example, through the integration of load management technologies shaving nearly 5,000 MW, which amounts to about 10% of total demand, combined with a more precise control enabled by the use of FACTS devices, which enable nearly 50% more transfer capability over existing transmission lines.
- Develop and deploy new technologies to improve transmission reliability and throughput (e.g., low sag composite conductors, high temperature superconducting cables, extra high voltage ac and dc transmission systems, and hierarchical control systems).
- Improve real-time control of networks via monitoring and data analysis of dynamic transmission conditions.
- Develop and deploy self-healing grid tools to adaptively respond to overload and emergency conditions.
- Digital control of the power delivery network (reliability, security, and power quality).
- Integrated electricity and communications for the user.
- Transformation of the meter into a two-way energy/information portal.
- Integration of distributed energy resource into the network.
- The complex grid can operate successfully *if* technology is deployed and operated in an integrated manner (there is no "silver bullet").

In addition, longer term strategic considerations must be addressed; they include:

- Greater fuel diversity—regional and national priorities.
- Risk-assessment of long-term U.S. reliance—analysis of the value of risk management through fuel diversity.
- Introduce time-varying prices and competitive market dynamics for all customers.
- Create a planning process and *in silico* testing of designs, devices and power markets.
- Model market efficiencies, environmental constraints, and renewables.
- Develop advanced EM threat detection, shielding, and surge-suppression capabilities.
- Develop the tools/ procedures to ensure a robust and secure marketplace for electricity.
- Develop the portfolio of advanced power generation technologies to assure energy security.
- Transmission network expansion and RTOs. For example, would an RTO complement a competitive wholesale power market and result in a sustainable and robust system? How large should they be?
- Comprehensive architecture for power supply and delivery infrastructure that anticipates rapidly escalating demands of digital society.
- Enable self-healing power delivery infrastructure.
- Significant investment in R&D, transmission, generation, and conservation resources are needed.
- Incentives for technology innovation and accountability for R&D.

[2][Online]. Available: http://www.economist.com/surveys/displayStory.cfm?story_id=2 609 467

- Revitalize the national public/private electricity infrastructure partnership needed to fund the "self-healing grid" deployment.
- The "law of unintended consequences" should be considered in crafting any solution.

Having discussed the above technology-intensive "push," we must also consider the fact that adoption of new technologies often creates equally new markets. For example, wireless communication creates the market of spectrum, and broad-band technologies create the market of bandwidth. Reduced regulation of major industries has required new markets wherever the infrastructure is congested: airlines compete for landing rights, power generators for transmission rights, oil and gas producers for pipeline capacity.

From a national perspective, a key grand challenge before us is, how do we redesign, retrofit, and upgrade the nearly 240 000 miles of electromechanically controlled system into a smart self-healing grid that is driven by a well-designed market approach?

In addressing this challenge, as technology progresses, and the economy becomes increasingly dependent on markets, infrastructures such as electric power, oil/gas/water pipelines, telecommunications, financial, and transportation networks becomes increasingly critical and complex. In particular, since it began in 1882, electric power has grown to become a major industry essential to a modern economy. From electric lights, elevators, and air conditioning to CD players, faxes, and computers, economical and reliable supplies of electricity are essential to support a wide range of services and activities in our society. Connecting almost every home, office, and factory in the developed world, the electric power system has fundamentally transformed the growth, productivity, living standards, and expectations of modern society.

Over the past two decades, governments around the globe have introduced increasing amounts of competition into network industries. With the advent of restructuring in the electric power industry, we are witnessing the onset of a historical transformation of the energy infrastructure in the context of global trends:

- increasing electricity demand as a consequence of economic and population growth;
- technological innovations in power generation, delivery, control, and communications;
- increasing public acceptance of market mechanisms;
- growing public concerns about environmental quality and depletion of exhaustible resources.

Services previously supplied by vertically integrated, regulated monopolies are now provided by multiple firms. The transition to competition has fundamentally altered important aspects of the engineering and economics of production. The long-term socioeconomic impacts of such a transformation will be huge, and the tasks are just as daunting, going well beyond the existing boundary of knowledge. This transformation has also created impediments to more efficient operation that can be best overcome through collaborative research between economists and engineers. The crisis in the California electricity market has exposed some of the problems.

This presents unique opportunities and challenges. Clearly, this change will have far-reaching implications for the future development of the electricity industry. More fundamentally, as we look beyond the horizon, this change will further power the information revolution and increasing global interdependence. The long-term socioeconomic impacts of such a transformation will be huge, and the tasks are just as daunting, going well beyond the boundary of existing knowledge.

To meet such a challenge, collaborative research between engineers and economists is critical to provide a holistic and robust basis that will support the design and management of complex technological and economic systems in the long term. The electric power industry offers an immediate opportunity for launching such research, as new ways are being sought to improve the efficiency of electricity markets while maintaining the reliability of the network. Complexity of the electric power grid combined with ever more intricate interactions with markets offers a plethora of new and exciting research opportunities.

X. 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 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 11 September 2001, the U.S. President's Commission on Critical Infrastructure Protection in 1997 highlighted the growing concern [8]. 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,

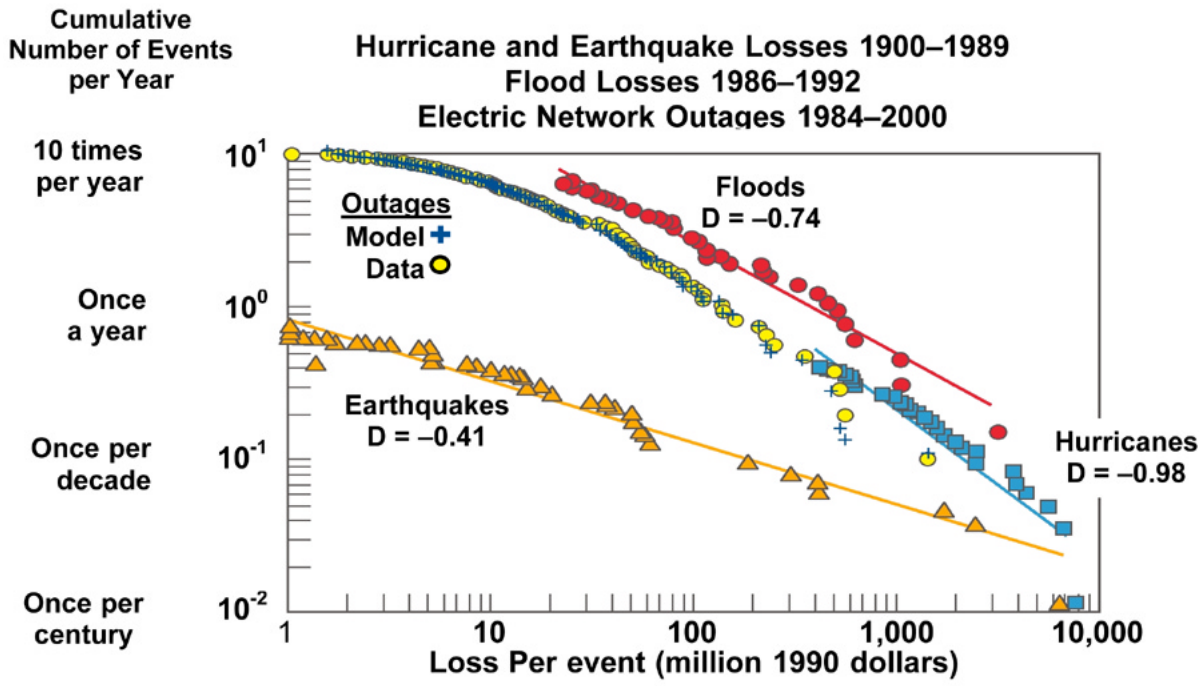

Fig. 4. Understanding complex systems and global dynamics. Economic losses from disasters were found to follow a power law distribution—for hurricanes, floods, earthquakes, and even electrical outages. Fundamental power law distributions also were found for forest fires, Internet congestion, and other systems. CIN/SI results such as these translate in new approaches for optimizing complex systems in terms of productivity and robustness to disaster. (Source: the EPRI/DOD Complex Interactive Networks/Systems Initiative.)

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 long-standing 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, the Internet, and other complex systems. For the first time, global dynamics for such systems can be understood fundamentally (Fig. 4).

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.

As part of enabling a self-healing grid, we have developed adaptive protection and coordination methods that minimize impact on the whole system performance (load dropped as

well as robust rapid restoration). There is a need to coordinate the protection actions of such relays and controllers with each other to achieve overall stability; single controller or relay cannot do all, and they are often tuned for worst cases, therefore, control action may become excessive from a system wide perspective. On the other hand, they may be tuned for best case, and then the control action may not be adequate. This calls for a coordinating protection and control—neither agent, using its local signal, can by itself stabilize a system; but with coordination, multiple agents, each using its local signal, can stabilize the overall system. It is important to note that the key elements and principles of operation for interconnected power systems were established in the 1960s, prior to the emergence of extensive computer and communication networks.

Computation is now heavily used in all levels of the power network—for planning and optimization, fast local control of equipment, processing of field data. But coordination across the network happens on a slower time scale. 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 emergencies.

From a broader perspective, any critical national infrastructure typically has many layers and decision-making units and is vulnerable to various types of disturbances. Effective, intelligent, distributed control is required that would enable parts of the constituent networks to remain operational and even automatically reconfigure in the event of local failures or threats of failure. In any situation subject to rapid changes, completely centralized control requires multiple, high-data-rate, two-way communication links, a powerful central computing facility, and an elaborate operations control center. But all of these are liable to disruption at the very time when they are most needed (i.e., when the system is stressed by natural disasters, purposeful attack, or unusually high demand).

When failures occur at various locations in such a network, the whole system breaks into isolated "islands," each of which must then fend for itself. With the intelligence distributed, and the components acting as independent agents, those in each island have the ability to reorganize themselves and make efficient use of whatever local resources remain to them in ways consonant with the established global goals to minimize adverse impact on the overall network. Local controllers will guide the isolated areas to operate independently while preparing them to rejoin the network, without creating unacceptable local conditions either during or after the transition. A network of local controllers can act as a parallel, distributed computer, communicating via microwaves, optical cables, or the power lines themselves and intelligently limiting their messages to only that information necessary to achieve global optimization and facilitate recovery after failure.

Over the last seven years, our efforts in this area have developed, among other things, a new vision for the integrated sensing, communications, protection, and control of the power grid. However, instead of performing *in vivo* societal tests which can be disruptive, we have performed extensive "wind-tunnel" simulation testing (*in silico*) of devices and policies in the context of the whole system along with prediction of unintended consequences of designs and policies to provide a greater understanding of how policies, economic designs and technology might fit into the continental grid, as well as guidance for their effective deployment and operation.

If organized in coordination with the internal structure existing in a complex infrastructure and with the physics specific to the components they control, these agents promise to provide effective local oversight and control without need of excessive communications, supervision, or initial programming. Indeed, they can be used even if human understanding of the complex system in question is incomplete. These agents exist in every local subsystem—from "horseshoe nail" up to "kingdom"—and perform preprogrammed self-healing actions that require an immediate response. Such simple agents already are embedded in many systems today, such as circuit breakers and fuses as well as diagnostic routines. The observation is that we can definitely account for loose nails and save the kingdom.

Another key insight came out of analysis of forest fires, which researchers in the one of the six funded consortia which I led found to have similar "failure-cascade" behavior to electric power grids. In a forest fire, the spread of a spark into a conflagration depends on how close together are the trees. If there is just one tree in a barren field and it is hit by lightning, it burns but no big blaze results. But if there are many trees and they are close enough together—which is the usual case with trees because nature is prolific and efficient in using resources—the single lightning strike can result in a forest fire that burns until it reaches a natural barrier such as a rocky ridge, river, or road. If the barrier is narrow enough that a burning tree can fall across it or it includes a burnable flaw such as a wooden bridge, the fire jumps the barrier and burns on. It is the role of first-response wildland firefighters such as smokejumpers to contain a small fire before it spreads by reinforcing an existing barrier or scraping out a defensible fire line barrier around the original blaze.

Similar results hold for failures in electric power grids. For power grids, the "one-tree" situation is a case in which every single electric socket has a dedicated wire connecting it to a dedicated generator. A lightning strike on any wire would take out that one circuit and no more. But like trees in nature, electrical systems are designed for efficient use of resources, which means numerous sockets served by a single circuit and multiple circuits for each generator. A failure anywhere on the system causes additional failures until a barrier—a surge protector or circuit breaker, say—is reached. If the barrier does not function properly or is insufficiently large, the failure bypasses it and continues cascading across the system.

These preliminary findings suggest approaches by which the natural barriers in power grids may be made more robust by simple design changes in the configuration of the system, and eventually how small failures might be contained by active smokejumper-like controllers before they grow into large

problems. Other research into fundamental theory of complex interactive systems is exploring means of quickly identifying weak links and failures within a system.

CIN/SI has developed, among other things, a new vision for the integrated sensing, communications, and control of the energy infrastructure. 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 [22]: "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 which are now part of EPRI's IntelliGrid. The methodologies for fast look-ahead simulation and modeling, are being developed in the Fast Simulation and Modeling (FSM) program. In addition, integrated probabilistic risk assessment and protection of interdependent infrastructures, along with adaptive intelligent islanding and strategic power infrastructure protection systems, are of special interest for improving grid security from terrorist attack.

XI. Conclusions: Toward a Secure and Efficient Infrastructure

How to sense, control and defend 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 have made considerable progress. The electric power industry offers an immediate opportunity for launching such collaboration, as new ways are being sought to improve the efficiency of electricity markets while maintaining the reliability of the network. But considerable technical challenges as well as several economic and policy issues remain to be addressed, include the following.

- 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. Electricity shall prevail at the quality, efficiency, and reliability that customers demand and are willing to pay for. On the one hand the question is who provides it; on the other hand it is important to note that achieving the grid performance, security, and reliability are a national profitable investment, not a cost burden on the taxpayer. The economic payback is three to seven times and in some cases an order of magnitude greater than the money invested. Further, the payback starts with the completion of each sequence of grid improvement. The issue is not merely who invests money because that is ultimately the public, whether through taxes or kilowatt–hour rates. Considering the impact of regulatory agencies, they should be able to induce the electricity producers to plan and fund the process. That may be the most efficient way to get it in operation. The current absence of a coordinated national decision making is a major obstacle. State's rights, and state public utility commission (PUC) regulations have removed the individual state utility's motivation for a national plan. Investor utilities face either collaboration on a national level, or a forced nationalization of the industry.

In conclusion, it is important to note that some of the failures identified by the Joint U.S.–Canada Task Force that investigated the 14 August 2003 blackout were not technological at all. Rather, many were human operator training issues and failures to perform simple, but time-consuming and expensive, tasks such as tree trimming along transmission right-of-ways. Such failures are readily remedied through greater awareness, improved training, and adequate monetary resources.

Leadership in innovation and R&D is fundamental to U.S. and global prosperity and security. 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?

Acknowledgment

The author developed most of the material and findings presented here while he was at the Electric Power Research Institute (EPRI), Palo Alto, CA. For feedback and support, the author would like to thank numerous colleagues at EPRI, universities, industry, and government agencies who served as reviewers for this special issue and have provided their tireless efforts and leadership.

References

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

[2] ——, "Security challenges for the electricity infrastructure," *IEEE Computer (Special Supplement on Security and Privacy)*, vol. 35, no. 4, pp. 8–10, Apr. 2002.
[3] ——, "Toward self-healing energy infrastructure systems," *IEEE Comput. Appl. Power*, vol. 14, no. 1, pp. 20–28, Jan. 2001.
[4] ——, "Toward self-healing infrastructure systems," *IEEE Computer*, vol. 33, no. 8, pp. 44–53, Aug. 2000.
[5] ——, *IEEE Control Syst. Mag. (Special Issue on Control of Complex Networks)*, vol. 21, no. 6, Dec. 2001.
[6] M. Amin, *IEEE Control Syst. Mag. (Special Issue on Control of Complex Networks)*, vol. 22, no. 1, Feb. 2001.
[7] (2003) Blackout 2003: How did it happen and why?. House Comm. Energy Commerce. [Online]. Available: http://energycommerce.house.gov
[8] (1997) Critical foundations: Protecting America's infrastructures. President's Commission Critical Infrastructure Protection, Washington, DC. [Online]. Available: http://www.ciao.ncr.gov
[9] (2002) National transmission grid study. U.S. Dept. Energy. [Online]. Available: http://tis.eh.doe.gov/ntgs/gridstudy/main_screen.pdf
[10] Annual Energy Outlook 2003. Energy Inf. Admin., Dept. Energy. [Online]. Available: http://www.eia.doe.gov/oiaf/aeo/figure_3.html
[11] *North American Electric Reliability Council (NERC) Disturbance Analysis Working Group (DAWG) Database*. [Online]. Available: http://www.nerc.com/~dawg/
[12] "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," Electric Power Res. Inst. (EPRI), Palo Alto, CA, 2003.
[13] *Electricity Infrastructure Security Assessment*, vol. 1-2, Electric Power Res. Inst. (EPRI), Palo Alto, CA, 2001.
[14] "Communication security assessment for the United States electric utility infrastructure," Electric Power Res. Inst. (EPRI), Palo Alto, CA, 1 001 174, 2000.
[15] *Electricity Technology Roadmap: Synthesis Module on Power Delivery System and Electricity Markets of the Future*, Electric Power Res. Inst. (EPRI), Palo Alto, CA, 2003.
[16] "Electricity technology roadmap: 1999 summary and synthesis," Electric Power Res. Inst. (EPRI), Palo Alto, CA, Tech. Rep. CI-112 677-V1, 1999.
[17] F. F. Hauer and J. E. Dagle, *Review of Recent Reliability Issues and System Events*. Washington, DC: U.S. Dept. Energy, 1999.
[18] Kundur, *Power System Stability and Control*. New York: McGraw-Hill, 1994, EPRI Power System Engineering Series.
[19] T. E. DyLiacco, "The adaptive reliability control system," *IEEE Trans. Power App. Syst.*, pp. 517–561, May 1967.
[20] L. H. Fink and K. Carlsen, "Operating under stress and strain," *IEEE Spectr.*, pp. 48–53, Mar. 1978.
[21] "Research and development in industry: 2000," Div. Sci. Resources Stat., Nat. Sci. Found., Arlington, VA, NSF 03-318, 2003.
[22] S. Silberman. (2001, Jul.) The energy web. *Wired* [Online]. Available: http://wired-vig.wired.com/wired/archive/9.07/juice.html
[23] M. Amin, *Proc. IEEE (Special Issue on Energy Infrastructure Defense Systems)*, vol. 93, no. 5, pp. **<<ED: in pages—???>>–???**, May 2005.
[24] M. Samotyj, C. Gellings, and M. Amin, "Power system infrastructure for a digital society: Creating the new frontiers," in *Proc. GIGRE/IEEE Power Engineering Soc. Symp. Quality and Security of Electric Power Delivery*, 2003, p. 10.
[25] G. E. Boukarim, S. Wang, J. H. Chow, G. N. Taranto, and N. Martins, "A comparison of classical, robust, and decentralized control designs for multiple power systems stabilizers," *IEEE Trans. Power Syst.*, vol. 15, no. 4, pp. 1287–1292, Nov. 2000.
[26] A. Bykhovsky and J. H. Chow, "Dynamic data recording in the New England power system and an event analyzer for the northfield monitor," presented at the VII SEPOPE Conf., Curitiba, Brazil, 2000.
[27] C. A. Canizares and F. L. Alvarado, "Point of collapse and continuation method for large AS/DC systems," *IEEE Trans. Power Syst.*, vol. 8, no. 1, Feb. 1993.
[28] C. Gama, L. Anguist, G. Ingestrom, and M. Noroozian, "Commissioning and operative experience of the imperatriz TCSC for damping power oscillation in the Brazilian north-south interconnection," presented at the VII SEPOPE Conf., Curitiba, Brazil, 2000.
[29] J. H. Chow and K. W. Cheung, "A toolbox for power system dynamics and control engineering education," *IEEE Trans. Power Syst.*, vol. 7, no. 4, pp. 1559–1564, Nov. 1992.
[30] X. Cheng and B. H. Krogh, "Stability constrained model predictive control for nonlinear systems," in *Proc. 36th IEEE Conf. Decision and Control*, vol. 3, 1998, pp. 2091–2096.
[31] T. C. Cihlar, J. H. Wear, D. N. Ewart, and L. K. Kirchmayer, "Electric utility system security," presented at the Amer. Power Conf., 1969.
[32] R. Christie. Power system test case archive. [Online]. Available: http://www.ee.washington.edu/research/pstca
[33] N. Flatabo, R. Ognedal, and T. Carlson, "Voltage stability condition in a power transmission system calculated by sensitivity methods," *IEEE Trans. Power Syst.*, vol. 5, no. 4, pp. 1286–1293, Nov. 1990.
[34] M. Ghandhari, G. Andersson, and I. A. Hiskens, "Control Lyapunov function for controllable series devices," presented at the VII SEPOPE Conf., Curitiba, Brazil, 2000.
[35] J. D. Glover and M. S. Sarma, *Power System Analysis and Design*. Boston, MA: PWS, 1993.
[36] B. Gao, G. K. Morison, and P. Kundar, "Voltage stability evaluation using modal analysis," *IEEE Trans. Power Syst.*, vol. 7, no. 4, pp. 1529–1542, Nov. 1992.
[37] N. G. Hingorani, "Flexible AC transmission," *IEEE Spectr.*, vol. 30, no. 4, pp. 40–45, Apr. 1993.
[38] J. F. Hauer, "Robust damping control for large power systems," *IEEE Control Syst. Mag.*, vol. 9, no. 1, pp. 12–18, Jan. 1989.
[39] J. F. Hauer, D. J. Trudnowski, G. J. Rogers, W. A. Mittelstadt, W. H. Litzenberger, and J. M. Johnson, "Keeping an eye on power system dynamics," *IEEE Comput. Appl. Power*, vol. 10, no. 4, pp. 50–54, Oct. 1997.
[40] IEEE Recommended Practice for Excitation System Models for Power System Stability Studies [Online]. Available: IEEE Standard 421.5-1992
[41] "Dynamic models for steam and hydro turbines in power system studies," *IEEE Trans. Power App. Syst.*, vol. PAS-92, no. 6, pp. 1904–1915, Nov./Dec. 1973.
[42] P. Kessel and H. Glavitsch, "Estimating the voltage stability of a power system," *IEEE Trans. Power Del.*, vol. PWRD-1, no. 3, pp. 346–354, Jul. 1986.
[43] M. K. Pai, "Voltage stability conditions considering load characteristics," *IEEE Trans. Power Syst.*, vol. 7, no. 1, pp. 243–249, Feb. 1992.
[44] M. Pavella and P. G. Murthy, *Transient Stability of Power Systems: Theory and Practice*. New York: Wiley, 1994.
[45] H. E. Pierce, Jr., H. W. Colborn, D. W. Coleman, E. A. Marriage, J. C. Richard, L. J. Rindt, L. J. Rubino, G. W. Stagg, T. P. Traub, J. Vandergrift, C. E. Winn, and C. C. Young, "Common format for exchange of solved load flow data," *IEEE Trans. Power App. Syst.*, vol. PAS-92, no. 6, pp. 1916–1925, Dec. 1973.
[46] R. P. Schulz and W. W. Price, "Classification and identification of power system emergencies," *IEEE Trans. Power App. Syst.*, vol. PAS-103, no. 12, pp. 3471–3479, Dec. 1984.
[47] R. P. Schulz, L. S. VanSlyck, and S. H. Horowitz, "Classification and identification of power system emergencies," in *Proc. IEEE PICA Conf.*, 1989, pp. 49–55.
[48] D. D. Siljak, *Decentralized Control of Complex Systems*. New York: Academic, 1990.
[49] C. W. Taylor, *Power System Voltage Stability*. New York: McGraw-Hill, 1994.
[50] C. W. Taylor and D. C. Erickson, "Recording and analyzing the July 2 cascading outage," *IEEE Comput. Appl. Power*, vol. 10, no. 1, pp. 26–30, Jan. 1997.
[51] F. F. Wu and P. Varaiya, "Coordinated multilateral trade for electric power networks: Theory and implementation," Dept. Elect. Comput. Eng., Univ. California, Berkeley, Working Paper PWP-031, 1995.
[52] J. Zaborszky, K. W. Whang, and K. V. Prasad, "Monitoring, evaluation and control of power system emergencies," in *Proc. Systems Engineering for Power Conf.*, Davos, Switzerland, 1979, Eng. Found. Rep. CONF-790 904-P1.
[53] A. Zobian and M. D. Ilic, "Unbundling of transmission and ancillary services: Part I: Technical issues," *IEEE Trans. Power Syst.*, vol. 12, no. 2, pp. 539–548, May 1997.

Massoud Amin (Senior Member, IEEE) received the B.S. (cum laude) and M.S. degrees in electrical and computer engineering from the University of Massachusetts, Amherst, in 1982 and 1985, respectively, and the M.S. and D.Sc. degrees in systems science and mathematics from Washington University, St. Louis, MO, in 1986 and 1990, respectively.

Before joining the University of Minnesota, Minneapolis, in March 2003, he was with the Electric Power Research Institute (EPRI), where he held positions of increased responsibility including Area Manager of Infrastructure Security, Grid Operations/Planning, Markets, Risk and Policy Assessment, developed the foundations of and coined the term "self-healing grid," and led the development of more than 19 technologies being transferred to industry. After the events of 11 September 2001, he directed all security-related research and development. Prior to October 2001, he served as manager of mathematics and information science at EPRI, where he led strategic R&D in modeling, simulation, optimization, and adaptive control of national infrastructures for energy, telecommunication, transportation, and finance. He is currently Professor of Electrical and Computer Engineering, directs the Center for the Development of Technological Leadership (CDTL), and holds the H. W. Sweatt Chair in Technological Leadership at the University of Minnesota. He has worked with military, government, 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.

Dr. Amin has twice received Chauncey Awards at EPRI, the institute's highest honor. He is a Member of the Board on Infrastructure and the Constructed Environment (BICE) at the U.S. National Academy of Engineering. For additional publications, see http://umn.edu/~amin