North American Electricity Infrastructure:

System Security, Quality, Reliability, Availability, and Efficiency Challenges and their Societal Impacts

Massoud Amin
University of Minnesota

A. Introduction

I was asked to write the chapter on "Societal Pains" caused by outages and major power quality disruptions and their impact on our society. Indeed our national security and digital economy place increased demand for reliable and disturbance-free electricity. The massive power outages in the United States, Canada, UK and Italy in 2003 underscored electricity infrastructure's vulnerabilities [1-11]. 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 de-regulation 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 [9-16].

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. 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 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.

B. 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 multi-scale, multi-component, 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, 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 non-competitive, 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 U.S. increased some 35%, while capacity has increased only 18%. The most visible parts of a larger and growing US 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*).

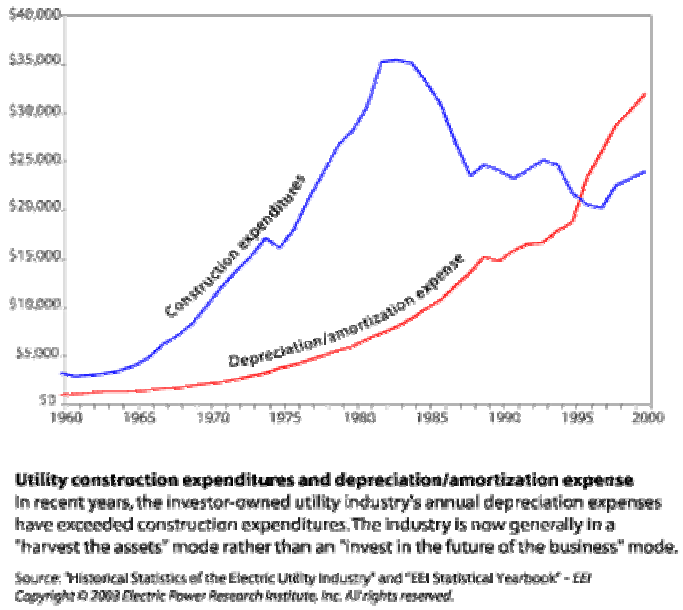

Figure 1: Since the "cross over" point in about 1995 utility construction expenditures have lagged behind asset depreciation. This has resulted in a mode of operation of the system analogous to "harvesting the farm far more rapidly than planting new seeds" (data provided by EEI and graph courtesy of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

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.

C. 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 [6-10, 16]. 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 US Department of Energy (DOE), which requires electric utilities to report system emergencies that include electric service interruptions, voltage reductions, acts of sabotage, unusual occurrences that can affect the reliability of bulk power delivery systems, and fuel problems. [1, 3-5, 9, 10, 16, 22]

Coupling these analyses with diminished infrastructure investments, and noting that the cross-over point for the utility construction investment vs. 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 [1, 14] of data in NERC's Disturbance Analysis Working Group (DAWG) database [1, 9, 10], 41 percent 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

North American electricity infrastructure vulnerabilities and cost of cascading failures

Attention to the grid has gradually increased after several cascading failures. The August 10, 1996 blackout cost was over $1.5 billion and included all aspects of interconnected infrastructures and even the environment. Most recently, the August 13, 2003 outage is estimated to have a cost in the range of $6-$10 billions. Past disturbances in both the power grid give you some idea of how cascading failures work:

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

percent 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 megawatts (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 percent, from 798 MW from 1991 to 1995 to 1067 MW from 1996 to 2000 (Figure 2). [1, 9, 10, 14]

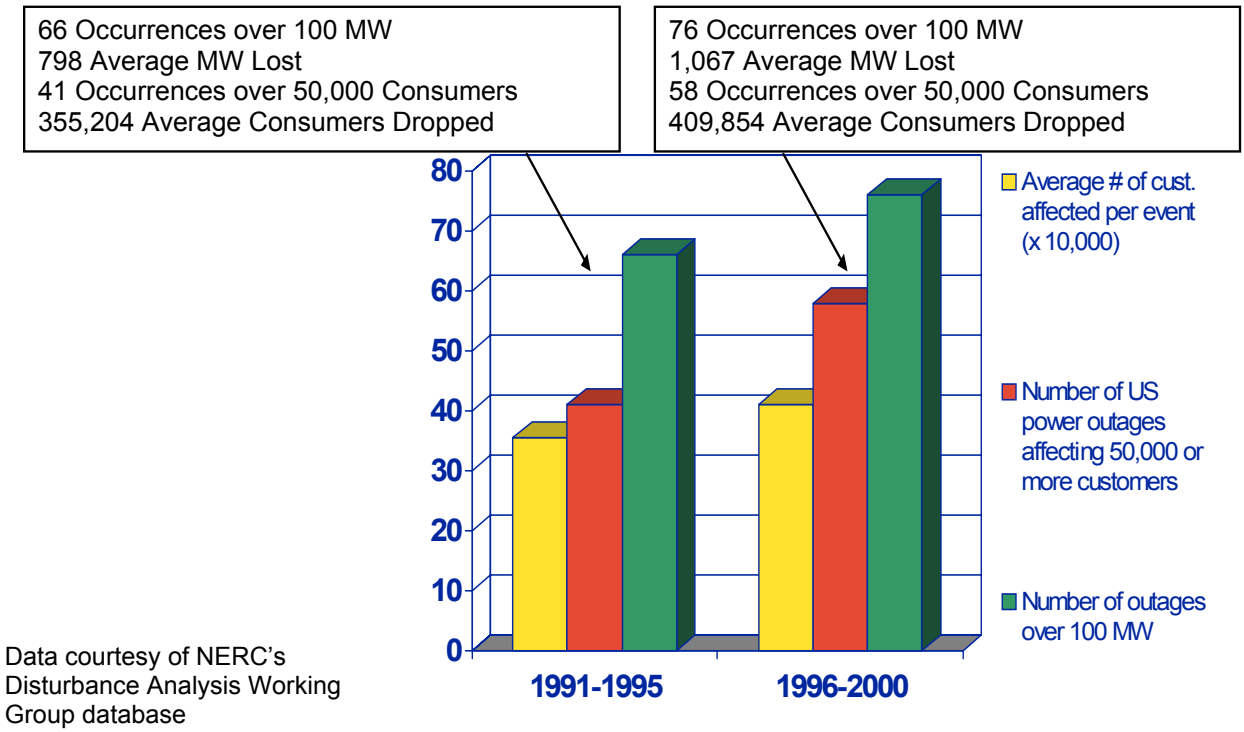

Figure 2: Increasing frequency and size of US power outages 100 MW or more (1991-1995 versus 1996-2000), affecting 50,000 or more consumers per event. Generally, a relatively small number of US consumers experience a large number of outages; conversely, outages that affect a large number of consumers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

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; and
- 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
- This 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

D. 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 11th 2001 attacks highlights three different kinds of potential threats to the US electricity infrastructure [1-2, 3, 12]:

- **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, multi-pronged attack intended to bring down the entire grid in a region of the U.S. 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 to with the intention of damaging computer and/or telecommunications infrastructure.

E. 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 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.

F. 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.

G. 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 over-all 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 percent 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 post Auguts 14th 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 on-line 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-acces 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: Flexible AC Transmission Systems (FACTS); Fault Current Limiters (FCL)
- Intelligent Electronic Devices with security provisions bulit in- combining sensors, computers, telecomm. units, and actuators; integrated sensor; 2-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.

H. 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 parts of a larger and growing US energy crisis that is the result of years of inadequate investments in the infrastructure.

For example, at the root of the California crisis was declining investment in infrastructure components that led to a fundamental imbalance between growing demand for power and an almost stagnant supply. The imbalance had been brewing for many years and is prevalent throughout the nation (see EPRI's Western States Power Crises white paper; www.epri.com/WesternStatesPowerCrisisSynthesis.pdf).

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
- Congestion in transmission network is rising, as indicated by increase of number of Transmission Loading Relief (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 on-going intermediate loss to businesses may well be considerably higher. For a pertinent analyses/survey, please see May 1st 2004 issue of the Economist magazine:

> "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 under investments 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 non-competitive

contracts which did not address the undercurrents and shortcomings of the earlier policies. As the Economist points out (http://www.economist.com/surveys/displayStory.cfm?story_id=2609467):

> "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 10m 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:

- Deploy existing technologies to improve use of already in place transmission assets (e.g., Flexible AC Transmission Systems (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, Hierarchical Control Systems).
- Improve real-time control of network 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. E.g., would an RTO, compliment 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
- 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 broadband 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 200,000 miles of electro-mechanically 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.

I. 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 September 11th, the U.S. President's Commission on Critical Infrastructure Protection in 1997 highlighted the growing concern [7]. 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 May 22, 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-- 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 US universities, focused on advancing basic knowledge and developing breakthrough concepts in modeling and simulation, measurement sensing and visualization, control systems, and operations and management. 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.

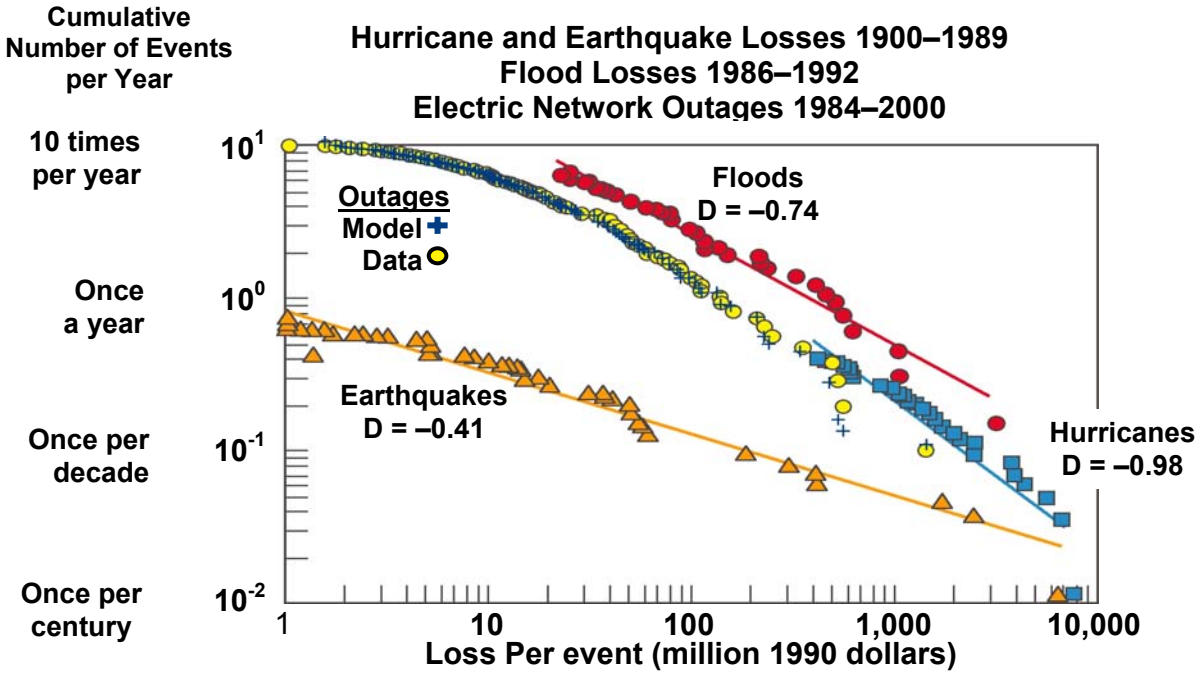

Figure 3: Understanding Complex Systems and Global Dynamics. Economic losses from disasters were found to follow a power law distribution—for hurricanes, floods, earthquakes, and even electrical outages. Fundamental power law distributions also were found for forest fires, Internet congestion, and other systems. CIN/SI results such as these translate in new approaches for optimizing complex systems in terms of productivity and robustness to disaster. Source: The EPRI/DoD Complex Interactive Networks/Systems Initiative (CIN/SI). 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

As an example, related to numerous major outages, narrowly-programmed protection devices have contributed to worsening the severity and impact of the outage-- typically performing a simple on/off logic which locally acts as pre-programmed while destabilizing a larger regional interconnection.

With its millions of relays, controls and other components, the parameter settings and structures of the protection devices and controllers in the electricity infrastructure can be a crucial issue. It is analogous to the poem "for want of a horseshoe nail… the kingdom was lost." i.e. relying on an "inexpensive 25 cent chip" and narrow control logic to operate and protect a multi-billion dollar machine.

Another analogous example is whether one would fly the next generation of advanced fighter aircraft such as the Joint Strike Fighter, but make it rely on Wright Brothers' or more realistically using the 1960s F-4 flight control technologies… and without "wind-tunnel" testing of designs, markets and policies?

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. Some of the pertinent issues are why/how to develop protection and control devices for centralized versus decentralized control and issues involving adaptive operation and robustness to various destabilizers. 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 lose nails and to 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 wild-land 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 had 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 power grid. Some of the pertinent issues are why/how to develop controllers for centralized vs. 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 [21]: “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 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.

J. 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. It is important to note that achieving the grid performance outlined in this chapter is a national profitable investment, not a cost burden on the taxpayer. The economic pay-back is 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 investments money because that is ultimately the public, whether through taxes or kwh 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.

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 twenty-first century's digital society — a smart grid with self-healing capabilities — or be left behind as a twentieth century industrial relic?

Acknowledgments

Most of the materials in this chapter are published in the IEEE Security and Privacy Magazine, September/October 2003, and in the July/August 2004 issue of the IEEE Power and Energy Magazine. 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.

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 9/11 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

Further Reading and References

1. Amin, "North America's Electricity Infrastructure: Are We Ready for More Perfect Storms?" *IEEE* Security and Privacy Magazine, Vol. 1, No.5, pp. 19-25, September/October 2003

2. Amin, "Security Challenges for the Electricity Infrastructure," special issue of the *IEEE Computer Magazine* on Security and Privacy, April 2002

3. M. Amin, "Toward Self-Healing Energy Infrastructure Systems," cover feature in the *IEEE Computer Applications in Power*, pp. 20-28, Vol. 14, No. 1, January 2001

4. M. Amin, "Toward Self-Healing Infrastructure Systems," *IEEE Computer Magazine*, pp. 44-53, Vol. 33, No. 8, Aug. 2000

5. M. Amin, Special issues of IEEE Control Systems Magazine on Control of Complex Networks, Vol. 21, No. 6, December 2001 and Vol. 22, No. 1, February 2002

6. Committee hearing of the House Committee on Energy and Commerce, "Blackout 2003: How Did It Happen and Why?" September 3-4, 2003, http://energycommerce.house.gov

7. Critical Foundations: Protecting America's Infrastructures, The report of the President's Commission on Critical Infrastructure Protection, October 1997, Washington DC, www.ciao.ncr.gov

8. DOE, "National Transmission Grid Study," U.S. Department of Energy, May 2002, http://tis.eh.doe.gov/ntgs/gridstudy/main_screen.pdf.

9. Energy Information Administration, DOE, Annual Energy Outlook 2003, http://www.eia.doe.gov/oiaf/aeo/figure_3.html

10. North American Electric Reliability Council (NERC) Disturbance Analysis Working Group (DAWG) database

11. EPRI. 2003. 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, 155 pp. EPRI, Palo Alto, Dec. 2003

12. EPRI 2001, Electricity Infrastructure Security Assessment, Vol. I-II, EPRI, Palo Alto, CA, Nov. and Dec. 2001.

13. EPRI 2000, "Communication Security Assessment for the United States Electric Utility Infrastructure," (December 2000), EPRI Report 1001174, page 4-11.

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

15. EPRI. 1999. Electricity Technology Roadmap: 1999 Summary and Synthesis, Technical Report, CI-112677-V1, 160 pp. EPRI, Palo Alto, July 1999 (http://www.epri.com/corporate/discover_epri/roadmap/index.html)

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

17. Kundur. *Power System Stability and Control*. EPRI Power System Engineering Series., McGraw-Hill, Inc., 1994

18. T.E. Dy Liacco. "The Adaptive Reliability Control System." IEEE on PAS, May, pp. 517-561, 1967

19. L.H. Fink and K. Carlsen. "Operating Under Stress and Strain." IEEE Spectrum, March, pp. 48-53, 1978

20. 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.

21. S. Silberman, "The Energy Web," *Wired*, vol. 9, no.7, July 2001

22. M. Amin, Special Issue of the Proceedings of the IEEE on *Energy Infrastructure Defense Systems*, forthcoming in 2005

23. M. Samotyj, C. Gellings, and M. Amin, "Power System Infrastructure for a Digital Society: Creating the New Frontiers," in proceedings and keynote address at the GIGRE/IEEE-PES Symp. on Quality and Security of Electric Power Delivery, 10pp., Montreal, October 7-10, 2003