Wiley Handbook of
Science and Technology for
Homeland Security

Countermeasures: robustness, resilience and security

Journal:	*Wiley Handbook of Science and Technology for Homeland Security*
Manuscript ID:	2c1ed-d-09-0008.R1
Wiley - Manuscript type:	Original Manuscript
Date Submitted by the Author:	
Complete List of Authors:	Amin, Massoud; University of Minnesota, Center for the Development of Technological Leadership (CDTL), and dept. of Electrical & Computer Engineering (ECE)
Keywords:	Robustness, Resilience, and Security, Lifeline Infrastructure Interdependencies, Smart Grid, Self-healing Infrastruture, Complex Interdependent Networks/Systems

Countermeasures: Robustness, Resilience, and Security

S. Massoud Amin, D.Sc.[1]
University of Minnesota
Minneapolis, MN 55454 USA

National Critical Infrastructure Systems: Underpinning our economy, global competitiveness, security, and quality of life

Virtually every crucial economic and social function depends on the secure, reliable operation of energy, telecommunications, transportation, financial, and other infrastructures. Indeed, they have provided much of the good life that the more developed countries enjoy. However, with increased benefit has come increased risk. As these infrastructures have grown more complex to handle a variety of demands, they have become more interdependent.

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 lynchpin 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 infiltrating other networks.

A growing portion of the world's business and industry, art and science, entertainment and even crime are conducted through the World Wide Web and the Internet. But the use of these electronic information systems depends, as do the more mundane activities of daily life, on many other complex infrastructures, such as cable and wireless telecommunications, banking and finance, land, water and air transportation, gas, water and oil pipelines, and the electric power grid. All of these are, themselves, complex networks, geographically dispersed, non-linear, and interacting both among themselves and with their human owners, operators, and users. Energy, telecommunications, transportation, and financial infrastructures are becoming increasingly interconnected, thus, posing new challenges for their secure and reliable operation.

> **What is "Infrastructure"?** Infrastructure is the linked socio-technological system of facilities and activities that provides the range of essential services generally necessary to support our economy and quality of life.
>
> **What is a socio-technological system?** Socio-technological systems include the physical infrastructure, the people and organizations who build, run, and use it, as well as the economic and legal conditions for operations.

There is reasonable concern that both national and international energy and information infrastructures have reached a level of complexity, and interconnection which makes them particularly vulnerable to cascading outages, initiated by material failure, natural calamities, intentional attack, or human error. 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. Although there are some similarities, the electric power grid is quite different from

[1] Honeywell/H.W. Sweatt Chair in Technological Leadership, Director of the Technological Leadership Institute, Professor of Electrical & Computer Engineering, and University Distinguished Teaching Professor. Contact information: amin@umn.edu, or http://umn.edu/~amin

gas, oil or water networks-- phase shifters rather than valves are used, and there is no way to store significant amounts of electricity. To provide the desired flow on one line often results in "loop flows" on several other lines.

Our studies in the areas of stability, robustness, resilience, and security span from marco systems (including interdependent national infrastructure and enterprises), to micro (individuals/people) within these large-scale uncertain systems, which are modeled as complex adaptive systems.

As a "micro" example, living beings must constantly adapt to changing environmental conditions and turbulence. Some seem inherently more capable of this resilient adaptation than others. As with leadership in general, there are some innate attributes that predispose some to be more resilient than others. And as cumulative life stress increases pushing one to his/her "maximum emotional capacity" we need to learn to diffuse some of this emotion or it will push us beyond our upper control limit (i.e., exceed our max emotional bandwidth). The key is to learn to manage our "signal to noise ratio" in such a way that we never lose sight of our own unique inner signal. Similarly, understanding how to transform our complex infrastructure systems to be much more sensitive, discerning yet resilient, robust and adaptive will represent a breakthrough in systems engineering.

As the world becomes increasingly VUCA (volatile, uncertain, complex and adaptive), resulting a wide spectrum of opportunities and challenges of complex systems abound, and concerns about the instability of these systems and their potential for large and possible catastrophic regime shifts are a dominant social concern, with "systemic risk" as a generic problem.

These concerns are at the leading edge of many environmental and engineering sciences: for example, in atmospheric science in studies of climate change; for financial risk management in the couplings and resultant systemic risks; for fisheries managers concerned with the sudden collapse of certain economically important fish stocks; for communication networks, concerned with system reliability and security in the face of evolving cyber risks; in electrical and power engineering concerned with preventing disruptions to the North American power grid.

The commonality of the problem of stability and resilience to shocks in complex systems that these examples point to raises the possibility that approaches to risk management in natural and physical systems with pertinence to nearly all aspects of our lives. Some of the methods for managing risk in engineering systems, such as "multi-objective trade-off analysis" in which Pareto-optimal actions are derived by considering the subjective probabilities and payoffs associated with different shocks and their primary, secondary and tertiary propagation pathways and consequences.

Modeling interdependent complex systems and lifeline infrastructures (e.g. the electric power, together with telecommunications, oil/gas pipelines and energy markets) in a control theory context is especially pertinent since the current movement toward deregulation and competition will ultimately be limited only by the physics of electricity and the topology of the grid. In addition, mathematical models of complex networks are typically vague (or may not even exist); 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. In what follows, as examples, we briefly summarize four interdependent infrastructures, and the associated countermeasures for increased robustness, resilience, and security.

Example: Transportation

The backbone of the US transportation system and economy—the road infrastructure system—has continually evolved since the 1930s, but the cost to build and maintain it is rising. The US Department of Transportation estimates that the annual cost of congestion in lost productivity alone is more than $100 billion. In addition, more than 40,000 persons are killed and another 5 million injured each year in traffic accidents. This infrastructure, faced with the increased density in today's urban population centers, is becoming increasingly congested. Human population centers have grown dramatically in the past century, creating a "trilemma" of sustainability issues: population, poverty, and pollution. The U.S. along with many other nations is seeking a solution to this worsening traffic congestion problem. Such solutions have to be viewed in terms of the economic, social, and political environments, along with the technological capability of the nation. Furthermore, the costs associated with generating and maintaining the road infrastructure are becoming increasingly higher, and the impact of inefficiencies can be measured in quantifiable terms of loss of labor-hours in the work place, loss of fuel, as well as intangibly in terms of pollution, and the general increased stress level of the work force who uses these transportation channels.

Where feasible, increasing the number of lanes or building new roads can expand present capacity, but the demand in some areas (both from population growth and travel demand) can't be met by adding roads. A less expensive and disruptive solution is to intelligently manage the existing road infrastructure. The idea is to create and deploy technologies to improve the safety, capacity, and operational efficiency of the surface transportation system, while simultaneously reducing the burden on the environment and on our energy sources. With these objectives in mind, Congress launched the US Intelligent Transportation Systems (ITS) program in 1991. One of the program's goals is to develop Advanced Traffic Management Systems. ATMS will rely on the consolidation of information, automotive, and highway technology. A wide range of small, complementary systems—from electronic route guidance to pre-emptive signal control—will essentially automate highways. Sensors and communication devices will be along the roads, as well as in the vehicle. Thus, the road will "know" its operational status, which it will then communicate to the vehicle. The vehicle operator can then make informed decisions about which routes to take to optimize individual trips and daily travel plans. Entities such as traveler information services and fleet management can use the data to plan, implement, and manage their daily operations.

Both public and private outfits can also use the road to plan, implement, and manage their daily operations, including traveler information, traffic management, public and rural transportation management, priority vehicle management, and freight and fleet management. Thus, although they pose great analytical challenges, the ATMS thrust offers significant payoff because of its broad geographical coverage and direct impact on regional economies. As complex as it is[2], the road system is only one segment of the

[2] A few statistics on how we get around in America:

- Length of public roads: 46,036 miles of interstate highways (1%); over 112,450 miles of National highway System (3%); and 3.76M miles of other (96%)
- Personal Travel by Mode:
  - 208M vehicles: Private Vehicles 85.9%, Public Transport 2.8%, other means 11.3%
  - About 130M cars, 69M light trucks, 7M commercial trucks and 700K buses (e.g., CA has 15.5M motor vehicles, FL has 7.3M,…)
  - About 1.2M rail cars, 68 ferries, 6,000 aircraft
- Half of the total petroleum consumption in the U.S. is for highway vehicles and another 18% for other transportation:
  - Fuel consumption: 148 billion gallons of gasoline, 28B gallons of Diesel, and about 4B gallons other.
- Fatalities: 22,416 in cars (50.4%), 9,901 truck occupants (22.2%), 2,160 on motorcycles (4.9%), 1,088 on aircraft (3.1%), and 624 on trains (1.4%)

transportation network. As in the other infrastructures, there are diverse sources of complexity and interdependence. Emerging issues include:

- Impact of Information Technology: IT and transportation systems' inter-relations. Transportation is increasing links with sensors, telecommunications, and even satellites.
- Electrification of multi-modal transportation systems: E.g., rail networks are becoming increasingly dependent on electricity (electric and magnetic levitation trains).
- Fertile area at the intersection of CE/CS/EnvE/EE/ME/OR/Math/Control/Economics
- Traffic modeling, prediction, and management: from operational issues to expansion planning
- Multiresolutional simulations; Real-time optimization, epsilon-optimality, provable performance bounds.

In the area of multi-modal transportation and distribution networks (air, land, and sea), emerging issues include: electrification of transportation; links with sensors, telecommunications and satellites; traffic modeling, prediction, and management; multi-resolutional simulations; real-time optimization with provable performance bounds with risk management; and how to develop tools in the intersection of mathematics, risk management, operations research, control theory, system science, computer science, artificial intelligence, economics, and even biology to tackle these problems. Several researchers have referred to this as 'intelligent or adaptive control'; the challenge is how to develop systems that can sense, identify and build realistic models? And can also adapt, control and achieve their goals?

These are challenges not only in transportation systems, but are the characteristics of any industry made up of many, geographically dispersed components that can exhibit rapid global change as a result of local actions. Prime examples are the highly interconnected and interactive industries, which make up a national or international "infrastructure," including telecommunications, transportation, gas, water and oil pipelines, the electric power grid, and even the collection of satellites in earth orbit.

Example: Telecommunications

The globalization of our economy is built on telecommunication networks, including fixed networks, (public switched telephone and data networks), wireless (cellular, PCS, wireless ATM), and computers (Internet and millions of computers in public and private use). These networks are growing rapidly and require secure, reliable, high-quality power supplies. This telecommunication infrastructure, like the power grid, is becoming overburdened. The satellite network, just one segment of the infrastructure, is a good example. The satellite network has three main layers:

- low-earth orbit, 200 to 2,000 km ("little LEOs" at 750-1500 km), operating at VHF, UHF below500MHz; low complexity;
- medium-earth orbit, 2000 to 20,000 km (big LEOs/MEOs at 750-11,000 km) operating at Land S microwave (1.6 and 2.5 GHz) with high to very high complexity; and
- geosynchronous orbit (GEO), at 36,000 km, operating at K microwave (19 and 29 GHz), with variable low to high complexity.

Some of the most familiar services are detailed Earth imaging, remote monitoring of dispersed locations, and highly accurate location and tracking using the continuous signals of the global positioning system (GPS). Satellite-based business and personal voice and data services are now available throughout much of the world.

- Fatal accident types amenable to technological prevention: Off-road (36%), angle collision (18%), head-on collision (17%), rear-end collision (5%), sideswipe (2%).

The Internet is rapidly expanding the range of applications for satellite-based data communications; two of the most popular applications are accessing the Internet itself and connecting remote sites to corporate networks. Some satellite systems, including those of satellite TV providers, let users browse Web pages and download data—at 400 kbps—through a 21-inch (53cm) roof-mounted dish receiver connected to a personal computer with an interface card. This capability could become a valuable tool for expanding an enterprise network to remote offices around the world.

Some utilities are diversifying their businesses by investing in telecommunications and creating innovative communications networks that cope with industry trends toward distributed resources, two-way customer communications, and business expansion, as well as addressing the measurement of complex and data-intensive energy systems via wide-area monitoring and control. Challenges include how to handle network disruptions and delays and manage orbits from the satellite. A big source of complexity is the interdependence of the telecommunication networks and the power grid.

The telecommunications network and the electric power grid are becoming increasingly interdependent. Issues range from the highest command and control level to the individual power stations and substations at the middle level, and then to the devices and power equipment at the lowest level.

Example: Financial Systems[3]

The stability of the financial system and the potential for systemic events to alter the functioning of that system have long been important topics for central banks and the related research community. Developments such as increasing industry consolidation, global networking, terrorist threats, and an increasing dependence on computer technologies underscore the importance of this area of research. Recent events, however, including the terrorist attacks of September 11th and the demise of Long Term Capital Management, suggest that existing models of systemic shocks in the financial system may no longer adequately capture the possible channels of propagation and feedback arising from major disturbances. Nor do existing models fully account for the increasing complexity of the financial system’s structure, the complete range of financial and information flows, or the endogenous behavior of different agents in the system. Fresh thinking on systemic risk is, therefore, required.

In order to promote a better understanding of systemic risk, the National Academy of Sciences and the Federal Reserve Bank of New York convened a conference in New York in May of 2006 drawing together a broadly interdisciplinary group of scientists, engineers and financial practitioners, ranging from electrical engineers and academic economists to risk analysts and asset managers from major investment banks. The primary purpose of the conference was to promote a cross-disciplinary dialogue in order to examine what possible leverage on the topic of systemic risk could be gained from areas of science not directly related to finance or economics. Accordingly, conference participants from the natural and mathematical sciences and from engineering disciplines drew heavily upon research on complex adaptive systems in order to build a framework both to give some substance and definition to the notion of systemic risk and to point to possible linkages between this research and research on the financial system. Similarly, research economists presented papers that showed how some of these linkages could be leveraged, for example in studies of international trade and, crucially for the Federal Reserve policy, in the management of the payments system. Participants from the financial industry also highlighted how thinking on systemic risk and actual systemic events affect trading activities in order to provide a context for the discussion.

[3] This section on financial systems is based on my presentation and related discussions at the “New Directions for Understanding Systemic Risk: A report on a Conference Cosponsored by the Federal Reserve Bank of New York and the National Academy of Sciences,” for the NAS book and complete FRBNY report please see: Economic Policy Review, Federal reserve Bank of New York, Vol. 13, Number 2, Nov. 2007, and New Directions for Understanding Systemic Risk, 108 pp, Nat’l Acad. Press, Washington DC, 2007. Input and material from NAS/BMSA and FRBNY is gratefully acknowledged.

For more information, please see the above-referenced report as well as the prevalence of systemic risk in very diverse areas ranging from biological and natural ecologies to financial, built and engineered complex systems in which prediction and management of systemic failures are critical.

In an engineered system, like the electric power grid or a telecommunication network, there is indeed the opportunity for control systems, and these can be quite advanced. Creating such a control capability for the electric grid required a mixture of tools from dynamical systems, statistical physics, information and communication science, along with research to reduce the computational complexity of the algorithms so they can scale up with the large size of the system being controlled. Our earlier work has led to working methods that have been applied to a variety of situations, including the electricity infrastructure coupled with telecommunications and the energy markets, cell phone networks on the Internet, and some biological systems. This is a multiscale challenge: detection of troublesome signals must be done within milliseconds, with some compensatory actions taken automatically, while some load balancing and frequency control on the grid is controlled on a timescale of seconds. At the same time, control functions such as load forecasting and management and generation scheduling take place on a timescale of hours or days. Developing a picture at the atomic level of what is going on in a system and then building up to the macro-scale is a challenge that requires multi-resolutional modeling in both space and time.

Just to give an idea of the complexity of modeling and controlling the electrical grid, in North America, there are more than 15,000 generators, and over 216,000 miles of high-voltage lines. The overall grid is divided in several very large interconnected regions, and modeling one of them (which is necessary for understanding the systemic risks) might entail a simulation with 50,000 lines and 3,000 generators. The system is typically designed to withstand the loss of any single element. To determine whether the grid can attain that design goal, we need to simulate the loss of each of 53,000 elements and calculate the effects on each of 50,000 lines, leading to over 2.6 billion cases. The analysis of these systemic risks is very challenging, but it can really make a difference in how to operate the system.

As an additional illustration of the level of detail that can successfully be modeled, we developed an example of a complex model to predict load and demand for DeKalb, Illinois, which is a sizeable market with a mixture of commercial and residential customers. Deregulation of the electric system has reduced the correlation between power flow and demand, thus introducing uncertainty into the system, and so there has been a good deal of research to understand this phenomenon and develop the means to monitor and control it. The models and algorithms are now good enough to simulate the demand by customer type (residential, small commercial, large commercial) on an hour-by-hour basis and attain 99.6-99.7 percent accuracy over the entire year. One value of these predictions is that they enable the power company to proactively dispatch small generators to meet anticipated high demands.

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.

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 to save the kingdom.

Another key insight came out of analysis of forest fires, which researchers in one of the six funded consortia 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 the trees are. If there is just one tree in a barren field and it is hit by lightning, it burns but no large 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-such as a surge protector or circuit breaker-is reached. If the barrier does not function properly or is insufficiently large, the failure bypasses it and continues cascading across the system.

These 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.

Work during the past eleven years in this area has developed, among other things, a new vision for the integrated sensing, communications, and control-issues surrounding the power grid. Some of the pertinent issues are why/how to develop protection and control devices for centralized versus decentralized control, as well as 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.

This is not meant to imply that ecology and engineering have overcome all the challenges associated with representing and analyzing complex adaptive systems. Sensing the state of such systems is one ongoing challenge, as is the question of what to measure. Validation of models and verification of software remains a major challenge. There are major computational problems, including how to break models into tractable components. Self-similar systems can be reduced, but not complex systems like the electrical grid. One can use approximations to decouple complex systems, but it is difficult to analyze the errors thus introduced. One can find parts of an engineered system—and presumably in other systems—that are weakly coupled in terms of the dynamics transferred through the system and then approximate those portions with standalone models. This can help us reduce the complexity by dividing and conquering.

It is important to emphasize the difficulty of identifying meaningful signals from complex systems. For example, when monitoring a large fraction of the U.S. electrical grid, how can we discern whether a perturbation in the system (be it financial, physical, communication, or cyber or a combination of them), is a natural fluctuation or the signature of a catastrophic failure? Does it reflect a naturally caused phenomenon, perhaps triggered by heat, high humidity, or a high demand in one portion of the grid, or is it actually an attack on the system or the precursor to major disturbance? How close is it to a regime shift or system flip? That can only be addressed with detection systems that can pull up all the data, do data mining, pattern recognition, and then statistical analysis to derive the probability that we were sensing a catastrophic failure or a precursor of one.

This system monitoring problem is exacerbated if sharing of information is limited, as is the case in the banking sector. For example, I am often asked how one would monitor and control the reliability of the electrical grid under the assumption that companies did not cooperate with each other but, instead, competed and didn't share information? Such a situation would lead to a new control mechanism, and the logical question is whether this would stabilize or destabilize the system? For an EPRI project from the late 1990s, Simulator for Electric Power Industry Agents (SEPIA), we began exploring this case. The analysis was done for four large regions of the United States, and explored whether one could increase efficiency without diminishing reliability. This concept would need to be scaled up in order to reach a definitive conclusion.[4]

There is also the work on highly optimized tolerance that Professors John Doyle and Jean Carlson have been developing in California, in which they basically use a genetic algorithm, a neural network approach to evolve the properties of systems. They consider a variety of systems with particular structures and feedback properties, expose them to perturbations, observe their recovery, and just as one would train a chess playing program, these systems are modified until they become more tolerant to the disturbances to which they are exposed. So that is a way how even when one can't solve the mathematics, one can improve the structure of systems. The difficulty with these approaches, as Doyle and Carlson point out, is that systems become robust yet fragile in their terminology, meaning systems that are engineered or have evolved to be tolerant to a particular set of disturbances often do so at the expense of their response to other classes of disturbances, something that we have to be careful about in the design of systems.[5]

Complex systems abound, and many different disciplines are concerned with understanding catastrophic change in such systems. We focus on three principal areas: risk assessment, modeling and prediction, and mitigation.

[4] See Amin, Massoud, Restructuring the Electric Enterprise: Simulating the Evolution of the Electric Power Industry with Adaptive Agents, Chapter 3 in *Market Based Pricing of Electricity*, A. Faruqui and M. Crew, eds., Kluwer Academic Publishers, Dec. 2002.

[5] See, e.g., T. Zhou, J. M. Carlson and J. Doyle, Mutation, specialization, and hypersensitivity in highly optimized tolerance, *Proceedings of the National Academy of Sciences* 99:2049-2054. 2002. and J. M. Carlson and J. Doyle, Complexity and robustness, *Proceedings of the National Academy of Sciences* 99 suppl. 1:2538-2545. 2002.

Example: North American Power Grid

Electrification of Transportation and Enabling a Smart Self-healing Grid

Our economy places increased demand for reliable, disturbance-free electricity. The electric power grid is quite different from other infrastructure systems, such as gas, oil or water networks. A distinguishing characteristic of electricity, for example, is that there is no way to store significant amounts of energy; thus the system is fundamentally operating in real-time. For this and related reasons, energy infrastructure systems have a unique combination of characteristics that makes control and reliable operation challenging:

- Attacks and disturbances can lead to widespread failure almost instantaneously.
- Billions of distributed heterogeneous infrastructure components are tightly interconnected.
- A variety of participants—owners, operators, sellers, buyers, customers, data and information providers, data and information users—interact at many points.
- The number of possible interactions increases dramatically as participants are added. No single centralized entity can evaluate, monitor, and manage them in real time.
- The relationships and interdependencies are too complex for conventional mathematical theories and control methods.

These characteristics create unique challenges in modeling, prediction, simulation, cause and effect relationships, analysis, optimization, and control, which have important implications for the use of IT for electric power. This chapter addresses these challenges by first presenting the technologies involved in the electricity infrastructure and then considers management and policy challenges to the effective performance both in the short and long term.

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 IT 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 (EIA 2003; EPRI 1999-2003).

At its most fundamental level, the network's transmission lines form a vertically integrated hierarchical network consisting of the generation layer (noted above) and three other network levels. 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 sub-transmission level. The second level is *sub-transmission*, 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 its adaptation to disturbances, a power system can be characterized as having multiple states, or "modes," during which specific operational and control actions and reactions take place: normal, disturbance, and restorative. 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. And in the restorative mode, priorities include re-scheduling, re-synchronization, and load restoration. Some authors include an Alert Mode before a disturbance actually affects the system. Others add a System Failure Mode before restoration is attempted.

Beyond the risk management note above, the electric power grid's emerging issues include 1) integration and management of renewable resources and "microgrids;" 2) use and management of the integrated infrastructure integrated with an overlaid sensor networks, secure communications and intelligent software agents (including dollars/economic factors and watts); 3) active-control high-voltage devices; 4) developing new business strategies for a deregulated energy market; and 5) ensuring system stability, reliability, robustness, and efficiency in a competitive marketplace and carbon-constrained world.

In addition, the electricity grid faces (at least) three looming challenges: its organization, its technical ability to meet 25 year and 50 year electricity needs, and its ability to increase its efficiency without diminishing its reliability and security.

Smart Self Healing Grid

The term "smart grid" refers to the use of computer, communication, sensing and control technology which operates in parallel with an electric power grid for the purpose of enhancing the reliability of electric power delivery, minimizing the cost of electric energy to consumers, and facilitating the interconnection of new generating sources to the grid.

The concept for smart grid research and development was originally conceived by this author when I was at the Electric Power Research Institute (EPRI) during 1998-2003. The genesis of the smart grid was in the EPRI/DOD Complex Interactive Networks/Systems Initiative (CIN/SI) that I created and led during 1998-2001.

Beginning in 1998, the original concept and tools developed within CIN/SI were referred to as "The Self Healing Grid". This name has undergone several changes and finally emerged as "The Smart grid."

More recently, after joining the University of Minnesota in 2003, my research team and I have been engaged in research and also in telling our colleagues about this concept through publications, lectures and seminars to diverse stakeholders, which include a wide spectrum -- from local to international utilities, companies, state and federal organizations, universities and think thanks, to congressional staffers, R&D caucus and committees who have invited our assessments and presentations.

The smart grid is a term also built into the Energy Independence and Security Act of 2007, and more recently the American Recovery and Reinvestment Act of 2009 (the stimulus bill). The US Congress allocated $11 billion to research and demonstration projects in the smart grid area. This technology is currently an active topic on TV news and is discussed widely in the media.

Title XIII of EISA 2007 mandates a "Smart Grid" that modernizes and improves the information infrastructure. The Smart Grid represents the information and control functionality that will monitor, control, manage, coordinate, integrate, facilitate, and enable achievement of many of the benefits of innovations envisioned in national energy policy. Examples of Smart Grid functionality include:

- Connecting end user loads to grid information and control to facilitate energy efficiency improvements
- Integrating alternative energy sources and providing the means for mitigating their intermittency
- Providing the necessary information and control to integrate pluggable hybrids into the grid
- Allowing problems to be detected and addressed before they become grid disturbances

Information on these is widely available through EPRI assessments and reports, the U.S. Department of Energy (The Smart Grid -- An Introduction, 2008), and the IEEE National Energy Policy Recommendations related to the Smart Grid is a great resource.

In summary an electric power system has two infrastructures:

- An electric infrastructure – that carries the electric energy in the power system, and
- An information infrastructure that monitors, controls, and performs other functions related to the electric infrastructure.

The existing electric power grid isn't dumb. It has long been designed to continue operating even in the face of problems. Equipment breaks, thunderstorms happen, curious animals get into substations, and drivers crash cars into distribution poles. The power grid is designed and operated so that any single situation does not interrupt the flow of power (the so-called “n-1 criterion”). That requires intelligence, which comes from electromechanical automation, Intelligent Electronic Devices (IEDs), control centers, computers, and communications systems. Such functions have been part of the electric grid for many years. However, because of a combination of cost and operational continuity issues, many of these systems lag, sometimes by decades, advances and capabilities in computer and communications technology.

The institutional and economic framework envisioned for the 21st Century Power System ultimately depends upon building new types and levels of functionality into today’s power system. These needed capabilities will be “enabled” by several breakthrough innovations, including but not limited to the following:

- **Digitally controlling the power delivery network** by replacing today’s electro-mechanical switching with real-time, power-electronic controls. This will become the foundation of a new “smart, self-healing power delivery system” that will enable innovative productivity advances throughout the economy. Digital control, coupled with communications and computational ability is the essential step needed to most cost-effectively address the combined reliability, capacity, security, and market-service vulnerabilities of today’s power delivery system.

- **Integrating communications** to create a dynamic, interactive power system for real-time information and power exchange. This capability is needed to enable retail energy markets; power interactive, microprocessor-based service networks; and fundamentally raise the value proposition for electricity. Through advanced information technology coupled with sensors, the system would be “self healing” in the sense that it is constantly self-monitoring and self-correcting to keep high-quality, reliable power flowing. It can sense disturbances and instantaneously counteract them, or reconfigure the flow of power to cordon off any damage before it can propagate.

- **Automating the distribution** system to meet evolving consumer needs. The value of a fully automated distribution system integrated with communication—derives from four basic functionality advantages:

  1. Reduced number and duration of consumer interruptions, fault anticipation, and rapid restoration.
  2. Increased ability to deliver varying levels of reliable, digital-grade power.
  3. Increased functional value for all consumers in terms of metering, billing, energy management, demand control, and security monitoring, among others.
  4. Access to selective consumer services including energy-smart appliances, electricity-market participation, security monitoring, and distributed generation.
  5. The value of these advantages to consumers, suppliers, and society alike more than justify the needed public/private investment commitment. This transformation will enable additional innovations in electricity service that are bounded only by our imagination.

- **Transforming the meter** into an EnergyPort (Energy Port is a service mark of EPRI). EnergyPort is a consumer gateway that allows price signals, decisions, communications, and network intelligence to flow back and forth through the two-way energy/information portal. This will be the linchpin technology that leads to a fully functioning marketplace with consumers responding (through microprocessor agents) to service offerings and price signals. This offers a tool for moving beyond the commodity paradigm of 20th Century electricity service, and quite possibly ushering in a set of new energy/information services as diverse as those in today's telecommunications.
- **Integrating distributed energy resources including intermittent and renewable generation and storage systems.** The smart power delivery system would also be able to seamlessly integrate an array of locally installed, distributed power generation as power system assets. Distributed power sources under could be deployed on both the supply and consumer side of the energy/information portal as essential assets dispatching reliability, capacity and efficiency.
- **Accelerating end-use efficiency**. The growing trend toward digital control can enable sustained improvements in efficiency and productivity for nearly all industrial and commercial operations. Similarly, the growth in end-use energy consuming devices and appliances, networked with system controls, will afford continuous improvements in productivity and efficiency.

Other benefits of the Smart Grid go beyond energy efficiency:

- The Smart Grid will facilitate use of alternative generation that supports energy independence. This is a matter of national security.
- Both cyber-security protection and defense against EMP: Components of the Smart Grid will need to be hardened by design.
- There are likely to be numerous benefits of the Smart Grid that defy quantification. Examples include the flexibility to accommodate new requirements, the ability to accommodate innovative grid technology, and the ability to support innovative regulatory concepts, all without major replacement of existing equipment.
- The flexibility may help avoid future rate increases as new technology or requirements arise, but the exact benefit might not be quantifiable.

Revolutionary developments in both information technology and material science and engineering promise significant improvement in the security, reliability, efficiency, and cost-effectiveness of all critical infrastructures. Steps taken now can ensure that critical infrastructures continue to support population growth and economic growth without environmental harm.

Digital Network Control: Operational Systems

IT has and will play a critical role in ensuring the reliable transmission and distribution of electricity. Electricity's share of total energy in the world is expected to continue to grow, as more efficient and intelligent processes are introduced, such as controllers based on power electronics combined with wide-area sensing and management systems for improved performance. In the next two decades, it is envisioned that the electric power grid will move from an electro-mechanically controlled system to one that is electronically controlled.

In this sense, the electrical infrastructure is becoming increasingly intertwined with the IT infrastructure that supports it. Current and future power systems applications for telecommunications include the following:

- Surveying overhead transmission circuits and rights-of-way
- Transmitting SCADA system data (usually via telephone circuits)
- Measuring overhead conductor sag
- Measuring phasors (using a precise timing signal derived from the GPS to time-tag measurements of ac signals)
- Fitting sine waves to ac signals, and determining magnitude and phase of v(t), i(t) in remote locations
- Enhancing situational awareness by generating real-time pictures of system states and real-time power flow as well as real-time estimation of the systems' state and topology
- Using data from Low Earth Orbit (LEO) satellites for faster-response control (more than 100 times less delay than High Earth Orbit (HEO) satellites) and connecting to existing parallel data stream facilities (effectively a high-speed global RS-232 channel)

The technologies support the operational control of electrical networks, ranging from energy management systems (EMS) to remote field devices. Critical systems include those described below.

Energy Management System (EMS): The objective of the EMS is to manage production, purchase, transmission, distribution and sale of electrical energy in the power system at a minimal cost with respect to safety and reliability. Management of the real-time operation of an electric power system is a complex task requiring interaction of human operators, computer systems, communications networks, and real-time data-gathering devices in power plants and substations. An EMS consists of computers, display devices, software, communication channels and remote terminal units that are connected to Remote Terminal Units (RTUs), control actuators, and transducers in power plants and substations. The main tasks it performs is dependent upon generator control and scheduling, network analysis and operator training. Control of generation requires that the EMS maintain system frequency and tie line flows while economically dispatching each generating unit. Management of the transmission network requires that the EMS monitor up to thousands of telemetered values, estimate the electrical state of the network, and inform the operator of the best strategy to handle potential outages that could result in an overload or voltage limits violation. EMSs can have real time two-way communication links between substations, power plants, independent system operators, and other utility EMSs.

Supervisory Control and Data Acquisition (SCADA) System: A SCADA system supports the operator control of remote (or local) equipment, such as opening or closing a breaker. A SCADA system provides three critical functions in the operation of an electric power system: data acquisition, supervisory control, and alarm display and control. It consists of one or more computers with appropriate applications software connected by a communications system to a number of RTUs placed at various locations to collect data, perform intelligent control of electrical system devices and report results back to an EMS. SCADAs can also be used for similar applications in natural gas pipeline transmission and distribution applications. A SCADA can have real time communication links with one or more EMSs and hundreds of substations.

Remote Terminal Unit (RTU): RTUs are special purpose microprocessor-based computers that contain analog to digital converters (ADC) and digital to analog converters (DAC), digital inputs for status and digital output for control. There are transmission substation RTUs and distribution automation (DA) RTUs. Transmission substation RTUs are deployed at substation and generation facilities where a large number of status and control points are required. DA RTUs are used to control air switches and various compensation capacitor banks (that support voltage) on utility poles, control pad-mounted switches, monitor and automate feeders, monitor and control underground networks and for various uses in smaller distribution substations. RTUs can be configured and interrogated using telecommunication technologies. They can have hundreds of real time communication links with other substations, EMS, and power plants.

Programmable Logic Controller (PLC): PLCs have been used extensively in manufacturing and process industries for many years and are now being used to implement relay and control systems in substations. PLCs have extended I/O systems similar to transmission substation RTUs. The control outputs can be controlled by software residing in the PLC and via remote commands from a SCADA system. The PLC user can make changes in the software without making any major hardware or software changes. In some applications, PLCs with RTU reporting capability may have advantages over conventional RTUs. PLCs are also used in many power plant and refinery applications. They were originally designed for use in discrete applications like coal handling. They are now being used in continuous control applications such as feedwater control. PLCs can have many real time communication links inside and outside substations or plants.

Protective Relays: Protective relays are designed to respond to system faults such as short circuits. When faults occur, the relays must signal the appropriate circuit breakers to trip and isolate the faulted equipment. Distribution system relaying must coordinate with fuses and reclosures for faults while ignoring cold-load pickup, capacitor bank switching and transformer energization. Transmission line relaying must locate and isolate a fault with sufficient speed to preserve stability, reduce fault damage and minimize the impact on the power system. Certain types of “smart” protective relays can be configured and interrogated using telecommunication technologies.

Automated Metering: Automated metering is designed to upload residential and/or commercial gas and/or electric meter data. This data can then be automatically downloaded to a PC or other device and transmitted to a central collection point. With this technology, real time communication links exist outside the utility infrastructure.

Plant Distributed Control Systems (DCSs): Plant Distributed Control Systems are plant-wide control systems that can be used for control and/or data acquisition. The input/output (I/O) count can be as high as 20,000 data points or higher. Often, the DCS is used as the plant data highway for communication to/from intelligent field devices, other control systems such as PLCs, RTUs, and even the corporate data network for Enterprise Resource Planning (ERP) applications. The DCS traditionally has used a proprietary operating system. Newer versions are moving toward open systems such as Windows NT, Sun Solaris, etc. DCS technology has been developed with operating efficiency and user configurability as drivers, rather than system security. Additionally, technologies have been developed that allow remote access, usually via PC, to view and potentially reconfigure the operating parameters.

Field Devices: Examples of field devices are process instrumentation such as pressure and temperature sensor and chemical analyzers. Other standard types of field devices include electric actuators. Intelligent field devices include electronics to enable field configuration, upload of calibration data, etc. These devices can be configured off-line. They also can have real time communication links between plant control systems, maintenance management systems, stand-alone PCs, and other devices inside and outside the facility.

Digital Interdependencies and Security Risks

Recognizing the increased interdependence between IT and electricity infrastructures, along with technical and business opportunities, 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. The energy industry has historically operated closed, tightly controlled networks. Deregulation and the resulting commercial influences have placed new information sharing demands on the energy industry. Traditional external entities like suppliers, consumers, regulators and even competitors now must have access to segments of the network. The definition of the network must be expanded to include the external wide area network connections for these external entities. This greatly increases the security risk to other functional segments of the internal network that must be protected from external connections. This is true whether a private network or the Internet is used to support the external wide area network.

The external entities already have connections to the Internet and as such the Internet can provide the backbone for the External Wide Area Network. Duplicating this backbone to create a private network requires not only large up front start up costs, but also ongoing maintenance costs and potentially higher individual transaction costs than using the Internet.

Information systems and on-line data processing tools include: the Open Access Same-time Information System (OASIS), which is now in operation over the Internet; 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 thermal, voltage, and interface limits.

Increased use of electronic automation raises issues regarding 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 world-wide location using an inexpensive computer and a modem; (3) use of networked electronic systems for metering, scheduling, trading or e-commerce imposes numerous financial risks.

Utility telecommunications often include several media and diversified communications networks which in part provide redundancy; these range from dedicated fiber optic cables, digital & analog microwave, and VSAT satellite to power line carrier technology as well as the use of multiple address radio, spread spectrum radio, trunked mobile radio, and cellular digital packet data. Security of the cyber and communication networks now used by businesses is fundamental to the reliable operation of the grid; as power systems start to rely more heavily on computerized communications and control, system security has become increasingly dependent on protecting the integrity of the associated information systems. Part of the problem is that existing control systems, which were originally designed for use with proprietary, stand-alone communications networks, were later connected to the Internet (because of its productivity advantages and lower costs), but without adding the technology needed to make them secure. Communication of critical business information and controlled sharing of that information are essential parts of all business operations and processes.

If the deregulation of the energy industry resumes, information security will become more important. Energy-related industries will have to balance what appear to be mutually exclusive goals of operating system flexibility with the need for security. Key electric energy operational systems depend on real-time communication links both internal and external to the enterprise. The functional diversity of these organizations has resulted in a need for these key systems to be designed with a focus on open systems that are user configurable to enable integration with other systems both internal and external to the enterprise. In many cases, these systems can be reconfigured for security using telecommunication technologies and in nearly all cases the systems dynamically exchange data in real time. Power plant DCS systems produce information necessary for dispatch and control. This requires real-time information flow between the power plant and the utility's control center, system dispatch center, regulatory authorities, etc. A power plant operating as part of a large wholesale power network may have links to an independent system operator, a power pool, etc. As the generation business moves more and more into market-driven competitive operation, both data integrity and confidentiality will become major concerns for the operating organizations.

Any telecommunication link which is even partially outside the control of the organization owning and operating power plants, SCADA systems or EMSs represents a potentially insecure pathway into business operations and to the grid itself. The interdependency analyses done by most companies during Y2K preparations has both identified these links and the systems' vulnerability to their failures. Thus they provide an excellent reference point for a cyber-vulnerability analysis.

In particular, monitoring and control of the overall grid system is a major challenge. Existing communication and information system architectures lack coordination among various operational components, which usually is the cause for the unchecked development of problems and delayed system restoration. Like any complex dynamic infrastructure system, the electricity grid has many layers and is vulnerable to many different types of disturbances. While strong centralized control is essential to reliable operations, this requires multiple, high-data-rate, two-way communication links, a powerful central computing facility, and an elaborate operations control center, all of which are especially vulnerable when they are needed most — during serious system stresses or power disruptions. For deeper protection, intelligent distributed control is also required; this would enable parts of the network to remain operational and even automatically reconfigure in the event of local failures or threats of failure.

Distributed control capability is becoming available in next-generation integrated sensors that are equipped with two-way communication capability and support "intelligent agent" functions — not just sensing, but data assessment, adaptive learning, decision making, and actuation. The development of Intelligent Electronic Devices (IEDs) that combine sensors, telecommunication units, computers, and actuators will allow highly automated adjustments to be made at many points on the system and protect substantially against cascading failures. The use of distributed intelligent agents also opens the door to the development of a self-healing power grid that responds adaptively to counteract disturbances at the site of their occurrence.

Intelligent sensors will be capable of gathering a wide range of operating data, including time-stamped measurements of voltage, current, frequency, phase angle, and harmonics. This information, which provides input for distributed control, can also be integrated into a real-time system-wide database and coupled with analysis tools that perform dynamic monitoring, state estimation, disturbance analysis, and contingency assessment for the grid as a whole. Unfortunately, simulation-based techniques and mathematical models are presently unable to accurately portray the behavior of interactive networks, whose dynamics can be highly nonlinear. Fine-tuning existing models with real-world input from distributed sensors may offer improvements, but substantial progress will require the formulation of new models.

SCADA and EMS system operations are critically dependent on the telecommunication links that gather data from geographically dispersed sources and transmit operational and control instructions to geographically dispersed facilities. In the North American grid these telecommunications links run the gamut from hardwired private networks to multi-network systems using a combination of private and public networks for both data acquisition and control. Not all of the networks are hardwired. Microwave and satellite communications links are common alternatives in areas where topography and/or distance makes wireless more cost effective. At first glance it would seem that a private, hardwired network that is totally within the control of the owner organization is a secure system. However, even hardwired private networks will be linked to networks outside the control of the company. Typical outside data sources are bulk power customers, major retail customers, bulk power providers, power pools, independent system operating entities, etc. These connections can offer a multitude of paths into the SCADA and EMS systems. Without proper security design and management, each link is a potential security risk.

Challenges include how to handle network disruptions and delays and manage orbits from the satellite. A major source of complexity is the interdependence of the telecommunication networks and the power grid. Issues range from the highest command and control level to the individual power stations and substations at the middle level, and then to the devices and power equipment at the lowest level.

As the readers of this Handbook know, technology is a two-edged sword. In the case of electricity, the aforementioned discussion reveals one edge (i.e., the risk) to be the extent to which IT introduces a new set of security concerns. The other edge (i.e., the promise) remains due to the substantial increases in capacity and efficiency that are made possible through continuing IT advancements. The following is a sample of the emerging technologies that promise continuing gains in the electricity sector:

- Flexible Alternating Current 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.
- Unified Power Flow Controller (UPFC), a third-generation FACTS device that uses solid-state electronics to direct power flow from one line to another to reduce overloads and improve reliability
- Fault Current Limiters (FCLs), which absorb the shock of short circuits for a few cycles to provide adequate time for a breaker to trip. Preliminary results of post August 14th outage show that FCLs could have served as "shock absorbers" to limit the size of blackouts.
- 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
- 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 total transfer capability for each transmission path posted on the OASIS network, while taking into account thermal, voltage, and interface limits
- 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
- Enhanced IT systems for Wide-Area Measurement/Management Systems (WAMS), Open-access Same-time Information System (OASIS), Supervisory Control and Data Acquisition (SCADA) and Systems, Energy Management Systems (EMS)
- Advanced software systems for dynamic security assessment of large/wide-area networks augmented with market/risk assessment

- Intelligent Electronic Devices with security provisions built in by combining sensors, computers, telecommunication units, and actuators; related "intelligent agent" functions such as assessment, decision, and learning

However, even if most of the above technologies are developed and deployed, there is still a major management challenge in making such a complex network perform reliably with security. These issues are taken up next.

Management

***Human Performance**:* Infrastructures are systems with "humans in the loop". This is indeed the case for electricity networks. Several key human resources issues arise in bringing IT to improve the performance of electric power. The first is operator experience. The second is retaining professionals in the field of electric power engineering. The third is how users and consumers can interface with IT-enabled electric power systems.

***Operator Training**:* Several root causes of the August 14th outage point to lack of operators' situational awareness and coordination. IT has a key role to play in the optimization of operator interfaces and other human factors issues. Basically, the problem is finding the most effective way for machines and humans to work together, and the data glut and maintaining operator attention is largely at the center of the problem. Good operator interfaces provide adequate visualization of the state of the system, and they should be designed so that the user can remain tuned in to many different factors while giving active attention to only a few.

Much of the answer is simply a matter of how information is packaged for viewing. IT innovations are expected to have applications in personnel training and optimization of human performance, for example through the use of virtual reality for training for maintenance or rapid repair work, especially those involving hazardous situations. Voice recognition is another technology expected to come into broad use over the next decade; replacement of keyboarding with voice-based input capability could greatly streamline and simplify human interaction with computers and other electronic control equipment.

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, 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.

Retaining a Trained Workforce: A growing concern related to the human network is the erosion of technical knowledge within the power industry. To a large extent this is a matter of the retirement of seasoned power engineers, exacerbated by recent downsizing and reductions of in-house workforce. These key employees take their knowledge with them when they go. It will take a long time to recruit replacements. A second related issue is that new engineers are not entering the field rapidly enough to replace retirees. The average power engineer's age has increased significantly over the last two decades. A serious shortage of power engineers is developing, and is expected to continue for several decades.

Users: Operators and maintenance personnel are obviously "inside" these networks and can have direct, real-time effects on them. But 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 nature, of 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 everyone's water pressure. 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, 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.

Information Security: The electric power industry traditionally has been a vertically integrated industry that in some cases operated in pseudo-monopolistic fashion. However, the industry is currently undergoing restructuring, which frequently results in a break-up of the vertical structure. Additionally, there has been a significant move on the part of the control system suppliers to electric and petrochemical industries toward open, user-configurable systems utilizing real time communications. With a vertical structure, local and wide-area networks were sufficient to maintain a reasonably secure data network. However, deregulation and new networking technologies are making secure communications more important, and more difficult to develop and maintain.

Information security is concerned with the relationships between people and information. In these relationships, people are owners, custodians, creators, readers, modifiers, certifiers, or even subjects of the information. It follows then that the information itself is the object of various actions by people — creation, destruction, reading, modification, and certification. Information security is concerned with first defining appropriate relationships between people as actors and information resources as objects; these relationships are usually defined as a set of rules defining permitted actions. Not all threats come from outside the organization nor are all threats malicious.

Information security is also concerned with controlling the relationships between people and information so that information is managed according to well-defined rules. Some human agent or institutional agency of authority is usually charged with creating, communicating, applying, monitoring and enforcing these information security rules. Examples of contemporary information security rules are: rules for handling government classified documents; rules for ensuring client-attorney privilege or privacy of shared information; rules followed by corporate accountants and checked by financial auditors; and rules for ensuring accuracy and completeness of patients' health records. Generally these rules define information security controls based on properties of special classes of information; these properties fall into three broad categories: confidentiality of sensitive information; integrity and authenticity of critical information; and availability of necessary information. These principles need to be applied to the management of electricity systems, including the operator and managers of these systems.

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, 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 growing concern (CIAO 1997). It noted the damaging and dangerous ways 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 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.

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

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

Next Steps

Funding and sustaining innovations, such as the smart self-healing grid, remain a challenge as utilities must meet many competing demands on precious resources while trying to be responsive to their stakeholders, who tend to limit R&D investments to immediate applications and short-term return on investment. In addition, utilities have little incentive to invest in the longer term. For regulated investor–owned utilities there is added pressure caused by Wall Street to increase dividends.

Several reports and studies have estimated that for existing technologies to evolve and for the innovative technologies to be realized, a sustained annual research and development investment of $10 billion is required. However, the current level of R&D funding in the electric industry is at an all-time low. The investment rates for the electricity sector are the lowest rates of any major industrial sector with the exception of the pulp and paper industry. The electricity sector invests at most only a few tenths of a percent of sales in research — this in contrast to fields such as electronics and pharmaceuticals in which R&D investment rates have been running between 8 and 12 percent of net sales — and all of these industry sectors fundamentally depend on reliable electricity.

A balanced, cost-effective approach to investments and use of technology can make a sizable difference in mitigating the risk.

Acknowledgments

I developed most of the context and many of findings presented here while I was at the Electric Power Research Institute (EPRI) in Palo Alto (during 1998-2003), and for the Galvin Electricity Initiative (during 2005-2006). I gratefully acknowledge the feedback from Mr. John Voeller (the editor of this series). The support and feedback from numerous colleagues at EPRI, universities, industry, national laboratories, and government agencies with funding from EPRI, NSF and the ORNL is gratefully acknowledged.

Biography

Dr. S. Massoud Amin, Professor of Electrical and Computer Engineering, directs the Technological Leadership Institute (TLI, formerly CDTL), and holds the Honeywell/H. W. Sweatt Chair in Technological Leadership at the University of Minnesota. Before joining the University, 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. In the aftermath of 9/11 he directed all security research and development at EPRI.

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. Dr. Amin pioneered R&D in the smart "self-healing grid", and led the development of more than 24 technologies transferred to industry. Dr. Amin twice received Chauncey Awards at EPRI, the institute's highest honor.

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. He served as a member of the Board on Infrastructure and the Constructed Environment (BICE) at the U.S. National Academy of Engineering (2001-2007), and is on the Board on Mathematical Sciences and Applications (BMSA) at the National Academy of Sciences (2006-2009). Dr. Amin holds 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 in St. Louis, Missouri. He is the author or co-author of more than 170 research papers and the editor of seven collections of manuscripts. For additional publications, please see http://umn.edu/~amin

References

1. Amin and Schewe, "Preventing Blackouts," Scientific American, pp. 60-67, www.Sciam.com, May 2007

2. Amin and Gellings, "The North American power delivery system: Balancing market restructuring and environmental economics with infrastructure security," *Energy,* Vol. 31, Issues 6-7, pp. 967-999, May-June 2006

3. Amin and Wollenberg "Toward a Smart Grid," IEEE Power and Energy Magazine, Vol.3, No 5, pp. 34-38, Sept/Oct. 2005

4. Amin, "Energy Infrastructure Defense Systems," *Proceedings of the IEEE*, Vol. 93, Number 5, pp. 861-875, May 2005

5. Amin, "Restructuring the Electric Enterprise: Simulating the Evolution of the Electric Power Industry with Adaptive Agents," Chapter 3, pp. 27-50, in *Electricity Pricing in Transition,* Ahmad Faruqui and Kelly Eakin (editors), Kluwer Academic Publishers, September 2002

6. Amin, "National Infrastructures as Complex Interactive Networks," chapter 14 in: *Automation, Control, and Complexity: An Integrated Approach*, T. Samad & J. Weyrauch (Eds.), pp. 263-286, John Wiley and Sons Ltd., NY, March 2000

7. Amin, “Toward Self-Healing Infrastructure Systems,” *IEEE Computer Magazine*, pp. 44-53, Vol. 33, No. 8, Aug. 2000

8. Amin, “Toward Self-Healing Energy Infrastructure Systems,” *IEEE Computer Applications in Power*, pp. 20-28, Vol. 14, No. 1, January 2001

9. Amin, “Modeling and Control of Electric Power Systems and Markets,” *IEEE Control Systems Magazine*, pp. 20-25, Vol. 20, No. 4, Aug. 2000

10. Amin and Ballard, “Defining New Markets for Intelligent Agents,” *IEEE IT Professional*, pp. 29-35, Vol. 2, No. 4, July/Aug. 2000

11. *Special Issue of Proceedings of the IEEE on Energy Infrastructure Defense Systems*, (Guest editor: Amin), Vol. 93, Number 5, pp. 855-1059, May 2005

12. *Special issues of IEEE Control Systems Magazine on Control of Complex Networks,* (Guest editor: Amin), Vol. 21, No. 6, December 2001 and Vol. 22, No. 1, February 2002

13. *Special issue of IEEE Control Systems Magazine on Power Systems and Markets,* (Guest editor: Amin), pp. 20-90, Vol. 20, Number 4, Aug. 2000

14. *Network, Control, Communications and Computing Technologies in Intelligent Transportation Systems*, (Guest co-editors: Amin, Garcia-Ortiz and Wootton), *Mathematical and Computer Modeling*, Elsevier Science Ltd, Vol. 22, No. 4-7, 454 pp. , Aug.-Oct. 1995

15. Amin, “Electricity,” in *Digital Infrastructures: Enabling Civil and Environmental Systems through Information Technology*, R. Zimmerman and T. Horan (Editors), Chapter 7, pp. 116-140, July 2004

16. Amin, “Balancing Market Priorities with Security Issues: Interconnected System Operations and Control under the Restructured Electricity Enterprise,” IEEE Power and Energy Magazine, Vol.2, No 4, pp. 30-38, July/August 2004

17. Starr and Amin, “Global Transition Dynamics: Unfolding the Full Social Implications of National Decision Pathways,” 11 pp., submitted to the President of the US National Academy of Engineering, September 2003