

# System-of-Systems Approach

Massoud Amin

**Abstract** Energy, telecommunications, transportation, and financial infrastructures are becoming increasingly interconnected, thus, posing new challenges for their secure, reliable and efficient operation. All of these infrastructures are, themselves, complex networks, geographically dispersed, non-linear, and interacting both among themselves and with their human owners, operators, and users. No single entity has complete control of these multi-scale, distributed, highly interactive networks, nor does any such entity have the ability to evaluate, monitor, and manage them in real time. In fact, the conventional mathematical methodologies that underpin today's modeling, simulation, and control paradigms are unable to handle the complexity and interconnectedness of these critical infrastructures.

**Keywords** System-of-systems · Critical infrastructure interdependencies · Complex systems · Smart self-healing infrastructure · Security · Risk · Uncertain dynamic systems

## 1 Introduction

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,

---

M. Amin (✉)

Technological Leadership Institute, University of Minnesota, 290 McNamara Alumni Center, 200 Oak Street Southeast, Minneapolis, MN 55455, USA  
e-mail: amin@umn.edu

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 [1, 2]. 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 into other networks.

Modeling interdependent 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.

There is reasonable concern that 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 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.

In the aftermath of the tragic events of September 11th and recent natural disasters and major power outages, there are increased national and international concerns about the security, resilience and robustness of critical infrastructures in response to evolving spectra of threats. Secure and reliable operation of these networks is fundamental to national and international economy, security and quality of life.

Our work in this area draws from methods in statistical physics, complex adaptive systems, discrete-event dynamical systems, and hybrid, layered networks. Modeling complex systems is one of three main areas in our ongoing work. The others are measurement—to know what is or will be happening and develop measurement techniques for visualizing and analyzing large-scale emergent behavior—and management—to develop anticipatory distributed management and control systems to keep power and energy infrastructures robust and operational. From a broader viewpoint, *agility* and *robustness/survivability* of smart grids as large-scale dynamic networks that face *new* and *unanticipated* operating conditions is presented.

## 2 Definition of Critical Infrastructure

Executive Order 13010, signed by President Clinton in 1996, defined critical infrastructures as “so vital that their incapacity or destruction would have debilitating impact on the defense or economic security of the United States” and included “telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services and continuity of government”.

The U.S. Department of Homeland Security (DHS) in the National Infrastructure Protection Plan has expanded the concept to include “key resources” and added food and agriculture, health and healthcare, defense industrial base, information technology, chemical manufacturing, postal and shipping, dams (including locks and levees), government facilities, commercial facilities, critical manufacturing and national monuments and icons [3].

The Board on Infrastructure and the Constructed Environment (BICE) has argued that five “lifeline” infrastructures are the most critical because all the others depend on them for survival. These are power, telecommunications, transportation, water and wastewater systems [4]. This chapter focuses on these five, agreeing with the BICE, but expecting that the results will ultimately apply to many of the 18 sectors identified by DHS. The focus, as an example, will be the critical infrastructures of the United States (US), as well as the current practices and investments (or lack of) taking place.

## 3 Consequences of Aging Infrastructures

The infrastructures provide the lifelines on which our communities and our economy depend. Many of these, however, are aging in place, imposing risks of fatalities, serious injuries and massive economic disruptions. For example, in the United States:

### 3.1 Highways

The vast bulk of our major highways were built in the 1950s and 1960s and have been maintained largely at the level of hot-patching even as the number of vehicles has increased enormously. (New highway construction, however, has continued.) Between 1970 and 2002, passenger travel doubled, with a growth of another 67 % by 2022. The Federal Highway Administration (FHWA) currently considers one-third of the nation’s roads to be “poor,” “mediocre” or “fair”—all three categories requiring investment. The American Automobile Association estimates that as many as 12,000 lives (of a total of 44,000) could be saved if highways were

improved by adding lighting and guardrails and straightening dangerous curves. The Road Information Program estimated costs as much as \$220 billion a year, which includes car repairs (\$65B), congestion (\$78B) and accidents (\$77B)—the equivalent of nearly 2 % points of the national economy.

### ***3.2 Bridges***

The age of famous bridges is illuminating: New York's Brooklyn Bridge is over 120 years old and its George Washington Bridge is 75+ years; St. Louis's Eads Bridge is 130+; San Francisco's Bay Bridge and Louisiana's Huey P. Long Bridge are both 70+. The FHWA rates 13.1 % of America's highway bridges "structurally deficient" and an additional 13.6 % as "functionally obsolete". Most remain open to traffic. One of these was the I-35 bridge over the Mississippi River that collapsed, killing 13 people in 2007. Others were the I-95 Mianus River Bridge in Greenwich, Connecticut, where three people died in 1982, and the New York Thruway Bridge near Amsterdam, N.Y., where ten people perished in 1987. More than 1,500 bridges failed between 1966 and 2005, 60 % due to soil erosion around the bridge supports, a potential weakness seldom checked in inspections.

### ***3.3 Dams and Levees***

Hoover Dam is 74 years old; the Wilson Dam, 84; the Grand Coulee Dam, 66; and all of the dams over the Tennessee River are more than 60 years old. The number of "high hazard" dams, whose failure would endanger human life, has increased from 9,281 in 1998 to 10,213 in 2007. In the past 2 years, more than 67 dam incidents, including 29 dam failures, were reported to the National Performance of Dams program. States report more than 3,500 "unsafe" dams with conditions that could cause them to fail. Seepage has been noted under the 55-year-old Wolf Creek Dam, forcing its water level to be lowered to avoid devastating failure of the dam holding the largest man-made reservoir east of the Mississippi and the flooding of Nashville and neighboring communities. Precautions came too late for the levees protecting New Orleans after Hurricane Katrina in 2005, killing almost 1,500 and making thousands refugees, many still far from returning to their homes.

### ***3.4 Electric Power***

Modern life depends on electricity. The transmission of electric power is largely based on technologies installed more than 50 years ago. From 1988 to 1998, US electricity demand rose by nearly 30 % while the transmission network's capacity

grew by only 15 %. The Electric Power Research Institute (EPRI) anticipated that the disparity would further increase during the period 1999–2009: The Institute projects demand to grow by 20 % and system capacity to increase by just 3.5 % [5]. The Northeast Blackout of 2003 [6], caused by human error and transmission lines contacting improperly trimmed trees, resulted in the shutdown of more than 100 power plants, denied power to 40 million Americans (one-seventh of the national population) and ten million Canadians (one-third of its national population), with a cost of more than six billion dollars. Water and wastewater plants were idled, transportation by all modes slowed to a stop, communications and industry were largely stopped and at least eleven fatalities were reported. In a CNN interview about the Blackout, Governor Bill Richardson of New Mexico, former U.S. Secretary of Energy, described the U.S. as “a major superpower with a third-world electrical grid” [7]. In the 1960s and before, blackouts lasting more than more than a few hours were rare but, by the mid-1990s, their frequency rose to yearly or greater. An EPRI survey of industry which tracked the cost of blackouts over this time indicated a rise from insignificant levels to \$100 billion/year. The White House’s National Energy Policy of 2001 suggests that the nation will need 1,300–1,900 new power plants in the next two decades, but this ignores the investments needed in transmission and distribution.

### ***3.5 Water and Wastewater***

Many cities, especially in the east and northwest, have water systems containing components more than 100 years old, including asbestos-cement pipes, lead pipes, even wooden pipes and storage tanks. New York City’s fresh water is transmitted through two tunnels, built in 1917 and 1936 (a third will be completed by 2020 if the schedule holds). A survey by EPA found that in systems that serve more than 100,000 people, about 30 % of the pipes are between 40 and 80 years old and about 10 % of the pipes are more than 80 years old. Some systems treat as much as 100 % more water than is consumed due to high rates of leakage from old transmission and distribution pipes. The U.S. Conference of Mayors reports that more than half of a 330-city survey suffer annual or more frequent water main breaks—some as many as 50 or more per year. During the 2003 Northeast Blackout, emergency generators in New York City failed and some 30 million gallons of raw sewage were dumped into the East River. In New York and many other cities, raw sewage mixes into waterways with every significant rainstorm. Sanitary sewer overflows caused by blocked or broken pipes result in the release of as much as 10 billion gallons of raw sewage annually, according to the EPA. During blackouts, pressure drops in water mains, impeding the cooling of high-rise buildings, severely limiting the ability to control fires, and risking introduction of contaminants into drinking water.

The consequences of aging infrastructures are dire and add to the congestion costs of inadequate infrastructure capacity in parts of the country undergoing

economic or population growth. A large and growing sentiment among the American public cries out for government at all levels and the private utilities that provide these services to invest in new, renewal and replacement infrastructure necessary to avoid or mitigate such consequences.

## 4 Recent and Near-Term Infrastructure Investment Rates

Hurricane Katrina and the collapse of Minneapolis's I-35 bridge have stimulated public awareness of the necessity for accelerated programs of new investment, replacement, rehabilitation and renewal. Most Americans are unaware of the magnitude or trends in American investment in infrastructure. In the sources cited below, the definition of investments included in "infrastructure" varies widely. Where possible, the text or figure labels will make clear what is included.

Most public infrastructure investment is in transportation and water, while most private sector infrastructure is in energy and telecommunications. Public investment in infrastructure has grown steadily since World War II (Fig. 1a), but, as a portion of Gross Domestic Product, has declined more or less steadily since the late 1950s (Fig. 1b).

Relative to its international competitors, the U.S. ranks 13th in infrastructure investment among OECD nations (Fig. 2a). Both China and India, not OECD members, also rank higher than the U.S. This is not a recent trend. U.S. infrastructure investment has been well below the average of the leading 17 countries in every decade since at least the 1970s (Fig. 2b, c).

In a more detailed look, capital investment by public and private sectors in selected infrastructures in 2004, the last year of complete data, totaled more than \$300 billion (Table 1), split about evenly between the public (mostly in transportation and water/wastewater) and the private sector (mostly in energy and telecommunications).

## 5 The Costs of Renewal or Replacement

In brief, vast sums of money are being and will be invested. The American Society of Civil Engineers (ASCE), however, has judged that it will not be nearly enough, estimating that \$2.2 *trillion* dollars will be required to restore the United States infrastructure to a sound level [8]. Some examples illustrate this pressing need:

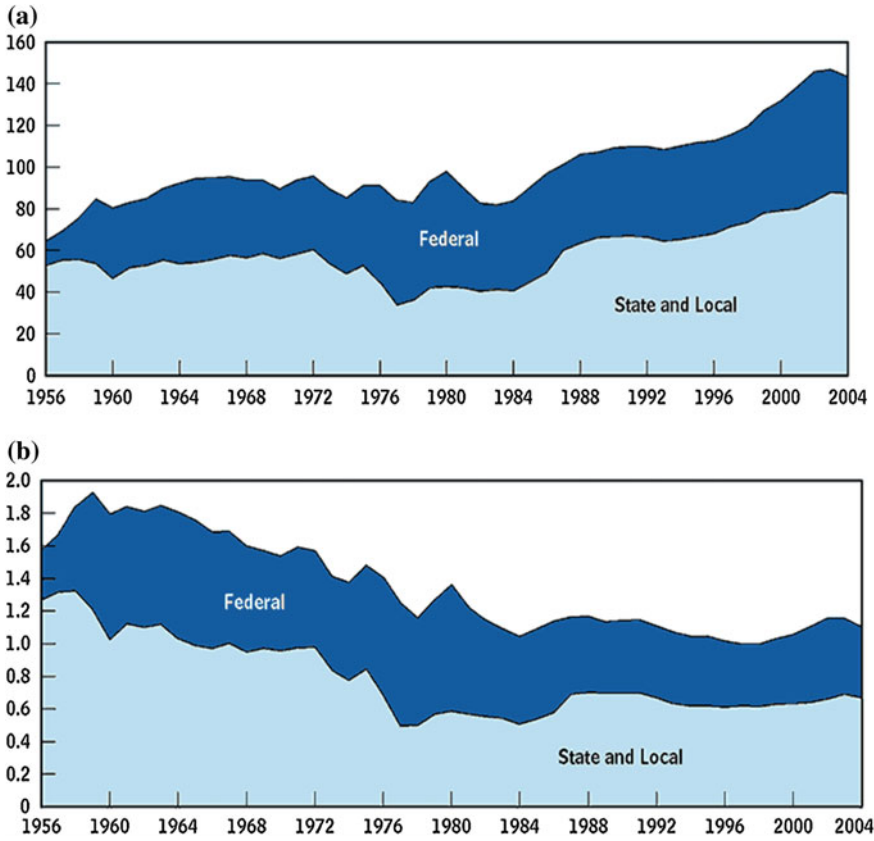
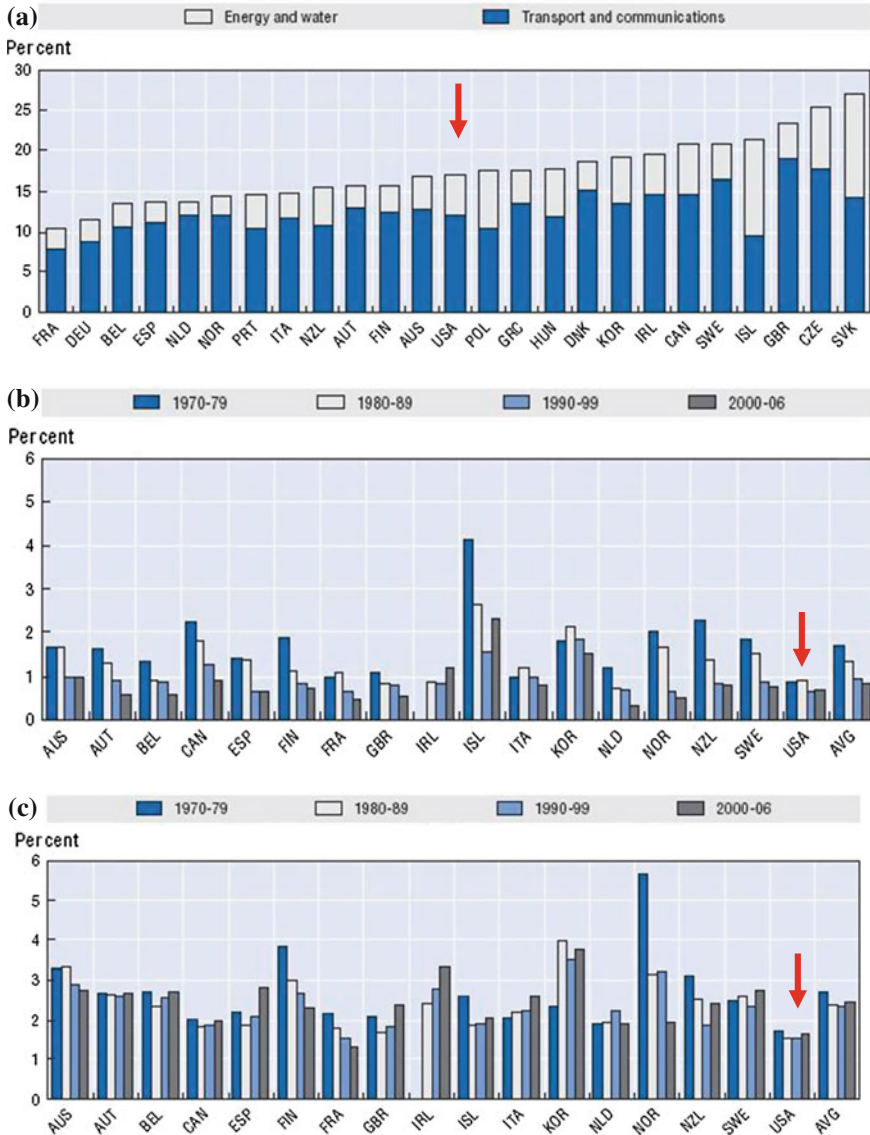


Fig. 1 Public capital spending on transportation and water infrastructure, 1956–2004 (Source CBO, 2008). a Billions of 2006 dollars. b Percentage of gross domestic product

### 5.1 Highways

The American Association of State Highway and Transportation Officials, Federal Highway Administration and ASCE all point to the need for massive increases in capital outlays by all levels of government to reach the cost-to-maintain level, and roughly double that to reach the cost-to-improve level. ASCE is calling for \$186 billion annually, compared to current actual outlays, well below even maintenance level.



**Fig. 2** U.S. infrastructure relative to other OECD nations (Source OECD, going for growth 2009). **a** Infrastructure investment as a percentage of total fixed investment, averages over latest 5 years. **b** Electricity, gas and water investment as a percentage of GDP. **c** Transport and communications investment as a percentage of GDP



**Table 1** Capital spending on infrastructure in 2004, by category (Billions of 2004 dollars; columns may not add due to rounding)

	Public <sup>a</sup>		Total			Amer. recovery and reinvestment act <sup>b</sup>
	Federal	State	Public	Private	Total	
Transportation						
Highways	30.2	36.5	66.7	n.a.	66.7	27.5
Mass transit	7.6	8.0	15.5	0	15.5	8.4
Railroads	0.7	0	0.7	6.4	7.1	9.3
Aviation	5.6	6.8	12.4	2.0	14.4	2.1
Water transportation	0.7	1.7	2.4	0.1	2.5	0.2
Total transportation	44.7	53.0	97.7	8.5	106.2	47.5
Drinking water and wastewater	2.6	25.4	28.0	n.a.	28.0	7.4
Energy	1.7	7.7	9.4	69.0	78.4	36.8
Telecommunications	3.9	n.a.	3.9	68.6	72.5	7.2
Pollution control and waste disposal	0.8	1.8	2.6	3.6	6.2	0.8
Water and other natural resources	7.1	4.3	11.3	n.a.	11.3	6.1
Total, non-transportation	16.1	39.2	55.2	141.2	196.4	58.3
Total	60.8	92.2	152.7	149.7	302.6	105.8

<sup>a</sup> Peter R. Orszag, Director, Congressional Budget Office, “Investing in Infrastructure,” Testimony before the Committee on finance, U.S. Senate, July 10, 2008, obtained from <http://www.cbo.gov/ftpdocs/95xx/MainText.1.2.shtml>, accessed on June 22, 2009. The original table included investments for schools (\$99.7 billion), prisons (\$2.9 billion) and postal facilities (\$0.9 billion), for a total of \$406.1 billion. These were deleted as not being parts of the infrastructures of interest in this chapter

<sup>b</sup> Interpreted from U.S. Congress, House Committee on Appropriations, “Summary: American Recovery and Reinvestment—Conference Agreement,” February 13, 2009

## 5.2 Bridges

ASCE estimates that it will cost \$17 billion per year over 20 years to eliminate bridge deficiencies compared to the \$10.5 billion currently being spent.

## 5.3 Dams and Levees

ASCE did not estimate the cost of restoring American dams to safety, but states that \$100 billion is needed to repair and rehabilitate U.S. levees.

## 5.4 Electrical Power

ASCE estimates that \$1.5 trillion in new investments will be needed by 2030.

## 5.5 Water and Wastewater

For drinking water, EPA estimates potential funding gaps as high as \$263 billion by 2019. For wastewater, EPA and ASCE estimate \$390 billion is needed to replace existing wastewater infrastructure systems and to build new ones.

## 6 Interdependent Infrastructures

Valuation of infrastructure investments is complicated by the dependencies and interdependencies *among* the constituent system elements of some infrastructures (e.g., the electricity system of power plants, substations, and transmission and distribution lines; the transportation system of ports, rail, barges, roads, highways, airports, bridges and tunnels; water storage dams and water supply). Interdependencies also exist *between* infrastructures, such as:

- Cooling of power plants uses about 40 % of the fresh water withdrawals, as much as all the nation's irrigation requirements;
- Water-related energy requirements are reported in California to account for 19 % of all power generated in the state;
- The Northeast Blackout of 2003 and Hurricane Isabel of 2005 illustrated how loss of electricity can cause loss or diminution of communications, water and sanitation services, automotive fuel pumping, rail transportation, traffic control, food distribution, building cooling, fire protection, hospital services and numerous other life-essential services—even power generation itself where cooling water relies on electrically powered pumps;
- The failure of one infrastructure in New Orleans, the levee system, caused the near total collapse of all the infrastructures—indeed, of basic human viability—following Hurricane Katrina.

Such interdependencies can and do result in “cascading failures”. These interdependencies make it difficult for decision-makers in the responsible institutions and organizations to consider *all* the consequences as they decide where to allocate their severely limited funds for infrastructure replacement and restoration. Often, whole metropolitan areas or even multi-state regions can be impacted by a single failure, such as a poorly trimmed tree in the wrong place. The interactions among infrastructures necessitate a “system-of-systems” analytic approach in which the

assets and networks of each infrastructure are assessed in the context of their consequences on all the impacted infrastructures and communities.

## 7 Infrastructure Investment Decision-Making

Infrastructure investment is a major societal challenge but the United States is currently ill-equipped to make the needed priority and resource allocation decisions. Rationally allocating such funds is complicated by long-standing, ingrained practices—“earmarks” and “pork-barrel” funding for special projects (some necessary, others perhaps less so); “trust-fund” single-purpose financing of some infrastructures (e.g., roads) and the absence of such funds for others (e.g., drinking water); formulaic allocation of block grants based on criteria at best loosely related to infrastructure requirements on the ground. Congressional committees and subcommittees authorize and appropriate funds that flow directly to specialized Federal agencies and, from there, often to state and local specialized agencies, creating “stove-pipes” from funds source to sink, from concept to spade tip, without any challenge of comparative assessment of the benefits and costs of the investments. The absence of a central clearing point or set of standard metrics makes essential comparisons for rational optimization impossible [9].

Powerful vested interests have a stake in maintaining the current jumble of allocation schemes because they are in the position to exercise power, take credit, and/or receive funding. Starting with Congressional earmarks and horse-trading, through trust funds and federal agency formula grants, clear through to state and local elected and appointed officials’ final decisions, there is little or no comprehensive, comparative analysis of value, sustainability, risk or resilience of potential infrastructure projects. Furthermore, certain individuals at each level profit from those arrangements. Availability of a competent, standardized technology for valuing and prioritizing infrastructure investments would permit the adaptation of existing processes to provide a more rational analytic underpinning and more nearly optimal allocation of investment funds.

Further, there are few incentives for the needed design and advocacy to be undertaken. Infrastructures are, almost by definition, networked and highly interdependent, so an improved valuation and selection method requires contributions from diverse disciplines and industries that seldom collaborate, making it unlikely that the needed research will be undertaken without Federal support.

To date, the combination of political and functional barriers has resulted in there being no comprehensive, comparative method for rationally undertaking these critically important decisions. Politically robust forces benefit materially from the current jumble of allocation processes and the requirements for constructing new, more competent methods cover too broad and diverse a set of disciplines to be feasible in the absence of a concentrated Federal effort. The opportunity cost of continuing with the present system will be enormous as the

United States rushes to make investments that will entail jobs, while potentially wasting tens or hundreds of billions of dollars.

According to a distinguished bipartisan commission that included two sitting Senators, two former Senators, three sitting governors and a number of former cabinet members and ambassadors, convened by the Center for Strategic and International Studies (CSIS), “America’s economic well-being and physical security depend on safe and reliable... infrastructure... But we are both under-investing in infrastructure and investing in the wrong projects: *new investments are critically needed, but we lack the policy structures to make the correct choices and investments...* A centralized infrastructure project approval process would force all infrastructure modes to be evaluated using common methods and parameters” (emphasis in original) [10]. The commission was not specific as to a particular set of “common methods and parameters”. Establishment of objective, transparent methods that use “common methods and parameters” that yield directly comparable estimates of benefits and costs of alternative investments is the *sine qua non* of rational allocation of limited resources.

Rehabilitating or renewing aging infrastructures often yields little near-term revenue or profit to companies and seldom reflects great credit on public officials faced with competing, more visible demands. Strong incentives encourage deferral of these investments. Accordingly, investment in older infrastructures lags behind the rate of deterioration. Conversely, most new infrastructure development conspicuously adds local employment, so tends to highlight politicians who can take credit, accounting for much of the “earmarking” for favored projects. Ribbon cutting for new, highly visible facilities attracts far more media attention than rehabilitating or upgrading existing structures.

The diversity among the infrastructures and the complexity of the interdependencies among them encourage decision-makers to evaluate their investment options from their own very limited perspective, even though the full consequences may have very far-reaching effects. Each infrastructure sector and each operator may use any perspective, methodology, metrics or level of rigor it chooses, within only broad guidelines, often prescribed by the oversight or funding authority. Numerous criteria and metrics for valuing benefits and costs are used, and usually, no attempt is made at optimizing the allocation of the resource base for aging infrastructures. Across all infrastructures, local to national in scale, this results in an absolute inability to compare one project’s benefits or costs to competing project opportunities. At best, resource allocation decisions can be “sub-optimized” as each oversight or funding authority, functional agency, utility operator or company makes its choices by its own criteria within its own “stove-pipe”. The overall national infrastructure portfolio cannot be optimized in any sense, so scarce resources are expended for less benefit than a more comprehensive approach could accomplish.

## **8 A Case Study: Interdependent End-to-End Power Infrastructure and its Couplings**

Power, telecommunications, banking and finance, transportation and distribution, and other infrastructures are becoming more and more congested partially due to dramatic population growth, particularly in urban centers. These infrastructures 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) by telecommunications, markets and computer networks. Furthermore, reliable electric service is critically dependent on the whole grid's ability to respond to changed conditions instantaneously. Dependencies of other infrastructures on electric power grid telecommunications, markets, and so much else...

Secure and reliable operation of complex networks poses significant theoretical and practical challenges in analysis, modeling, simulation, prediction, control, and optimization. The pioneering initiative in the area of complex interactive networks and infrastructure interdependency modeling, simulation, control and management was launched and successfully carried out its goals during 1998–2002, through the Complex Interactive Networks/Systems Initiative (CIN/SI) [5, 11], studied closely challenges to the interdependent electric power grid, energy, sensing and controls, communications, transportation, and financial infrastructures. It comprised of six university research groups consisting of 108 university faculty members and over 220 researchers involved in the joint Electric Power Research Institute (EPRI) and U.S. Department of Defense program. During 1998–2002, CIN/SI developed modeling, simulation, analysis, and synthesis tools for damage-resilient control of the electric power grid and interdependent infrastructures connected to it.

Earlier work by the author during the 1990s on damaged F-15 aircrafts in part provided background for the creation, successful launch, and management of research programs for the electric power industry, including the EPRI/DOD CIN/SI mentioned above, which involved six university research consortia, along with two energy companies, to address challenges posed by our critical infrastructures. This work was done during the period of 1998 to early 2002. CIN/SI laid the foundation for several on-going initiatives on the self-healing infrastructure and subsets focusing on smart reconfigurable electrical networks. These have now been under development for some time at several organizations, including programs sponsored by the U.S. NSF, DOD, DOE, and EPRI, including EPRI's "Intelligrid" program and the US Department of Energy's "Gridwise," "Modern Grid," and "Smart Grid" initiatives.

To provide a context for this, the EPRI/DOD CIN/SI aimed to develop modeling, simulation, analysis, and synthesis tools for robust, adaptive, and reconfigurable control of the electric power grid and infrastructures connected to it. In

part, this work showed that the grid can be operated close to the limit of stability given adequate situational awareness combined with better sensing of system conditions, communication, and controls. A grid operator is similar to a pilot flying the aircraft, monitoring how the system is being affected, how the “environment” is affecting it and having a solid sense of how to steer it in a stable fashion by keeping the lines within their operating limits while helping an instantaneous balance between loads (demand) and available generation—grid operators often make these quick decisions under considerable stress. Given that in recent decades we have reduced the generation and transmission capacity, we are indeed flying closer to the edge of the stability envelope.

As an example, one aspect of the Intelligrid program aimed at enabling grid operators greater look-ahead capability and foresight into the road-ahead overcoming limitations of the current schemes which at best have over a 30-s delay in assessing system behavior—analogue to driving the car by looking into the rear-view mirror instead of the road ahead. This tool using advanced sensing, communication and software module was proposed during 2000–2001 and the program was initiated in 2002 [12]. This advanced simulation and modeling program promotes greater grid self-awareness and resilience in times of crisis in three ways: by providing faster-than-real-time, look-ahead simulations (analogue to master chess players rapidly expanding and evaluating their various options under time constraints) and thus avoiding previously unforeseen disturbances; by performing what-if analysis for large-region power systems from both operations and planning points of view; and by integrating market, policy and risk analysis into system models, and quantifying their integrated effects on system security and reliability.

Focusing on the electric power sector, the power outages and power quality disturbances cost the U.S. economy over \$80 billion annually, and sometimes up to \$188 billion in a single year. Transmission and distribution losses in the U.S. were about 5 % in 1970, and grew to 9.5 % in 2001, due to heavier utilization and more frequent congestion. Regarding the former, starting in 1995, the amortization/ depreciation rate exceeded utility construction expenditures. Since that crossover point in 1995, utility construction expenditures have lagged behind asset depreciation. This has resulted in a mode of operation of the system that is analogue to harvesting more rapidly than planting replacement seeds. As a result of these diminished “shock absorbers,” the electric grid is becoming increasingly stressed, and whether the carrying capacity or safety margin will exist to support anticipated demand is in question.

To assess impacts one can use actual electric power outage data for the U.S., which are generally available from several sources, including from the U.S. DOE’s Energy Information Administration (EIA) and from the North American Electric Reliability Corporation (NERC). In general, the EIA database contains more events, and the NERC database gives more information about the events. Both databases are extremely valuable sources of information and insight. In both databases, a report of a single event may be missing certain data elements, such as the amount of load dropped or the number of customers affected. In the NERC database, the amount of load dropped is given for the majority of the reported

events, whereas the number of customers affected is given for less than half the reported events. Analyses of these data collected revealed that in the period from 1991 to 2000, there were 76 outages of 100 MW or more in the second half of the decade, compared to 66 such occurrences in the first half (Fig. 3) [13]. Furthermore, there were 41 % more outages affecting 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). In addition, between 1996 and 2000, outages affected 15 % more consumers than they did between 1991 and 1995 (the 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). Similar results were determined for a multitude of additional statistics such as the kilowatt magnitude of the outage, average load lost, etc. These trends have persisted in this decade. NERC data show that during 2001–2005 we had 140 occurrences of over 100 MW dropped, and 92 occurrences of over 50,000 or more consumers affected.

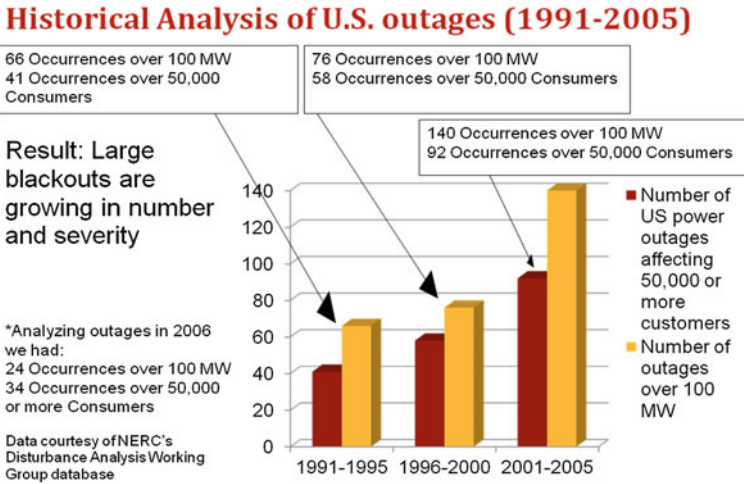
The U.S. electrical grid has been plagued by ever more and ever worse blackouts over the past 15 years. In an average year, outages total 92 min per year in the Midwest and 214 min in the Northeast. Japan, by contrast, averages only 4 min of interrupted service each year [14]. The outage data excludes interruptions caused by extraordinary events such as fires or extreme weather.

Two sets of data, one from the U.S. Department of Energy's Energy Information Administration (EIA) and the other from the North American Electric Reliability Corp. (NERC) are analyzed below. Generally, the EIA database contains more events, and the NERC database gives more information about the events, including the date and time of an outage, the utility involved, the region affected, the quantity of load dropped, the number of customers affected, the duration of the outage, and some information about the nature of the event. The narrative data in the NERC (and also the EIA) databases are sufficient to identify factors, such as equipment failure or severe weather (or a combination of both!) that may have contributed to an outage. Establishment of the precise cause is beyond the scope of most of the narratives. Both databases are extremely valuable sources of information and insight.

In both databases, a report of a single event may be missing certain data elements such as the amount of load dropped or the number of customers affected. In the NERC database, the amount of load dropped is given for the majority of the reported events, whereas the number of customers affected is given for less than half the reported events. In the EIA database, the number of customers affected is reported more frequently than the amount of load dropped.

In both sets, each 5-year period was worse than the preceding one: According to data assembled by the U.S. Energy Information Administration (EIA) for most of the past decade, there were 156 outages of 100 MW or more during 2000–2004; such outages increased to 264 during 2005–2009. The number of U.S. power outages affecting 50,000 or more consumers increased from 149 during 2000–2004 to 349 during 2005–2009, according to EIA (Fig. 4).

In 2003 EIA changed their reporting form from EIA-417R to OE-417. Both forms were attached with descriptions of reporting requirements (page 3 and page



**Fig. 3** U.S. electric power outages over 100 MW and affecting over 50,000 consumers (1991–2005)

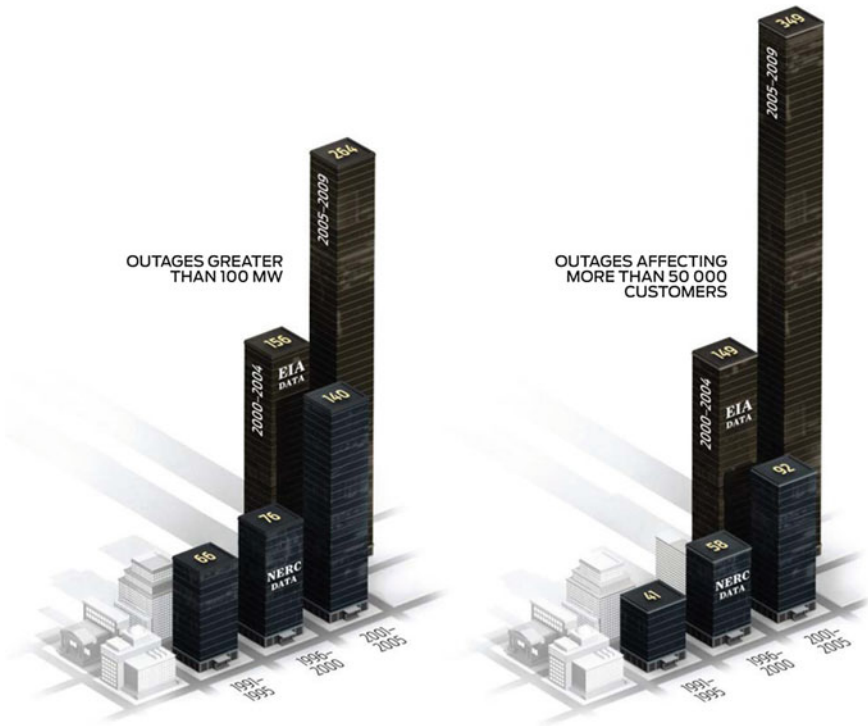
6 respectively). In all, the reporting requirements are very similar, with OE-417 being a little more stringent. The main change in the requirement affecting the above figures is that all outages greater than 50,000 customers for 1 h or more be reported in OE-417, where it was only required for 3 h or more in EIA-417R prior to 2003. Adjusting for the change in reporting in 2003 (using all the data from 2000–2009 and only counting the outages that met the less stringent requirements of the EIA-417R form used from 2000–2002), there were 152 outages of 100 MW or more during 2000–2004; such outages increased to 248 during 2005–2009. The number of U.S. power outages affecting 50,000 or more consumers increased from 130 during 2000–2004 to 272 during 2005–2009 (Fig. 5).

In summary the number of outages adjusted for 0.9 % annual increase in load and adjusted for change in reporting in 2003 is:

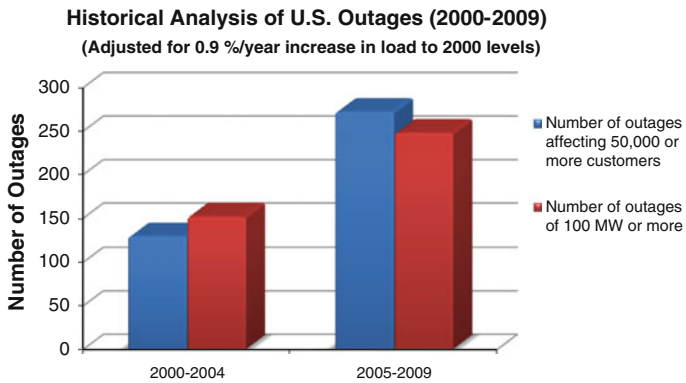
	Occurrences of 100 MW or more	Occurrences of 50,000 or more consumers
2000–2004	152	130
2005–2009	248	272

As an energy professional and electrical engineer, I cannot imagine how anyone could believe that in the United States we should learn to “cope” with these increasing blackouts—and that we do not have the technical know-how, the political will, or the money to bring our power grid up to 21st century standards. Coping as a primary strategy is ultimately defeatist. We absolutely can meet the needs of a pervasively digital society that relies on microprocessor-based devices in vehicles, homes, offices, and industrial facilities. And it is not just a matter of





**Fig. 4** Power outages have steadily increased [14]. (Research was supported by a grant from the NSF and a contract with the Sandia National Labs)



**Fig. 5** U.S. electric power outages over 100 MW and affecting over 50,000 consumers during 2000–2009, adjusted for 0.9 % annual increase in load and adjusted for change in reporting in 2003 (using all the data from 2000–2009 and only counting the outages that met the less stringent requirements of the EIA-417R form used during 2000–2002)

“can”. We must—if we want to continue on the road of technological advancement. However, it will not be easy or cheap [13, 15].

## **9 Background: Where Are We and How Did We Get Here?**

The existing electricity infrastructure evolved to its technology composition today from the convolution of several major forces, only one of which is technologically based. Today opportunities and challenges persist in world-wide electric power networks. These include: reducing transmission congestion, increasing system/cyber security, increasing overall system and end-use efficiency while maintaining reliability—many other challenges engage those who plan for the future of the power grid: producing power in a sustainable manner (embracing renewable fuels while accounting for their scalability limitations, e.g., increased use of land and natural resources to produce higher renewable electricity will not be sustainable, thus not being able to lower emissions from existing generators), delivering electricity to those who do not have it (not just on the basis of fairness but also because electricity is the most efficient form of energy, especially for things like lighting), and using electricity more wisely as a tool of economic development, and pondering the possible revival of advanced nuclear reactor construction. To prepare for a more efficient, resilient, secure and sustainable electrical system it is helpful to remember the historical context, associated pinch-points and forcing functions.

The trends of worldwide electrical grid deployment, costing trillions of dollars and reaching billions of people, began very humbly. Some obvious electrical and magnetic properties were known in antiquity. In the 17th and 18th centuries, partially through scientific experiments and partially through parlor games, more was learned about how electric charge is conducted and stored. But only in the 19th century, with the creation of powerful batteries, and through insights about the relations between electric and magnetic force could electricity in wires service large scale industries—first the telegraph and then telephones.

And only in the 1880s did the first grids come into being for bringing electrical energy to a variety of customers for a variety of uses, at first mostly for illumination but later for turning power machines and moving trolley cars. The most important of these early grids, the first established big city grid in North America, was the network built by Thomas Edison in lower Manhattan. From its power station on Pearl Street, practically in the shadow of the Brooklyn Bridge, Edison’s company supplied hundreds and then thousands of customers. Shortly thereafter, Edison’s patented devices, and those of his competitors—devices such as bulbs, generators, switching devices, generators, and motors—were in use in new grids in towns all over the industrialized world.

From a historical perspective the electric power system in the U.S. evolved in the first half of the 20th century without a clear awareness and analysis of the system-wide implications of its evolution. In 1940, 10 % of the energy consumption in America was used to produce electricity. By 1970, this had risen to 25 %, and by 2002 it had risen to 40 %. (Worldwide, current electricity production is near 15,000 billion Kilowatt-hours per year, with The United States, Canada, and Mexico responsible for about 30 % of this consumption). This grid now underlies every aspect of our economy and society, and it has been hailed by the National Academy of Engineering as the 20th century's engineering innovation most beneficial to our civilization. The role of electric power has grown steadily in both scope and importance during this time and electricity is increasingly recognized as a key to societal progress throughout the world, driving economic prosperity, security and improving the quality of life. Still it is noteworthy that at the time of this writing there are about 1.4 billion people in the world with no access to electricity, and another 1.2 billion people have inadequate access to electricity (meaning that they experience outages of 4 h or longer per day).

Once "loosely" interconnected networks of largely local systems, electric power grids increasingly host large-scale, long-distance wheeling (movement of wholesale power) from one region or company to another. Likewise, the connection of distributed resources, primarily small generators at the moment, is growing rapidly. The extent of interconnectedness, like the number of sources, controls, and loads, has grown with time. In terms of the sheer number of nodes, as well as the variety of sources, controls, and loads, electric power grids are among the most complex networks made.

In the coming decades, electricity's share of total energy is expected to continue to grow, as more efficient and intelligent processes are introduced into this network [12]. Electric power is expected to be the fastest-growing source of end-use energy supply throughout the world. To meet global power projections, it is estimated by the U.S. DOE/EIA that over \$1 trillion will have to be spent during the next 10 years. The electric power industry has undergone a substantial degree of privatization in a number of countries over the past few years. Power generation growth is expected to be particularly strong in the rapidly growing economies of Asia, with China leading the way.

The electric power grid's emerging issues include creating distributed management through using distributed intelligence and sensing; integration of renewable resources; use of active-control high-voltage devices; developing new business strategies for a deregulated energy market; and 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.

As an example of historical bifurcation points, the 1965 Northeast blackout not only brought the lights down, it also marked a turn in grid history. The previous economy of scale, according to which larger generators were always more efficient

than small machines, no longer seemed to be the only risk-managed option. In addition, in the 1970s two political crises—the Mideast war of 1973 and the Iranian Revolution in 1979—led to a crisis in fuel prices and a related jump in electric rates. For the first time in decades, demand for electricity stopped growing. Moreover, the prospects of power from nuclear reactors, once so promising, were now under public resistance and the resultant policy threats. Accidents at Brown's Ferry, Alabama in 1974 and Three Mile Island, Pennsylvania in 1979, and rapidly escalating construction costs caused a drastic turnaround in orders for new facilities. Some nuclear plants already under construction were abandoned.

In the search for a new course of action, conservation (using less energy) and efficiency measures (to use available energy more wisely) were put into place. Electrical appliances were re-engineered to use less power. For example, while on the average today's refrigerators are about 20 % larger than those made 30 years ago, they use less than half the electricity of older models. Furthermore, the Public Utility Regulatory Policy Act (PURPA) of 1978 stipulated that the main utilities were required to buy the power produced by certain independent companies which co-generated electricity and heat with great efficiency, providing the cost of the electricity was less than the cost it would take the utilities to make it for their own use.

What had been intended as an effort to promote energy efficiency, turned out, in the course of the 1980s and 1990s, to be a major instigator of change in the power industry as a whole. First, the independent power producers increased in size and in number. Then they won the right to sell power not only to the neighboring utility but also to other utilities further away, often over transmission lines owned by still other companies. With the encouragement of the Federal Energy Regulatory Commission (FERC), utilities began to sell off their own generators. Gradually the grid business, which for so long had operated under considerable government guidelines since so many utilities were effective monopolies, became a confusing mixture of regulated and unregulated companies.

Opening up the power industry to independent operators, a business reformation underway for some years in places like Chile, Australia, and Britain (where the power denationalization process was referred to as "liberalization"), proved to be a bumpy road in the US. For example, in 2001 in the state of California the effort to remove government regulations from the sale of electricity, even at the retail level, had to be rescinded in the face of huge fluctuations in electricity rates, rolling blackouts, and amid allegations of price-fixing among power suppliers. Later that year, Enron, a company that had grown immense through its pioneering ventures in energy trading and providing energy services in the new freed-up wholesale power market, declared bankruptcy.

Restructuring of the US power grid continues. Several states have put deregulation into effect in a variety of ways. New technology has helped to bring down costs and to address the need for reducing emission of greenhouse gases during the process of generating electricity. Examples include high-efficiency gas turbines, integrated "microgrids" of small generators (sometimes in the form of solar cells or fuel cells), and a greater use of wind turbines.

Much of the interest in restructuring has centered around the generation part of the power business and less on expanding the transmission grid itself. About 25 years ago, the generation capacity margin, the ability to meet peak demand, was between 25 and 30 %—it has now reduced to less than half and is currently at about 10–15 %. These “shock absorbers” have been shrinking; e.g., during the 1990s actual demand in the U.S. increased some 35 %, while transmission capacity has increased only 18 %. In the current decade, the demand is expected to grow about 20 %, with new transmission capacity lagging behind at under 4 % growth.

In the past, extra generation capacity served to reduce the risk of generation shortages in case equipment failed and had to be taken out of production, or in case there was an unusually high demand for power, such as on very hot or cold days. As a result, capacity margins, both for generation and transmission, are shrinking. Other changes add to the pressure on the national power infrastructure as well. Increasing inter-regional bulk power transactions strain grid capacity. New environmental considerations, energy conservation efforts, and cost competition require greater efficiency throughout the grid.

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 most visible parts of a larger and growing US energy crisis are the result of years of inadequate investments in the infrastructure. The reason for this neglect is caused partly by uncertainties over what government regulators will do next and what investors will do next.

Growth, environmental issues, and other factors contribute to the difficult challenge of ensuring infrastructure adequacy and security. Not only are infrastructures becoming more complexly interwoven and more difficult to comprehend and control, there is less investment available to support their development. Investment is down in many industries. For the power industry, direct infrastructure investment has declined in an environment of regulatory uncertainty due to deregulation, and infrastructure R&D funding has declined in an environment of increased competition because of restructuring. Electricity investment was not large to begin with. Presently the power industry spends a smaller proportion of annual sales on R&D than do the dog foods, leather, insurance, or many other industries—less than 0.3 %, or about \$600 million per year.

Most industry observers recognize this shortage of transmission capability, and indeed many of the large blackouts in recent years can be traced to transmission problems, either because of faults in the lines themselves or in the coordination of power flow over increasingly congested lines. However, in the need to stay “competitive,” many energy companies, and the regional grid operators that work with them, are “flying” the grid with less and less margin for error. This means keeping costs down, not investing sufficiently in new equipment, and not building new transmission highways to free up bottlenecks.

## 10 A Stressed Infrastructure

From a broader view, the North American electricity infrastructure is vulnerable to increasing stresses from several sources. One stress is caused by an imbalance between growth in demand for power and enhancement of the power delivery system to support this growth. From 1988 to 1998, the United States electricity demand rose by nearly 30 %, but the capacity of its transmission network grew by only 15 %. This disparity increased from 1999 to 2009: demand grew by about 20 %, while planned transmission systems grow by only under 3.8 % [1]. Along with that imbalance, today's power system has several sources of stress:

- *Demand is outpacing infrastructure expansion and maintenance investments.* Generation and transmission capacity margins are shrinking and unable to meet peak conditions, particularly when multiple failures occur while electricity demand continues to grow.
- *The transition to deregulation is creating new demands that are not being met.* The electricity infrastructure is not being expanded or enhanced to meet the demands of wholesale competition in the industry; so connectivity between consumers and markets is at a gridlock.
- *The present power delivery infrastructure cannot adequately handle those new demands of high-end digital customers and 21st century economy.* It cannot support levels of security, quality, reliability, and availability needed for economic prosperity.
- *The infrastructure has not kept up with new technology.* Many distribution systems have not been updated with current technology including IT.
- *Proliferation of distributed energy resources (DER).* DER includes a variety of energy sources—micro turbines, fuel cells, photovoltaics, and energy storage devices—with capacities from approximately 1 kW to 10 MW. DER can play an important role in strengthening energy infrastructure. Currently, DER accounts for about 7 % of total capacity in the United States, mostly in the form of backup generation, yet very little is connected to the power delivery system. By 2020, DER could account for as much as 25 % of total U.S. capacity, with most DER devices connected to the power delivery system.
- *Return on investment (ROI) uncertainties are discouraging investments in the infrastructure upgrades.* Investing new technology in the infrastructure can meet these aforementioned demands. More specifically, according to a June 2003 report by the National Science Foundation, R&D spending in the U.S. as a percent of net sales was about 10 % in the computer and electronic products industry and 12 % for the communication equipment industry in 1999. Conversely, R&D investment by electric utilities was less than 0.5 % during the same period. R&D investment in most other industries is also significantly greater than that in the electric power industry (NSF 2003).
- *Concern about the national infrastructure's security* [13]; EPRI (2001). A successful terrorist attempt to disrupt electricity supplies could have devastating effects on national security, the economy, and human life. Yet power

systems have widely dispersed assets that can never be absolutely defended against a determined attack.

Competition and deregulation have created multiple energy producers that share the same energy distribution network, one that now lacks the carrying capacity or safety margin to support anticipated demand. Investments in maintenance and research and development continue to decline in the North American electrical grid. Yet, investment in core systems and related IT components are required to insure the level of reliability and security that users of the system have come to expect.

In addition, the power industry is just beginning to adapt to a wider spectrum of risks. Both the number and frequency of weather-caused major outages have increased from 2 to 5 during 1950s–1980s and even early 1990s to a range of 70–130 per year during 2008–2012—now accounting for 66 % root cause of disruptions affecting 178 million customers (meters), and accounting for about 1333 outages, comprising 78 % of all outages, during 1992–2011. We are at the early stages of this adaption process to implement the strategies, systems, technologies and practices that will harden the grid and improve restoration performance after a physical disturbance.

## ***10.1 Smart Self-Healing Grid***

An interdependent, secure, integrated, reconfigurable, electronically controlled system that operates in parallel with an electric power grid. An electric power grid can be defined as the entire apparatus of wires and machines that connects power plants with customers. Adding and utilizing a “smart” element—sensors, communications, monitors, optimal controls and computers—to the electric grid can substantially improve its efficiency and reliability. In particular, secure digital technologies added to the grid and the architecture used to integrate these technologies into the infrastructure make it possible for the system to be electronically controlled and dynamically configured. This gives the grid unprecedented flexibility and functionality as well as a self-healing capability. It can react to and minimize the impact of unforeseen events, such as power outages, so that services are more robust and always available.

In addition, a stronger and smarter grid, combined with massive storage devices, can substantially increase the integration of wind and solar energy resources into the generation mix. It can support a wide-scale system for charging electric vehicles. Utilities can use its technologies to charge variable rates based on real-time fluctuations in supply and demand, and consumers can directly configure their services to minimize electricity costs.

## 10.2 Smart Grids and the Consumer: Empowered Consumers

Throughout the history of electric power systems, grid operators have largely worked in the paradigm that supply (i.e., generators) exists to follow all variability in consumers' demand. This has profound implications for how we design and operate the grid: the size of system peak relative to average power influences how much capacity needs to be built and the leveled costs of existing capacity, short time scale (sub-daily) variability determines how much flexible generation is required to follow ramps in demand and forecast errors.

Also throughout the history of power systems, though electricity prices that follow *fixed* time-of-use schedules have been common, the price of electricity most consumers pay has been independent of the evolution of system conditions on a day-to-day or hour-to-hour basis. For example, if consumers demand more electricity and requires more expensive generation to do so, the price consumers pay would nonetheless remain the same. Moreover system operators have had very few tools to reduce demand from customers *with their permission*; emergency load shedding programs and rolling blackouts are among the system operators' bluntest tools, and they only use them in the most extreme conditions.

However, a number of changes in technology and society are inspiring a move away from the world of "inflexible loads" and into a world where loads become enabled for real-time responsiveness to system conditions. As we will mention below, some of this responsiveness (motivated by dynamic prices or reliability signals) has existed in parts of the commercial and industrial sector for some time and there are many practical lessons to be learned from that history. However, though we do not yet fully understand what the benefits would be, it is possible that the scale of consumer engagement in power systems could be many orders of magnitude greater than it is today.

The Smart Grid extends all the way from the source of fuel for the electric power production to the many devices that use electricity, such as a household refrigerator, a piece of manufacturing equipment or a city park's lighting fixtures.

The Smart Grid is essential to support the related goals of price transparency, clean energy, grid reliability and electrified transportation. For example, Smart Grids allow for charging variable rates for energy based on supply and demand. This will reduce peak usage and increase system reliability by providing an incentive for consumers to shift their heavy uses of electricity (such as for heavy-duty appliances or processes that are less time-sensitive) to times of the day when demand is low (called peak shaving or load leveling).

These technologies provide consumers with the ability to obtain information, control and options of their own energy consumption. This involves advanced metering and demand response technologies. Two way communications and consumer-ready interfaces are essential for the success of this technology group. Conditional information of the grid and utility systems are additional benefits.



The data interfaces and communications are essential pieces to link to the other areas. These combinations of technologies enable customer empowerment.

### ***10.3 Smart Grids and the Supplier***

The U.S. federal government recognized this potential by implementing the Energy Independence and Security Act (EISA) of 2007. Title XIII of the Act mandates a Smart Grid that is focused on modernizing and improving the information and control infrastructure of the electric power system. Among the areas being addressed in the Smart Grid are: transmission, distribution, home-to-grid, industry-to-grid, building-to-grid, vehicle-to-grid, integration of renewable and distributed energy resources (such as wind and solar, which are intermittent), and demand response.

In particular, the secure digital technologies added to the grid and the architecture used to integrate these technologies into the infrastructure make it possible for the system to be electronically controlled and dynamically configured. This gives the end-to-end grid unprecedented flexibility and functionality and self-healing capability. It can react to and minimize the impact of unforeseen events, such as power outages, so that services are more robust and always available.

Operationally focused technologies are utilized not only on the utility-side of the smart grid, but also at the consumer and asset management side. Together these technologies allow for the realization of a number of different key deliverables for the execution of the smart grid. They allow for a Distribution Management System that can enable two-way power flow on the system. They form an Advanced Outage Management System that can integrate Consumer technologies and Advanced Distribution Operational technologies to detect and diagnose stressed areas in the system. There is also an increasing number of microgrid integration projects that allow the local grids to determine (in time of need) if they should remain interconnected or become islanded.

Microgrids are small power systems of several MW or less in scale with three primary characteristics: distributed generators with optional storage capacity, autonomous load centers, and the capability to operate interconnected with or islanded from a larger grid. Storage can be provided by batteries, supercapacitors, flywheels, or other sources. Microgrid assemblies are groups of interconnected microgrids that are in some sense “near” one another so that interconnection distances are small. As a result, line characteristics for such assemblies are similar to those of distribution systems.

Certainly, the power grid backbone also needs to become increasingly efficient and smart grids are designed to do this by efficiently integrating renewable resources that reduce society’s need for fossil-based resources, among other approaches. The upgraded backbone, combined with microgrids, will help us meet our goals for an efficient and eco-friendly electric power system.

The smart grid also has very important features that help the planet deal with energy and environmental challenges and reduce carbon emissions. Smart grids have the potential to substantially reduce energy consumption and CO<sub>2</sub> emissions. In fact CO<sub>2</sub> emissions alone could be reduced by 58 % in 2030, compared to 2005 emissions.

In summary a stronger and smarter grid, combined with massive storage devices, can substantially increase the integration of wind and solar energy resources into the generation mix. It can support a wide-scale system for charging electric vehicles. Utilities can use its technologies to charge variable rates based on real-time fluctuations in supply and demand, and consumers can directly configure their services to minimize electricity costs.

## 11 A New Energy Value Chain

In the past, power grids consisted of loosely connected networks of largely local systems. Today, however, they increasingly host the movement of wholesale power from one company to another (sometimes over the transmission lines of a third company) and from one region to another. Likewise, more and more distributed resources, primarily small generators, are connecting to the grid. The extent of interconnectedness, like the number of sources, controls, and loads, has grown with time.

As a result of these new technologies, players, regulatory environments that encourage competitive markets, a new energy value chain is emerging. In the past, much of the focus was on the supply side to enable competitive wholesale transactions. Changes in technology and the resulting economics have disrupted this traditional value chain and stimulated the adoption of distributed energy resources (DER). These distributed resources can assume many forms, but some key examples are distributed generation and storage, and plug-in hybrid electric vehicles (PHEVs).

In addition, because of competition and deregulation, an entire new area of energy services and transactions has been created around the demand side of the value chain. One of these new energy services is demand response (DR). DR enables load and other DER resources to provide capacity into the bulk power system in response to grid contingencies and market pricing signals. DR is an example of an energy service that requires the interaction and integration of multiple-party business systems and physical assets, resulting in both physical and financial transactions.

## 12 The Self-Healing Grid

A self-healing smart grid can be built to fulfill three primary objectives. The most fundamental is real-time monitoring and reaction [6]. An array of sensors would monitor electrical parameters such as voltage and current, as well as the condition of critical components. These measurements would enable the system to constantly tune itself to an optimal state.

The second goal is anticipation. The automated system constantly looks for potential problems that could trigger larger disturbances, such as a transformer that is overheating. Computers would assess trouble signs and possible consequences. They would then identify corrective actions, simulate the effectiveness of each action, and present the most useful responses to human operators, who could then quickly implement corrective action by dispatching the grid's many automated control features. This is a fast look-ahead capability to anticipate problems, to adapt to new conditions after an outage, or an attack, the way a fighter plane reconfigures its systems to stay aloft even after being damaged. This advanced feature enables resilience in times of crisis in three ways: by providing faster-than-real-time, look-ahead simulations (analogous to master chess players rapidly expanding and evaluating their various options under time constraints) and thus avoiding previously unforeseen disturbances; by performing what-if analysis for large-region power systems from both operations and planning points of view; and by integrating market, policy and risk analysis into system models, and quantifying their integrated effects on system security and reliability.

The third objective is rapid isolation. If failures were to occur, the whole network would break into isolated "islands," each of which must fend for itself. Each island would reorganize its power plants and transmission flows as best it could. Although this might cause voltage fluctuations or even small outages, it would prevent the cascades that cause major blackouts. As line crews repaired the failures, human controllers would prepare each island to smoothly rejoin the larger grid. The controllers and their computers would function as a distributed network, communicating via microwaves, optical fibers or the power lines themselves. As soon as power flows were restored, the system would again start to self-optimize.

## 13 Smart Grids and Security

The existing end-to-end energy and power-delivery system is vulnerable to natural disasters and intentional cyber-attacks. Virtually every crucial economic and social function depends on the secure, reliable operation of power and energy infrastructures. Energy, electric power, telecommunications, transportation, and financial infrastructures are becoming interconnected, thus posing new challenges for their secure, reliable, and efficient operation. All of these interdependent infrastructures are complex networks, geographically dispersed, non-linear, and

interacting both among themselves and with their human owners, operators, and users.

Challenges to the security of the electric infrastructure include:

**Physical security**—The size and complexity of the North American electric power grid makes it impossible both financially and logistically to physically protect the entire end-to-end and interdependent infrastructure. There currently exist over 450,000 miles of 100 kV or higher transmission lines, and many more thousands of miles of lower-voltage lines. As an increasing amount of electricity is generated from distributed renewable sources, the problem will only be exacerbated.

**Cyber security**—Threats from cyberspace to our electrical grid are rapidly increasing and evolving. While there have been no publicly known major power disruptions due to cyber-attacks, public disclosures of vulnerabilities are making these systems more attractive as targets.

**Security**,<sup>7</sup> which includes privacy and cybersecurity, is fundamentally necessary for reliable grid operations and for customer acceptance of smart grids, and many in IEEE and the smart grid community are developing technologies and standards addressing this issue. What is most important, however, is that security is incorporated into the architectures and designs at the outset, not as an afterthought. For the microgrids it is necessary to employ security technologies for each equipment component that is used and for each customer application that is developed. If any part of the system is compromised, the system reconfigures to protect itself, localize and fend off the attacks.

Due to the increasingly sophisticated nature and speed of some malicious code, intrusions, and denial-of-service attacks, human response may be inadequate. Furthermore, currently more than 90 % of successful intrusions and cyber-attacks take advantage of known vulnerabilities and misconfigured operating systems, servers, and network devices. Technological advances targeting system awareness, cryptography, trust management and access controls are underway and continued attention is needed on these key technological solutions.

---

<sup>7</sup> Regarding interoperability and emerging security standards, the IEEE-SA has published an architectural framework for the smart grid, called IEEE 2030, which defines the interconnection and interoperability standards for the power, IT and communications technologies that will be used in smart grids. IEEE-SA is working actively on standardization with the NIST Smart Grid Interoperability Panel, which includes IEEE-SA standards in its catalog of smart grid standards. IEEE-SA also collaborates with many standards organizations that represent specific industries, countries or regions to help make sure that products that operate on smart grids are complementary and compatible with one another.

## 14 Smart Grid: Costs and Benefits

What are the costs/benefits and range of new consumer-centered services enabled by smart grids? What is the smart grid's potential to drive economic growth? To begin addressing these, the costs of full implementation for a nationwide Smart Grid range over a 20-year period (2010–2030):

- According to energy consulting firm Brattle Group, the necessary investment to achieve an overhaul of the entire electricity infrastructure and a smart grid is \$1.5 trillion spread over 20 years (~\$75 billion/year), including new generators and power delivery systems.
- A detailed study by the Electric Power Research Institute (EPRI) published in April 2011, finds that the estimated *net* investment needed to realize the envisioned power delivery system of the future is between \$338 and \$476 billion. The new estimates translate into annual investment levels of between \$17 and \$24 billion over the next 20 years.

The costs cover a wide variety of enhancements to bring the power delivery system to the performance levels required for a smart grid. They include the infrastructure to integrate distributed energy resources and achieve full customer connectivity but exclude the cost of generation, the cost of transmission expansion to add renewables and to meet load growth and a category of customer costs for smart-grid-ready appliances and devices. Despite the costs of implementation, investing in the grid would pay for itself, to a great extent. Integration of the Smart Grid will result in:

- (1) Costs of outages reduced by about \$49B per year,
- (2) Increased efficiency and reduced emissions by 12–18 % per year (PNNL report, January 2010),
- (3) A greater than 4 % reduction in energy use by 2030; translating into \$20.4 billion in savings,
- (4) More efficient to move electrical power through the transmission system than to ship fuels the same distance. From an overall system's perspective, with goals of increased efficiency, sustainability, reliability, security and resilience, we need both:
  - Local microgrids (that can be as self-sufficient as possible and island rapidly during emergencies), and
  - Interconnected, smarter and stronger power grid backbone that can efficiently integrate intermittent sources, and to provide power for end-to-end electrification of transportation.
- (5) Reduction in the cost of infrastructure expansion and overhaul in response to annual peaks. The demand response and smart grid applications could reduce these costs significantly.

- (6) The benefit-to-cost ratios are found to range from 2.8 to 6.0. Thus, the smart grid definition used as the basis for the study could have been even wider, and yet benefits of building a smart grid still would exceed costs by a healthy margin. By enhancing efficiency, for example, the smart grid could reduce 2030 overall CO<sub>2</sub> emissions from the electric sector by 58 %, relative to 2005 emissions.
- (7) Increased cyber/IT security, and overall energy security, if security is built in the design as part of layered defense system architecture.

On options and pathways forward, I am often asked “*should we have a high-voltage power grid or go for a totally distributed generation, for example with microgrids?*” We need both, as the “choice” in the question poses a false dichotomy. It is not a matter of “this OR that” but it is an “AND”. To elaborate briefly, from an overall energy system’s perspective (with goals of efficiency, eco-friendly, reliability, security and resilience) we need both (1) microgrids (that can be as efficient and self-sufficient as possible, and to island rapidly during emergencies), AND we need (2) a stronger and smarter power grid as a backbone to efficiently integrate intermittent renewable sources into the overall system.

The global investments so far in advanced metering infrastructure and the coming wave of investment in distribution automation are but the beginning of a multi-decade, multi-billion-dollar effort to achieve an end-to-end, intelligent, secure, resilient, and self-healing system. It is noteworthy that the cost-effective investments to harden the grid and support resilience will vary by region, by utility, by the legacy equipment involved and even by the function and location of equipment within a utility’s service territory.

## **15 Options and Possible Futures: What Will It Take to Succeed?**

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.

As a result of demand growth, regulatory uncertainty, and the increasing connectedness of critical infrastructures, it is quite possible that in the near future the ability, for example, of the electricity grid to deliver the power that customers require in real-time, on demand, within acceptable voltage and frequency limits, and in a reliable and economic manner may become severely tried. Other infrastructures similarly may be tested.

At the same time, deregulation and restructuring have added concern about the future of the electric power infrastructure (and other industries as well). This shift marked a fundamental change from an industry that was historically operated in a

very conservative and largely centralized way as a regulated monopoly, to an industry operated in a decentralized way by economic incentives and market forces. The shift impacts every aspect of electrical power including its price, availability, and quality. For example, as a result of deregulation, the number of interacting entities on the electric grid (and hence its complexity) has been dramatically increasing while, at the same time, a trend towards reduced capacity margins has appeared. Yet, when deregulation was initiated, little was known about its large-scale, long-term impacts on the electricity infrastructure, and no mathematical tools were available to explore possible changes and their ramifications.

It was in this environment of concern that the smart self-healing grid was conceived. One event in particular precipitated the creation of its foundations: a power outage that cascaded across the western United States and Canada on August 10, 1996. This outage began with two relatively minor transmission-line faults in Oregon. But ripple effects from these faults tripped generators at McNary dam, producing a 500 MW-wave of oscillations on the transmission grid that caused separation of the primary West Coast transmission circuit, the Pacific Intertie, at the California-Oregon border. The result: blackouts in 13 states and provinces costing some \$1.5 billion in damages and lost productivity. Subsequent analysis suggests that shedding (dropping) some 0.4 % of the total load on the grid for just 30 min would have prevented the cascading effects and prevented large-scale regional outages (note that load shedding is not typically a first option for power grid operators faced with problems).

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).

Had the results of the CIN/SI been in place at the time of the August 1996 blackout, the events might have unfolded very differently. For example, fault anticipators located at one end of the high voltage transmission lines would have detected abnormal signals, and making adaptive reconfiguration of the system to sectionalize the disturbance and minimize the impact of components failures several hours before the line failed. The look-ahead simulations would have identified the line as having a higher than normal probability of failure. Quickly, cognitive agents (implemented as distributed software and hardware in the infrastructure components and in control centers) would have run failure scenarios on their virtual system models to determine the ideal corrective response. When the high-voltage line actually failed, the sensor network would have detected the voltage fluctuation and communicate the information to reactive agents located at

substations. The reactive agents would have executed the pre-determined corrective actions, isolating the high-voltage line and re-routed power to other parts of the grid. No customer in the wider area would even be aware that a catastrophic event had impended, or had seen a few flickers in the light.

Such an approach provides an expanded stability region with larger operational range; as the operating point nears the limit to how much the grid could have adapted (e.g., by automatically rerouting power and/or balancing dropping a small amount of load or generation), rather than cascading failures and large-scale regional system blackouts, the system will be reconfigured to minimize severity/size of outages, to shorten duration of brownouts/blackouts, and to enable rapid/efficient restoration.

This kind of distributed grid control has many advantages if coordination, communication, bandwidth, and security can be assured. This is especially true when the major components are geographically dispersed, as in a large telecommunications, transportation, or computer network. It is almost always preferable to delegate to the local level, as much of the control as is practical.

The simplest kind of distributed control would combine remote sensors and actuators to form regulators (e.g., intelligent electronically controlled secure devices), and adjust their set points or biases with signals from a central location. Such an approach requires a different way of modeling—of thinking about, organizing and designing—the control of a complex, distributed system. Recent research results from a variety of fields, including nonlinear dynamical systems, artificial intelligence, game theory, and software engineering have led to a general theory of complex adaptive systems (CAS). Mathematical and computational techniques originally developed and enhanced for the scientific study of CAS provide new tools for the engineering design of distributed control so that both centralized decision-making and the communication burden it creates can be minimized. The basic approach to analyzing a CAS is to model its components as independent adaptive software and hardware “agents”—partly cooperating and partly competing with each other in their local operations while pursuing global goals set by a minimal supervisory function.

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 the 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 are already 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. 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 has a dedicated wire connecting it to a dedicated generator. A lightning strike on any wire would take out that one circuit and no more. But like trees in nature, electrical systems are designed for efficient use of resources, which means numerous sockets served by a single circuit and multiple circuits for each generator. A failure anywhere on the system causes additional failures until a barrier—a surge protector or circuit breaker, say—is reached. If the barrier does not function properly or is insufficiently large, the failure bypasses it and continues cascading across the system [16].

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. CIN/SI developed, among other things, a new vision for the integrated sensing, communications, and control of the power grid. Some of the pertinent issues are why/how to develop controllers for centralized versus decentralized control and issues involving adaptive operation and robustness to disturbances that include various types of failures.

Modern computer and communications technologies now allow us to think beyond the protection systems and the central control systems to a fully distributed system that places intelligent devices at each component, substation and power plant. This distributed system will enable us to build a truly smart grid.

One of the problems common to the management of central control facilities is the fact that any equipment changes to a substation or power plant must be described and entered manually into the central computer system’s database and electrical one-line diagrams. Often this work is performed some time after the equipment is installed and there is thus a permanent set of incorrect data and diagrams in use by the operators. What is needed is the ability to have this information entered automatically when the component is connected to the substation—much as a computer operating system automatically updates itself when a new disk drive or other device is connected.

## 16 Potential Road Ahead

Electric power systems constitute the fundamental infrastructure of modern society. Often continental in scale, electric power grids and distribution networks reach virtually every home, office, factory, and institution in developed countries and have made remarkable, if remarkably insufficient, penetration in developing countries such as China and India.

Global trends toward interconnectedness, privatization, deregulation, economic development, accessibility of information, and the continued technical trend of rapidly advancing information and telecommunication technologies all suggest that the complexity, interactivity, and interdependence of infrastructure networks will continue to grow.

The existing electricity infrastructure evolved to its technology composition today from the convolution of several major forces, only one of which was technologically based. During the past 15 years, we have systematically scanned science and technology, investment and policy dimensions to gain clearer insight on current science and technology assets when looked at from a consumer-centered future perspective, rather than just incremental contributions to today's electric energy system and services.

The goal of transforming the current infrastructures to self-healing energy delivery, markets, computer and communications networks with unprecedented robustness, reliability, efficiency and quality for customers and our society is ambitious. This will require addressing challenges and developing tools, techniques, and integrated probabilistic risk assessment/impact analysis for wide-area sensing and control for digital-quality infrastructure—sensors, communication and data management, as well as improved state estimation, monitoring and simulation linked to intelligent and robust controllers leading to improved protection and discrete-event control. These follow-on activities will build on the foundations of CIN/SI and current programs that include self-healing systems and real-time dynamic information and emergency management and control.

More specifically, the operation of a modern power system depends on a complex system of sensors and automated and manual controls, all of which are tied together through communication systems. While the direct physical destruction of generators, substations, or power lines, may be the most obvious strategy for causing blackouts, activities that compromise the operation of sensors, communication and control systems by spoofing, jamming, or sending improper commands could also disrupt the system, cause blackouts, and in some cases result in physical damage to key system components. Hacking and cyber attacks are becoming increasingly common.

Most early communication and control systems used in the operation of the power system were carefully isolated from the outside world, and were separated from other systems, such as corporate enterprise computing. However, economic pressures created incentives for utilities to make greater use of commercially available communications and other equipment that was not originally designed

with security in mind. Unfortunately, from a security perspective, such interconnections with office and electronic business systems through other layers of communications created vulnerabilities. While this problem is now well understood in the industry and corrective action is being taken, we are still in a transition period during which some control systems have been inadvertently exposed to access from the Internet, intranets, and remote dial-up capabilities that are vulnerable to cyber intrusions.

Many elements of the distributed control systems now in use in power systems are also used in a variety of applications in process control, manufacturing, chemical process control and refineries, transportation, and other critical infrastructure sectors and hence vulnerable to similar modes of attack. Dozens of communication and cyber security intrusions, and penetration red-team attacks have been conducted by DOE, EPRI, electric utilities, commercial security consultants, KEMA, and others. These “attacks” have uncovered a variety of cyber vulnerabilities including unauthorized access, penetration and hijacking of control.

While some of the operations of the system are automatic, ultimately human operators in the system control center make decisions and take actions to control the operation of the system. In addition, to the physical threats to such centers and the communication links that flow in and out of them, one must also be concerned about two other factors: the reliability of the operators within the center, and the possibility that insecure code has been added to one of the programs in a center computer. The threats posed by “insider” threats, as well as the risk of a “Trojan horse” embedded in the software of one or more of the control centers is real, and can only be addressed by careful security measures both within the commercial firms that develop and supply this software, and care security screening of the utility and outside service personnel who perform software maintenance within the center. Today security patches are often not always supplied to end-users, or users are not applying the patches for fear of impacting system performance. Current practice is to apply the upgrades/patches after SCADA vendors thoroughly test and validate patches, sometimes incurring a delay in patch deployment of several months.

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.

As a part of enabling a smart self-healing grid, we have developed fast look-ahead modeling and simulation, precursor detection, adaptive protection and coordination methods that minimize the 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; a 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, and 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.

Over the last 15 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.

Advanced technology now under development or under consideration holds the promise of meeting the electricity needs of a robust digital economy. The architecture for this new technology framework is evolving through early research on concepts and the necessary enabling platforms. This architectural framework envisions an integrated, self-healing, electronically controlled electricity supply system of extreme resiliency and responsiveness—one that is fully capable of responding in real time to the billions of decisions made by consumers and their increasingly sophisticated agents. The potential exists to create an electricity system that provides the same efficiency, precision and interconnectivity as the billions of microprocessors that it will power.

## 17 Next Steps

A new mega-infrastructure is emerging from the convergence of energy (including the electric grid, water, oil and gas pipelines), telecommunications, transportation, Internet and electronic commerce. Furthermore, in the electric power industry and other critical infrastructures, new ways are being sought to improve network

efficiency and eliminate congestion problems without seriously diminishing reliability and security.

A balanced, cost-effective approach to investments and use of technology can make a sizable difference in mitigating the risk. As expressed in the July 2001 issue of *Wired* magazine: “The best minds in electricity R&D have a plan: Every node in the power network of the future will be awake, responsive, adaptive, price-smart, eco-sensitive, real-time, flexible, humming—and interconnected with everything else”. The technologies include, for example, the concept of self-healing electricity infrastructure, 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 attacks.

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.

The increased deployment of feedback and communication implies that loops are being closed where they have never been closed before, across multiple temporal and spatial scales, thereby creating a gold mine of opportunities for control. Control systems are needed to facilitate decision-making under myriad uncertainties, across broad temporal, geographical, and industry scales—from devices to power-system-wide, from fuel sources to consumers, and from utility pricing to demand-response. The various challenges introduced can be posed as a system-of-systems problem, necessitating new control themes, architectures, and algorithms. These architectures and algorithms need to be designed so that they embrace the resident complexity in the grid: large-scale, distributed, hierarchical, stochastic, and uncertain. With information and communication technologies and advanced power electronics providing the infrastructure, these architectures and algorithms will need to provide the smarts, and leverage all advances in communications and computation such as 4G networks, cloud computing, and multi-core processors.

Given economic, societal, and quality-of-life issues and the ever-increasing interdependencies among infrastructures, a key challenge before us is whether the electricity and our interdependent infrastructures will evolve to become the primary support for the 21st century’s digital society—smart secure infrastructures with self-healing capabilities—or be left behind as a 20th century industrial relic.

## References

1. Amin, S.M.: North America's electricity infrastructure: are we ready for more perfect storms? *IEEE Secur. Priv. Mag.* **1**(5), 19–25 (2003)
2. Amin, S.M.: Toward self-healing energy infrastructure systems cover feature. *IEEE Comput. Appl. Power* **14**(1), 20–28 (2001)
3. U.S. Department of Homeland Security. National Infrastructure Protection Plan. [http://www.dhs.gov/xlibrary/assets/NIPP\\_Plan.pdf](http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf). Accessed Dec 2012
4. "Sustainable Critical Infrastructure Systems—a Framework for Meeting 21st Century Imperatives," Board on Infrastructure and the Constructed Environment (BICE), Division on Engineering and Physical Sciences, National Research Council of the National Academies, The National Academies Press, Washington, DC (2009)
5. EPRI 2003: Complex Interactive Networks/Systems Initiative: Final Summary Report—Overview and Summary Final Report for Joint EPRI and US DoD University Research Initiative, pp. 155. EPRI, Palo Alto, Dec 2003
6. Amin, S.M., Schewe, P.F.: Preventing Blackouts," *Sci. Am.* **296**(5), 60–67 (2007)
7. Firestone, "Power Failure Reveals a Creaky System, Energy Experts Believe," *The New York Times*. <http://www.nytimes.com/2003/08/15/nyregion/15GRID.html>. Accessed Nov 2012
8. American Society of Civil Engineers, "2009 Report Card for America's Infrastructure," [http://www.infrastructurereportcard.org/sites/default/files/RC2009\\_full\\_report.pdf](http://www.infrastructurereportcard.org/sites/default/files/RC2009_full_report.pdf). Accessed June 2009
9. "Decision Technology for Rational Selection of Infrastructure Investments: Final Report of ASME Foundation Strategic Proposal Grant Fund," ASME Innovative Technologies Institute, LLC, Washington, DC, July 16, 2009
10. Center for Strategic and International Studies Commission on Public Infrastructure, Guiding Principles for Strengthening America's Infrastructure, 2006
11. Amin, S.M.: National infrastructures as complex interactive networks. In: Samad, T., Weyrauch, J. (eds.) *Automation, Control, and Complexity: An Integrated Approach*, Chap. 14, pp. 263–286. John Wiley and Sons Ltd., New York (2000)
12. Amin, S.M., Stringer, J.: The electric power grid: today and tomorrow. *MRS Bull.* **33**(4), 399–407 (2008)
13. Amin, S.M.: Powering the 21st century: we can—and must—modernize the grid. *IEEE Power Energ. Mag.* **3**(2), 93–96 (2005)
14. Amin, S.M.: U.S. grid gets less reliable. *IEEE Spectr.* **48**(1), p. 80 (2011)
15. Amin, S.M., Wollenberg, B.F.: Toward a smart grid: power delivery for the 21st century. *IEEE Power Energ. Mag.* **3**(5), 34–41 (2005)
16. Amin, S.M.: For the good of the grid: toward Increased efficiencies and integration of renewable resources for future electric power networks. *IEEE Power Energ. Mag.* **6**(6), 48–59 (2008)