European Journal of Control (2011)5-6:547–567
© 2011 EUCA
DOI:10.3166/EJC.17.547–567

European
Journal of
Control

Smart Grid: Overview, Issues and Opportunities. Advances and Challenges in Sensing, Modeling, Simulation, Optimization and Control

S. Massoud Amin

Technological Leadership Institute, Honeywell/H.W. Sweatt Chair in Technological Leadership, Electrical and Computer Engineering, University of Minnesota, Minneapolis, USA

The genesis of early power systems and electric power grids during the past 130 years was enabled by automation and control of electromechanical machinery and power delivery networks. Today's end-to-end power and energy systems (from fuel source to end use) fundamentally depend on embedded and often an overlaid systems of sensors, computation, communication, control and optimization. There are even more opportunities and challenges in today's devices and systems, as well as in the emerging modern power systems – ranging from dollars, watts, emissions, standards, and more – at nearly every scale of sensing and control. Recent policies combined with potential for technological innovations and business opportunities, have attracted a high level of interest in smart grids. The potential for a highly distributed system with a high penetration of intermittent sources poses opportunities and challenges. Any complex dynamic infrastructure network typically has many layers, decision-making units and is vulnerable to various types of disturbances. Effective, intelligent, distributed control is required that would enable parts of the networks to remain operational and even automatically reconfigure in the event of local failures or threats of failure.

This presentation provides an overview of smart grids and recent advances in distributed sensing, modeling, and control, particularly at both the high-voltage power grid and at consumer level. Such advances may contribute toward the development of an effective, intelligent, distributed control of power system networks with a focus on addressing distributed sensing, computation, estimation, controls and dynamical systems challenges and opportunities ahead.

Keywords: Smart grids, self-healing energy infrastructures, uncertain dynamical systems.

1. Focus

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, albeit remarkably insufficient, penetration in developing countries such as China and India.

Once "loosely" interconnected networks of largely local systems, electric power grids increasingly host large-scale, long-distance wheeling of power (the movement of wholesale power from one company to another, sometimes over the transmission lines of a third party company) from one region to another [1–7, 17, 34]. 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

*Correspondence to: S. Massoud Amin, E-mail: amin@umn.edu.

Received 15 August 2011; Accepted 15 September 2011
Recommended by Eduardo F. Camacho

power grids are among the most complex networks ever made.

The term "smart grid" refers to the use of computer, communication, sensing, and control technology which operates in parallel with an electric power grid for the purpose of enhancing the reliability of electric power delivery, minimizing the cost of electric energy to consumers, and facilitating the interconnection of new generating sources to the grid [4–7].

Control systems are needed across broad temporal, geographical, and industry scales—from devices to power-system-wide, from fuel sources to consumers, from utility pricing to demand response, and so on. With increased deployment of feedback and communication, opportunities arise for reducing consumption, for better exploiting renewable sources, and for increasing the reliability and performance of the transmission and distribution networks. At the same time, however, closing loops where they have never been closed before, across multiple temporal and spatial scales, create control challenges as well. The control systems community has a very rich history of making pioneering contributions both the to theory as well as developing important applications in this area, they range from sensing to computation and visualization, estimation, optimization and controls – from devices and machinery to high-voltage grids to local distribution systems [2–33, 40–50].

How to manage or 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. This paper provides an overview of smart grids and the pivotal role that the control systems community can play with the goal of increased agility, security and resilience for smart grids and large-scale layered systems.

Societal and governmental visions for the smart grid will require the engagement of the controls community for their realization. Feedback, optimization, estimation, dynamics, stability... these and other control system concepts are core to smart grid technology. In many ways, the smart grid is a control problem!

2. Synopsis

Recent policies in the U.S., China, India, EU, UK and other nations throughout the World, combined with potential for technological innovations and business opportunities, have attracted a high level of interest in smart grids. Nations, regions and cities that best implement new strategies and infrastructure may reshuffle the world pecking order. Emerging markets could leapfrog other nations:

- **U.S.** investment is at about $7 billion in smart grid technologies
- **China** invested $7.3 billion; will spend $96 billion in smart grid technology by 2020
  - China's energy needs to double by 2020
  - Many changes will happen in the homes themselves
  - China will account for 18.2% of global smart grid appliance spending by 2015.
- **South Korea** at nearly $1 billion:
  - A $65 million pilot program on Jeju Island is implementing a fully integrated grid for 6,000 homes, a series of wind farms and four distribution lines. Its leaders plan to implement smart grids nationwide by 2030.
- **Brazil**: 60% growth in electricity consumption between 2007 and 2017 with 16-34% increase in renewables from hydro, biomass and wind. But they have an aging grid that is currently a one-way power flow that needs to move in two directions.

In 2007, the United States Congress passed the Energy Independence and Security Act outlining specific goals for the development of the nation's smart grid. Section 1301 states that, "It is the policy of the United States to support the modernization of the Nation's electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure that can meet future demand growth and to achieve each of the following, which together characterize a smart grid:

1. Increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid.
2. Dynamic optimization of grid operations and resources, with full cyber-security…".

Smart Grid is a concept and a range of functionalities: It is designed to be inherently flexible, accommodating a variety of energy production sources and adapting to and incorporating new technologies as they are developed. It allows for charging variable rates for energy, based upon supply and demand at the time. In theory, this will incentivize 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. As an example of these range of functionalities, in 2008, U.S. Department of Energy (DOE) defined functions of a smart grid as:

- "Self-healing" from power disturbance events
- Enabling active participation by consumers in de response
- Operating resiliently against physical and cyber attacks
- Providing power quality for 21st century needs

- Accommodating all generation and storage options
- Enabling new products, services, and markets
- Optimizing assets and operating efficiently.

The ultimate goal of is for the end-to-end electric power system (from fuel source, to generation, transmission, distribution, and end use) of the future will:

- Allow secure and real-time 2-way power and information flows
- Enable integration of intermittent renewable energy sources and help decarbonize power system
- Enable effective demand management, customer choice, secure and efficient operation of the grid
- Enable the secure collection and communication of detailed data regarding energy usage to help reduce demand and increase efficiency.

3. Data Tsunami Developing: Opportunities for the CSS

During the last 14 years, we have increasingly focused on incorporating sensors, electronic communications, and computational ability across all generation, transmission and distribution assets to enhance the value of electricity to society [20–22]. Information Technology (IT) serves as a lynchpin in this system and keeps the network together. However, we are concerned that the evolution in advanced IT, communications and control systems may not be brisk enough to meet the needs of our customers. Fig. 1 depicts the increased services expected in the near future due to tremendous amounts of data being generated. This "tsunami" of incoming data will change how utilities operate and maintain the grid. Naturally, among the issues to be explored is whether all these data need to be centralized and how it may be reduced to information and managed or where it is stored.

Fig. 1 illustrates the data that could be generated by a typical utility that decides to overlay a communications infrastructure on its power delivery system and begin to enhance the functionality of its system in stages from distribution automation through to full connectivity with customers.

To put Fig. 1 in perspective, the US Library of Congress contains 20 terabytes (TB) of data; the British National Archive, which represents 1,000 years of British history, contains 600 TB; Google's search engine crawler processes about 850 TB of information (that is the amount of raw data from the web). One TB equals 1,024 gigabytes (GB).

This increase in volumes of data has led to investment and technology development, at least in the short term, in the following areas:

- Analytics: Mining data to increase understanding and for business potential;
- Standards consolidation to enable interoperability and enhance security;
- Increasing penetration of solar and electric vehicles: Demand shifts, integrate new tools and technologies.

There are many remaining challenges relating to the development and wide-spread deployment of smart grids:

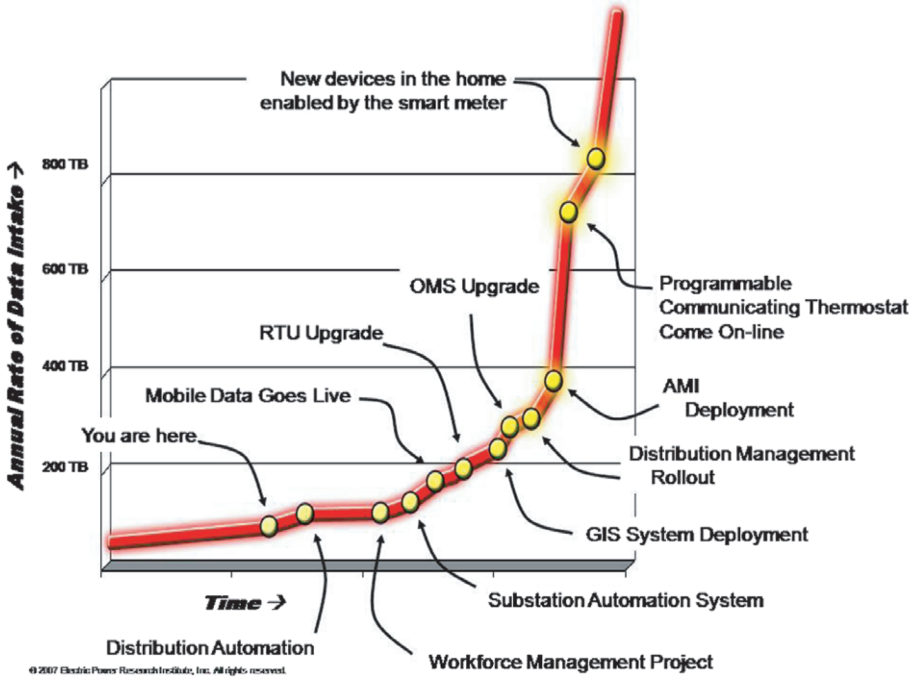
- The electric power industry, computer, communication, and electronics industries have begun to develop standards for communication, computer message structure, sensing and control device interfaces, however, much remains to be done before the smart grid can be built.
- A major source of complexity is the interdependence of the multi-scaled sensing and telecommunication networks and the power grid. Issues range from the highest command and control level to the individual power stations and substations at the middle level, and then to the devices and power equipment at the lowest level.
- The potential for a highly distributed system with a high penetration of renewable sources that exhibit variable generation and non-dispatchability poses opportunities and challenges for the control community and the broader society.

We focus on the sensing, communications, and control aspects of the challenges posed by this rapid growth: improving existing technology through engineering and inventing new technologies requiring new methods and materials. Some methods or materials advances will improve present technology (e.g., faster dynamic risk assessment and control, stronger, higher current overhead lines), some will enable emerging technology (e.g., superconducting cables, fault current limiters, and transformers), and some will anticipate technologies that are still conceptual (e.g., storage for extensive solar or wind energy generation).

4. Overview/Summary of this presentation:

The electric power network, combined with overlaid networks of sensing, communication and control constitutes a complex dynamical network, geographically dispersed, non-linear, and interacting both among its components and with its 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



© 2007 Electric Power Research Institute, Inc. All rights reserved.

Fig. 1. A tsunami of incoming data (Note: AMI in the diagram refers to advanced metering infrastructure).

paradigms are unable to handle the complexity and interconnectedness of these critical infrastructures. The targets pertinent to the CSS to consider and address include:

- **Systems Science:** How to retrofit and engineer a stable, secure, robust and resilient grid with large numbers of such unpredictable power sources?
- **Modeling, Simulation, Control, and Optimization of Hybrid Systems with Uncertainty:** What roles will assets optimization, novel control algorithms, increased efficiency, control/coordination of energy storage, advanced power electronics, power quality, electrification of transportation, cyber security, policies, and technologies play in the smart grid of the future?
- **How can robust controls and observers be developed that can use secure sensing to identify and build realistic models and appropriate responses?** Will they be able to adapt, control, and mitigate disturbances to achieve their goals?
- **Intelligent Transmission Systems/Assets include self-monitoring and self-healing and the abilities to control real-time information for smart transmission utilization.** Smart, cyber-physical secured control strategies need to be developed to handle congestions, precursors to instability or reliability problems. Information exchange among renewable resources, and locational demands from plug-in hybrids/fuel cell transport systems need to be incorporated.
- **Real time monitoring sensors, communication and control technologies will constitute a lynchpin overlaid infrastructure of smart power systems.** However, increased use of electronic automation raises significant issues regarding the adequacy of operational security of the automation and control systems. In addition, the use of networked electronic systems for sending, metering, scheduling, trading, or e-commerce imposes numerous financial risks implied by use of this technology. A timely issue is merging of sensor-enabled data-based models with derived models from first principles combined with online updating.

There are several technical areas that the controls community can contribute to and that the IEEE CSS TC-SG can address, for example:

- Optimization of demand response under variable pricing
- Integration of distributed generation and storage in automation and control strategies
- Integration of plug-in electric and hybrid-electric vehicles
- Distributed state estimation of power systems, and elements thereof, with limited sensing and communication
- Cybersecurity in smart-grid control systems
- New power market designs that exploit feedback and information integration
- Stability issues, especially given latency and uncertainty in communication networks

- Self-monitoring and self-healing in intelligent transmission systems
- Modeling and analysis of multi-scale, complex grids
- The broader systems question: how can we engineer (and retrofit) a stable, secure, robust and resilient grid with large numbers of unpredictable power sources and variable demand.

After consultation with colleagues and volunteers involved in the IEEE Smart Grid, the IEEE CSS TC-SG and the Smart Grid Vision/Roadmap projects for CSS, CS and PES societies, the preliminary areas are as follows:

- *Demand-side optimization and control.* 90+% of the electricity generated in developed nations is consumed in residential, commercial, and industrial premises. Energy efficiency and peak load reduction are required to reduce overall electricity consumption, to minimize use of expensive peaking plants, and to fully exploit renewable sources. Automation and control systems in homes, buildings, and industrial plants will be needed to minimize consumption and cost.
- *Intelligent transmission and distribution.* New sensors and power-flow-management devices can, in principle, promise the fulfillment of the long-standing promise of self-healing grids. Key research needs include estimation, observers, and modeling under partial and uncertain information.
- *Policies and pricing mechanisms for real-time power markets.* Smart grids will result in new business and market structures. Issues related to information sharing, real-time or near-real-time dynamic pricing, fairness of access, and others must be resolved. Modeling, control, optimization, will be crucial.
- *Automation aspects of integrating distributed generation and storage.* Future power systems are likely to have substantially larger contribution from renewable sources such as wind and solar, which are characterized by intermittency of operation and a lack of ability to dispatch. Integrating such sources in an automation and control system is therefore challenging, since balance between instantaneous supply and demand must always be maintained. Storage technologies—and their control—will be crucial in this respect. Plug-in electric (including hybrid) vehicles must also be considered.

In summary, the strategic R&D challenges, innovations in electric power and energy include building a stronger and smarter end-to-end electrical energy infrastructure and the pertinent systems and controls R&D – focusing on the potential R&D focus areas for the CSS community's increased impacts from an end-to-end systems perspective, which includes many promising subareas in the whole spectrum noted below:

Sensing/Measurement → Analysis/Visualization → Automation/Self-healing Systems

4.1. Enabling Technologies

- **Monitoring and Analysis:** Seeing and understanding what is going on in complex dynamic systems and risk assessment
- **Automation/Control:** Active-control of high-voltage devices…Ensuring system stability, reliability, robustness, security and efficiency in a competitive marketplace and carbon-constrained world
- **Integration and adaptive control of Distributed Energy Resources (DER)** such as renewables, "microgrids," storage, solid oxide and other fuel cells, photovoltaics, superconducting magnetic energy storage (SMES), transportable battery energy storage systems (TBESS), etc. with integration and management of resources, and developing new business strategies for a deregulated energy markets

4.2. Research Challenges

Sensing/Measurement → Analysis/Visualization → Automation/Self-healing Systems

- Sensing, Communication and Data Management
  - Intelligent sensors as elements in real-time data base; seek appropriate high level query tools for such a database? sensor interface to multiresolutional models? Metrics?
  - Effect of market structures, distributed generation, other new features on above issues; economic evaluations
  - Increased dependence on information systems and software
  - Dependability/robustness is the key…V&V remains a big challenge
  - Flexible and robust communication architectures (wireless to optical backbone? powerline schemes?), protocols
  - Dealing with latency, variable time delay
  - Data management, calibration & validation (bad or missing or malicious data), sharing and distribution, archiving, hierarchical aggregation
  - Dynamic, distributed databases
  - Appropriate computer network architectures
- Mathematical/Theoretical foundation is fragmented: Computational complexity, information theory, dynamical systems and control science… need for a new science of interdependent complex networks and infrastructure security.

4.3. Enabling a Stronger and Smarter Grid

Complex Dynamical Systems: Systems Science, Controls and Applied Mathematics

- **Modeling:** Idealized models, consisting of static graph-theoretic models, and interactive dynamic models, such as interconnected differential-algebraic systems; Hybrid Models.
- **Robust Control:** Design of self-healing systems requires the extension of the theory of robust control in several ways beyond its present focus on the relatively narrow problem of feedback control.
- **Complex Systems:** Theoretical underpinnings of complex interactive systems.
- **Dynamic Interaction in Interdependent Layered Networks:** Characterization of uncertainty in large distributed networks: Multi-resolutional techniques where various levels of aggregation can co-exist.
- **Disturbance Propagation in Networks:** Prediction and detection of the onset of failures both in local and global network levels.
- **Forecasting, Handling Uncertainty and Risk:** Characterizing uncertainties and managing risk; Hierarchical and multi-resolutional modeling and identification; Stochastic analysis of network performance; Handling Rare Events.

4.4. Understanding what is going on: Improved State Estimation, Monitoring and Simulation

- Use sensed variables to improve quality and speed of state (and topology and parameter) estimation
- System-wide monitoring, disturbance signatures
- Situational awareness
- Post disturbance analysis
- Dynamic determination of Available Transfer Capability (ATC)
- Voltage instability prediction
- Use as corrective inputs to (near/faster than) real-time simulators (observers) for wide-area dynamics? – multi-resolutional models.
- Impact on market transactions?

4.5. Overall Systems Science and Dynamics (including infrastructure, ecology/environment, markets, and data-driven policy designs)

- Theoretical framework, modeling and simulation tools for infrastructure couplings and fundamental characteristics, to provide:
  - An understanding of true dynamics and impact on infrastructure reliability, robustness and resilience
  - Real-time state estimation and visualization of infrastructures– flexible and rapidly adaptable modeling and estimation
  - An understanding of emergent behaviors, and analysis of multi-scale and complexity issues and trends in the future growth and operations.
- Integrated dynamic risk assessment, monitoring, and early warning:
  - Vulnerability assessment, risk analysis and management
  - Underlying causes, distributions, and dynamics of and necessary/sufficient conditions for cascading breakdowns (metrics).
  - Infrastructure databases, data mining and early signature detection

Now let us press forward with a brief history of how we got here and potential roads ahead and how our community can and must be involved in shaping smarter and more resilient power and energy systems.

4.6. Background: Historical Perspective

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%.The 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 hours or longer per day).

Since the industrial revolution, worldwide energy consumption has been growing steadily. In 1890, the consumption of fossil fuels roughly equaled the amount of biomass fuel burned by households and industry. In 1900, global energy consumption equaled 0.7 TW (1 TW $=10^{12}$ Watts)[1]. The twentieth century saw a rapid twenty-fold increase in the use of fossil fuels. Between 1980 and 2004, the worldwide annual growth rate was 2%[1]. According to the US Energy Information Administration's (EIA's) 2006 estimate, of the estimated 15 TW of total energy consumption in 2004, fossil fuels supplied 86%. North

America consumed about 4,322 terawatt hours (TWh) of electricity in 2000, or about 30 percent of the estimated global electricity demand. Canada consumed 546 TWh; Mexico consumed 155 TWh; and the United States consumed 3,621 TWh.

EIA predicts that the world's electricity consumption will double in the next 25 years. Worldwide, current production is near 15,000 billion kilowatt-hours (kWh) per year. In 2030, projections reach more than 30,000 billion kWh/yr, which will require a rigorous 2 percent increase in electricity generating capacity each year between now and then.

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. 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.

4.7. The "Grid"

When most people talk about the 'grid' they are usually referring to the electrical transmission system, which moves the electricity from the power plants to the substations located close to large groups of users [2, 3, 45]. But, it also encompasses the distribution facilities that move the electricity from the substations to the individual users.

Possibly the largest machine in the world, the North American electric power network's transmission lines connect all generation and distribution on the continent to form a vertically integrated hierarchical network. In the US alone, the electrical network includes some 15,000 generators, with an average thermal efficiency of approximately 33% at 10,000 of these power plants. These generators send power through over 450,000 miles of high-voltage (>100KV) transmission lines. In addition, there are about 5,600 distribution facilities. In 2002, the installed generating capacity in the U.S. was 981,000 MW. If the power plants ran full time, the net annual generation would be 8,590 x 10^6 kWh; the actual net generation was 3,840 x 10^6 kWh, representing a 'capacity factor' of 44.7%.

While electricity demand increased about 25% since 1990, construction of transmission facilities decreased about 30%[2]. The planned transmission lines (230 kV or greater) for the period from 2004–2013 total approximately 7,000 miles[3]. According to the EIA, 281 GW of new generating capacity will be needed by 2025 to meet the growing demand for electricity; based on current needs, this implies a need for approximately 50,000 miles of new HV transmission lines.

As currently configured, the continental-scale grid is a multi-scale, multi-level hybrid system consisting of vertically integrated hierarchical networks including the generation layer and the following three basic levels:

- **Transmission:** Meshed networks combining extra high voltage (above 300 kV) and high voltage (100–300 kV) lines, connected to large generation units, very large customers, and, via tie-lines, to neighboring transmission networks and to the sub-transmission level.
- **Sub-transmission:** A radial or weakly coupled network including some high voltage (100–300 kV) lines but typically 5-15 kV lines connected to large customers and medium-size generators.
- **Distribution:** Typically a tree network including low voltage (110-115 or 220-240 V) and medium voltage (1-100 kV) lines, connected to small generators, medium-size customers, and local low-voltage networks for small customers.

In its adaptation to disturbances, a power system can be characterized as having multiple states, or "modes," during which specific operational and control actions and reactions are taking place:

- Normal: Economic dispatch, load frequency control, maintenance, forecasting, etc.
- Disturbance: Faults, instability, load shedding, etc.
- Restorative: Re-scheduling, re-synchronization, load restoration, etc.

In the normal mode, the priority is on economic dispatch, load frequency control, maintenance, and forecasting. In the disturbance mode, attention shifts to faults, instability, and load shedding. In the restorative mode, priorities include rescheduling, resynchronization, and load restoration. Some authors include an alert mode before the disturbance actually affects the system; DyLiacco [18] classified power system operating states into normal, emergency and restorative. The concept was extended by Cihlar *et al.* [14] by adding an alert state (Fig. 2).

Others add a system failure mode before restoration is attempted; Fink and Carlsen [24] further extended the classification by dividing the emergency state into two separate states, emergency and *in extremis*, based on system integrity and balance between generation and load. Another contribution was provided by Zaborszky *et al.* [50], who subdivided the emergency state into three crises (stability, viability, and integrity) to bring dynamics and time-frame characteristics into consideration. Stability emergencies include transient and oscillatory instability,

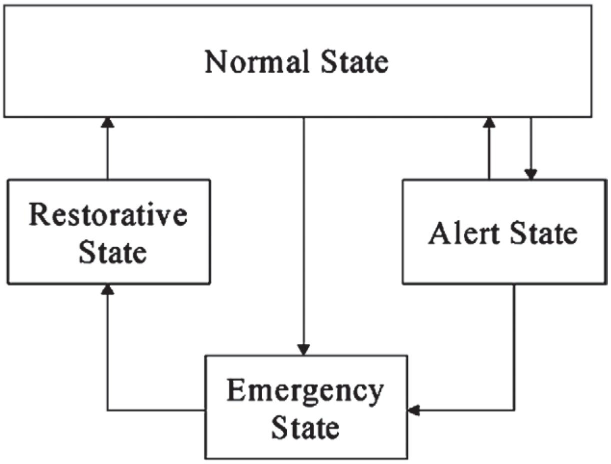


Fig. 2. Four states of a power system [14, 18, 24, 46, 47, 50]. ***Normal mode:*** economic dispatch, load frequency control, maintenance, forecasting, etc.; ***Alert mode:*** red flags, precursor detection, reconfiguration and response; ***Emergency/Disturbance mode:*** stability, viability, and integrity – instability, load shedding, etc.; ***Restorative mode:*** rescheduling, resynchronization, load restoration, etc.

which occur in time frames of a few to tens of seconds. Viability emergencies are longer term operation contingencies, such as voltage instability which may last for several minutes to even hours such as the precursor signatures in the reactive power during the August 2003 northeastern United States–Canada blackout.

Schulz and Price [46, 47] first addressed the issue of emergency identification by proposing emergency classification schemes with four dimensions: system integrity, branch loading, active power balance, and reactive power balance. An emergency detector was proposed that sensed local variables (such as voltages, power, and frequency), processed the data, compared them to *a priori* analysis results, and would initiate appropriate control actions if necessary. Besides these many operational, spatial, and energy levels, power systems are also multi-scaled in the time domain, from nanoseconds to decades, as shown in Table 1.

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

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

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

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

Besides these spatial, energy, and operational levels, power systems are also multi-scaled in the time domain, from nanoseconds to decades, as shown in Table 1.

Why the need for a system of such daunting complexity? In principle, it might seem possible to satisfy a small user group – for example, a small city – with one or two generator plants. However, the electricity supply system has a general objective of very high reliability, and that is not possible with a small number of generators. This is what led the industry to the existing system in North America where there are just three

Table 1. Multi-scale Time Hierarchy of Power Systems.

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

'interconnects.' Within each of these interconnects, all generators are tightly synchronized, and any failure in one generator immediately is covered by other parts of the system. The interconnects are the Eastern, covering the eastern two thirds of the U.S. and Canada; the Western, covering the rest of the two countries; and the Electric Reliability Council of Texas (ERCOT) covering most of Texas. The interconnects have limited DC links between them.

One of the important issues about the use of electricity is that storage is very difficult, and thus generation and use must be matched continuously. This means that generators must be dispatched as needed. The U.S. power grids have approximately 150 Control Area Operators using computerized control centers to meet this need. Generally, generators are classified as baseload, which are run all the time to supply the minimum demand level; peaking, which are run only to meet power needs at maximum load; and intermediate, which deal with the rest. Actually, the dispatch order is much more complicated than this, because of the variation in customer demand from day to night and season to season.

Furthermore 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 question is raised as to whether there is a unifying paradigm for the high-confidence and fast simulation, analysis, and optimization of time-critical operations (both financial transactions and actual physical control) in these multiscale, multicomponent, and distributed systems. In addition, mathematical models of interactive networks are typically vague (or may not even exist); moreover, existing and classical methods of solution either are unavailable or are not sufficiently powerful. For the most part, no present methodologies are suitable for understanding their behavior.

Another important dimension is the effect of deregulation and economic factors on a particular infrastructure. While other and more populous countries, such as China and India, will have greater potential electricity markets and demands, the United States is currently the largest national market for electric power. Its electric utilities have been mostly privately owned, vertically integrated, and locally regulated. National regulations in areas of safety, pollution and network reliability also constrain their operations to a degree, but local regulatory bodies, mostly at the state level, have set their prices and their return on investment, and have controlled their investment decisions while protecting them from outside competition. That situation changes during the last 15 years, as state regulators moved toward permitting and encouraging a competitive market in electric power.

4.8. An Increasingly Stressed Infrastructure

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 [1, 3, 20–23, 34]. This has resulted in a mode of operation of the system that is analogous 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

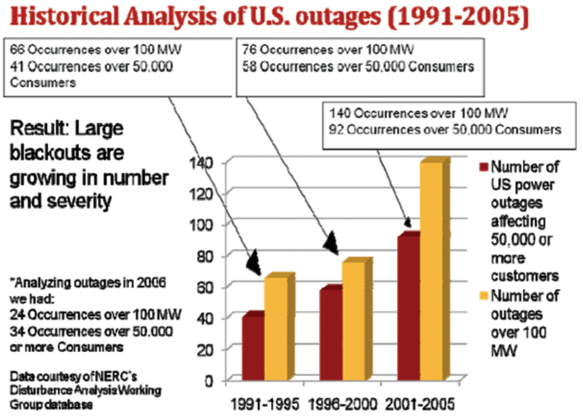


Fig. 3. U.S. Electric power outages over 100MW and affecting over 50,000 consumers (1991–2005).

margin will exist to support anticipated demand is in question.

To assess impacts using 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).

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 minutes per year in the Midwest and 214 minutes in the Northeast. Japan, by contrast, averages only 4 minutes of interrupted service each year. The outage data exclude interruptions caused by extraordinary events such as fires or extreme weather.

I analyzed 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). 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.

These two data sets each contain events not listed in the other data set. In general, the EIA database contains more events, and the NERC database gives more information about the events. 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 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 five-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 megawatts 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. 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 hour or more be reported in OE-417, where it was only required for 3 hours or more in EIA-417R prior to 2003. Adjusting for the change in reporting in

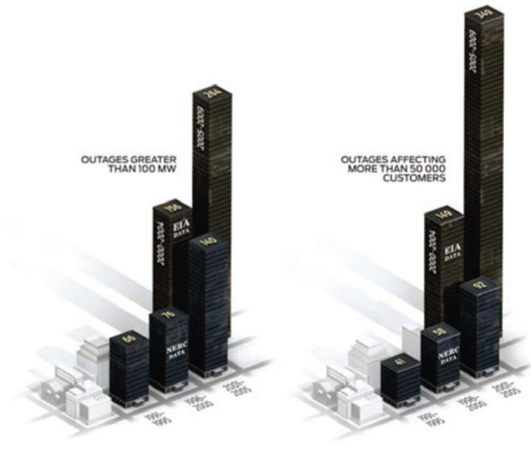


Fig. 4. Power Outages have steadily increased[1,2] in the most recent decade.

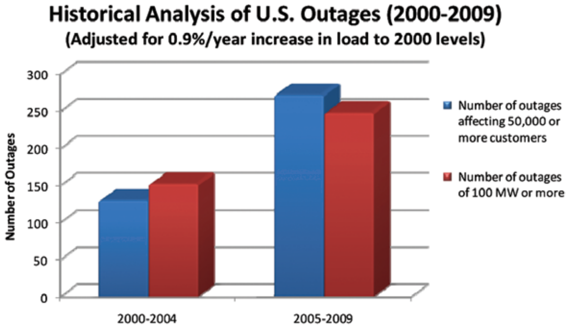


Fig. 5. U.S.electric power outages over 100MW and affecting over 50,000 consumers during 2000–2009, adjusted for 0.9% annual increase in load and adjusted for change in reporting in 2003 (using all the data from 2000–2009 and only counting the outages that met the less stringent requirements of the EIA-417R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

Table 2. U.S. electric power outages over 100MW 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).

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

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 (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 shown in Table 2.

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 "can." We must—if the United States is to continue to be an economic power. However, it will not be easy or cheap.

4.9. Pathways Forward: Costs/Benefits of Full Deployment of Stronger and Smarter Grids

In a recent nation-wide survey, most of consumers in the U.S. (~68%) did not know what "Smart Grid," meant. We must assess and clearly articulate: 1) what is the "Smart Grid" or what will it do for consumers? and 2) 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?

Regarding the first question... *So what is the smart self-healing grid?*

Here are the definitions for the smart "self-healing" grid, which I proposed and have utilized in all pertinent projects while at EPRI and beyond since January 1998:

- The term "smart grid" refers to the use of computer, communication, sensing and control technology which operates in parallel with an electric power grid for the purpose of enhancing the reliability of electric power delivery, minimizing the cost of electric energy to consumers, improving security, quality, resilience, robustness, and facilitating the interconnection of new generating sources to the grid.
- A system that uses information, sensing, control and communication technologies to allow it to deal with unforeseen events and minimize their adverse impact. It is a secure "architected" sensing, communications, automation/control, and energy overlaid infrastructure as an integrated, reconfigurable, and electronically controlled system that will offer unprecedented flexibility and functionality, and improve system availability, security, quality, resilience and robustness.

The concept of smart grids, pertinent R&D programs aimed at developing self-healing grids, and the associated terminology, date back to 1990s (Fig. 6). Of particular interest is a large-scale research program conducted jointly by the Electric Power Research Institute (EPRI) and the U.S. Department of Defense (DOD) during 1998 – 2002, titled Complex Interactive Networks/ Systems Initiative

[1] Source: Amin, M. "U.S. Electrical Grid Gets Less Reliable," IEEE Spectrum, January 2011, and online at http://spectrum.ieee.org/energy/policy/us-electrical-grid-gets-less-reliable

[2] Research is supported by a grant from the NSF and a contract with SNL.

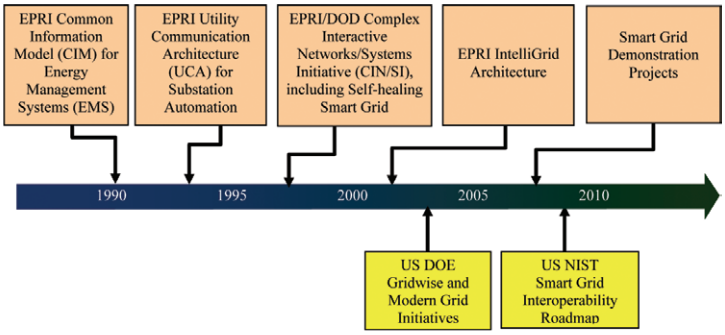

EPRI Common Information Model (CIM) for Energy Management Systems (EMS)
EPRI Utility Communication Architecture (UCA) for Substation Automation
EPRI/DOD Complex Interactive Networks/Systems Initiative (CIN/SI), including Self-healing Smart Grid
EPRI IntelliGrid Architecture
Smart Grid Demonstration Projects
1990
1995
2000
2005
2010
US DOE Gridwise and Modern Grid Initiatives
US NIST Smart Grid Interoperability Roadmap

Fig. 6. History and evolution of Smart Grid programs.

(CIN/SI [6, 7, 20]). This work provided the mathematical foundations and simulations for the smart self-healing grid and showed that the grid can be operated close to the limit of stability given adequate situational awareness combined with better secure communication and controls.

- 1998–2002: Self-Healing Grid as part of CIN/SI at the Electric Power Research Institute (EPRI)
  - 1998–2002: EPRI/DOD Complex Interactive Networks/Systems Initiative (CIN/SI): Mathematical underpinnings to model, simulate, optimize and manage the emerging interdependent power, energy, telecommunications, finance and transportation networks as Complex Adaptive Infrastructure Systems (with an underpinning smart grid or energy web)
  - 108 professors and over 240 graduate students in 28 U.S. universities funded, including Carnegie Mellon, Minnesota, Illinois, Arizona St., Iowa St., Purdue, Harvard, MIT, Cornell, UC-Berkeley, Wisconsin, RPI, UTAM, Cal Tech, UCLA, and Stanford.
  - 52 utilities and grid operators participated and provided feedback; 24 resultant technologies including smart self-healing grid extracted.
- 2001-present: Intelligrid (EPRI trademarked)
- 2004-present: Smart Grid (final name adopted at EPRI, industry, and US DOE)

As part of the joint EPRI and U.S. Department of Defense (DOD) program, the Complex Interactive Networks/Systems Initiative (CIN/SI), identified and addressed a broad spectrum of CSS-related challenges to the power grid, energy and communication infrastructures and developed modeling, simulation, analysis, and synthesis tools for damage-resilient control of the electric power grid and interdependent infrastructures connected to it. This work provided the mathematical foundations and simulations for the smart self-healing grid and showed that the grid can be operated close to the limit of stability given adequate situational awareness combined with better secure communication and controls.

Since then, there have been several convergent definitions of "smart grids", including within the 2007 Energy Bill, along with informative reports by EPRI (1998-present), NIST [38, 39] and U.S. DOE (2007–2010), and definitions by the IEEE, FERC, GE and Wikipedia. Many define "Smart Grid" in terms of its functionalities and performance objectives (e.g., two-way communications, interconnectivity renewable integration, demand response, efficiency, reliability, self-healing, etc.).

There are many definitions, but there is one vision of a highly instrumented overlaid system with advanced sensors and computing with the use of enabling platforms and technologies for secure sensing, communications, automation and controls as keys to: 1) engage consumers, 2) enhance efficiency, 3) ensure reliability, 4) enable integration of renewables and electric transportation.

Regarding the second set of questions... *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), incl. new generators and power delivery systems.
- A detailed study by the Electric Power Research Institute (EPRI) published in April 2011, finds that 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 [44],
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:

    a. Local microgrids (that can be as self-sufficient as possible and island rapidly during emergencies), and
    b. 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 gird 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 CO2 emissions from the electric sector by 58 percent, relative to 2005 emissions.
7. Increased cyber/IT security, and overall energy security, if security is built in the design as part of a layered defense system architecture.
8. Electricity's unique capability to be produced from a wide variety of local energy sources, along with its precision, cleanliness, and efficiency, make it the ideal energy carrier for economic and social development.

In addition, the current high-voltage system needs to be expanded and strengthened (U.S. DOE National Electric Transmission Congestion Study, AEP HV transmission assessment for wind integration, and EPRI assessments 2003-2009). The total cost of the expanded transmission system is about $82 billion.

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.

Upgrading control and communication systems for the power grid will present many new security challenges that must be dealt with before extensive deployment and implementation of smart grid technologies can begin. The digitalization of such systems may enable remote attacks to grow rapidly, potentially spanning countries or even continents. Moreover, the number of threats against computer systems is rapidly increasing due to the increased availability of more sophisticated hacker tools on the Internet and the decrease in technical knowledge required to use them to cause damage. While the digitalization of such systems will present many new security challenges, it will also provide the gird with increased flexibility to prevent and withstand potential threats.

4.10. Key Smart Grid Security Challenges

4.10.1. Physical

The size and complexity of the North American electric power grid makes it impossible both financially and logistically to physically protect the entire infrastructure. There currently exists over 450,000 miles of 100kV 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 as the DOE has concluded that generating 20% of electricity with land-based wind installations will require at least 20,000 square miles. Thus, it is probable that a well-organized determined group of terrorists could take out portions of the grid as they have previously done in the United States, Colombia, and other locations around the globe. Several publicly known cases in the United States have occurred during the last 30 years, including saboteurs in the Pacific Northwest and those using power lines and transformers for target practice on the East Coast. Colombia, for example, has faced up to 200 terrorist attacks per year on its transmission infrastructure over the last 11 years as reported in a recent *Power & Energy Magazine* article by Corredor and Ruiz.

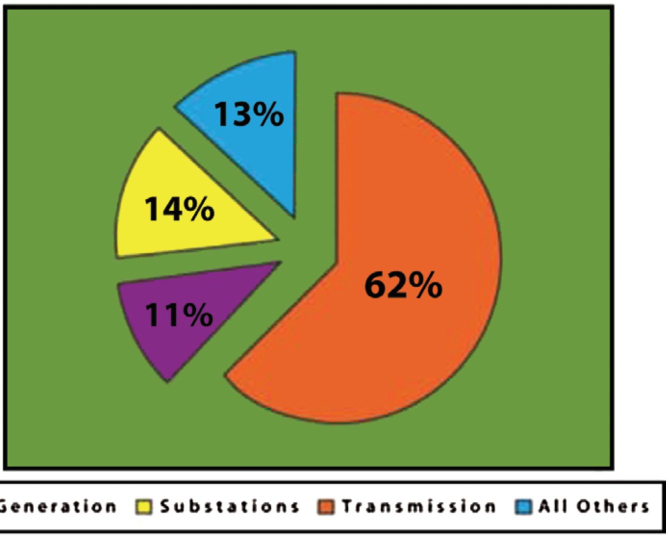


Fig. 7. Electric Terrorism: Grid Component Targets (1994–2004) [15].

However, such attacks, although troublesome and costly to the local region, affect only a small portion of the overall grid. To cause physical damage equivalent to that of a small- to moderate-scale tornado would be extremely difficult even for a large well-organized group of terrorists.

Data from the National Memorial Institute for the Prevention of Terrorism on terrorist attacks on the world's electricity sector from 1994–2004 show that transmission systems are by far the most common target in terms of the total number of physical attacks. Fig. 7 shows the percentage of terrorist attacks aimed at each of the major grid components.

One possible solution to increase the physical security of power lines is to bury them. However, a 2006 study by the Edison Electric Institute (EEI) calculated that putting power lines underground would cost about $1 million a mile compared with $100,000 for overhead lines, thus making it financially infeasible.

4.10.2. Cyber

The number of documented cyber attacks and intrusions worldwide has been rising very rapidly in recent years. The results of a 2007 survey by McAfee highlight the pervasiveness of such attacks. DDOS attacks utilize networks of infected computers, whose owners often do not even know that they have been infected, to overwhelm target networks with millions of fake requests for information over the Internet.

Due to the increasingly sophisticated nature and speed of some malicious code, intrusions, and denial-of-service attacks, human response may be inadequate. Fig. 8 shows the evolution of cyber threats over the last two decades and the types of responses that can be used to effectively combat them.

In addition, adversaries often have the potential to initiate attacks from nearly any location in the world. A July 2010 article in *The Economist* quoted one senior American military source saying that, "If any country were found to be planting logic bombs on the grid, it would provoke the equivalent of the Cuban missile crisis." Furthermore, currently more than 90% of successful cyber attacks take advantage of known vulnerabilities and misconfigured operating systems, servers, and network devices.

Security of cyber and communication networks is fundamental to the reliable operation of the grid. As power systems rely more heavily on computerized communications and control, system security has become increasingly dependent on protecting the integrity of the associated information systems. Part of the problem is that existing control systems, which were originally designed for use with proprietary, standalone communication networks, were later connected to the Internet (because of its productivity advantages and lower costs), but without adding the technology needed to make them secure. Moreover, numerous types of communication media and protocols are used in the communication and control of power systems. Within a substation control network, it is common to find commercial telephone lines, wireless, microwave, private fiber, and Internet connections. The diversity and lack of interoperability between the communication protocols causes problems for anyone who tries to establish secure communication to and from a substation.

Electric power utilities also typically own and operate at least parts of their own telecommunications systems, which often consist of backbone fiber optic or microwave,

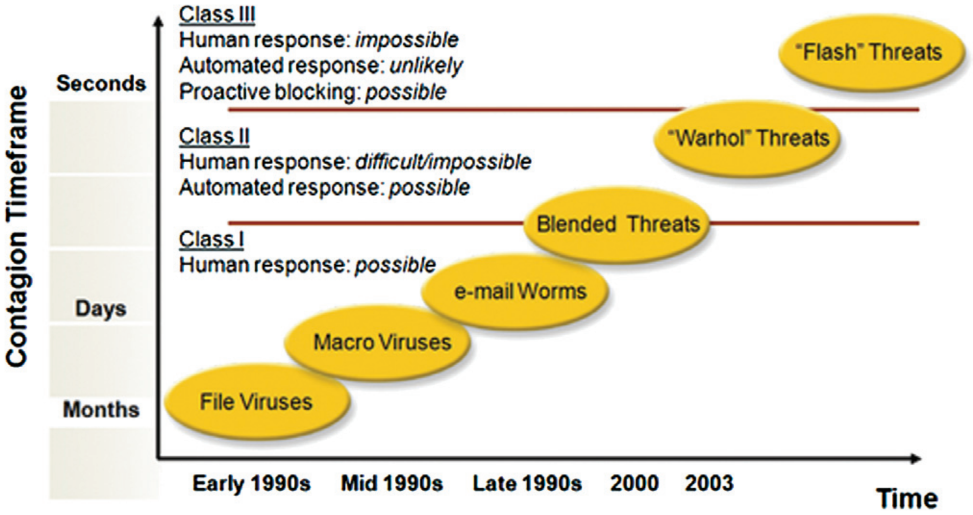


Fig. 8. Threat Evolution (EPRI EIS and ISI programs [4, 5]).

connecting major substations with spurs to smaller sites. Increased use of electronic automation raises significant issues regarding the adequacy of operational security, if security provisions are not built in.

More specifically, the operation of a modern power system depends on complex systems 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, communications, 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.

Any telecommunication link that is even partially outside the control of the organization that owns and operates power plants, Supervisory Control and Data Acquisition (SCADA) systems, or Energy Management Systems (EMSs) represents a potentially insecure pathway into the business operations of the company as well as a threat to the grid itself. The interdependency analyses done by most companies in the last 14 years (starting with preparations for Y2K, and after the tragic events of 9/11) have identified these links and the system's vulnerability to their failures. Thus, they provide an excellent reference point for a cyber-vulnerability analysis.

While some of the operations on the system are automatic, ultimately human operators in system control centers make decisions and take actions to control the operations 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 be concerned about two other factors: the reliability of the operators within the centers, and the possibility that insecure code has been added to a program in a center computer. The threats posed by "insiders," as well as the risk of a "Trojan horse" embedded in the software of one of more of the control centers is real. A 2008 survey by the Computer Security Institute/Federal Bureau of Investigation of data compiled from 522 computer security practitioners and senior executives from U.S. corporations, government agencies, financial and medical institutions, and universities reported that within a 12-month period, 59% of the respondents experienced an attack from a virus, 29% reported unauthorized use of computer services, and 44% reported insider abuse.

The threat of a "Trojan horse" embedded in the control center software can only be addressed by both careful security measures within the commercial firms that develop and supply this software, and careful security screening of the utility and outside service personnel who perform software maintenance within the centers. Today, security patches often are not supplied to end-users, or users are not applying the patches, as they fear they will affect system performance. Current practice is to apply an upgrade or patch only after SCADA vendors thoroughly test and validate them, sometimes causing a delay in their deployment of several months.

As a result, cyber security is just as important if not more so than physical security. Due to the gravity of these threats, the Federal Energy Regulatory Commission (FERC) policy statement on smart grid has stated that cyber security is essential to the operation of the smart grid and that the development of cyber security standards is a key priority. The U.S. DOE has also stated that the ability to resist attack – by identifying and responding to disruptions caused by sabotage – is one of Smart Grid's seven crucial functions. However, significant work must still be done to create standards that if implemented will adequately protect the grid from cyber attacks. Emerging standards fall well short of achieving this ultimate goal.

4.11. Smart Grid Security Needs

4.11.1. Layered Security

In order to protect electric infrastructure from the threats outlined above several layers of security are needed to minimize disruptions to system operations. Layered security (or defense-in-depth) involves strategically combining multiple security technologies at each layer of a computing system, with embedded security, in order to reduce the risk of unauthorized access due to the failure of any single security technology. It exponentially increases the cost and difficulty for an attacker to compromise a system by creating a much stronger defense than the use of any individual component alone, thus, reducing the likelihood of an attack.

The trend of connecting electrical control systems to the Internet exposes all layers of a system to possible attack. Computing layers that must be considered include:

- Personnel
- Networks
- Operating Systems
- Applications
- Databases

Security features to be employed at each layer include examination, detection, prevention, and encryption. To protect control systems, well-established information security practices must also be utilized.

4.11.2. Deception

An additional defense mechanism is the use of deception. Deception consists of two possible techniques, dissimulation, hiding the real, and simulation, showing the false. McQueen and Boyer describe several potential dissimulation and simulation techniques that can be used for control systems. Three potential dissimulation techniques described include:

1) **Masking** the real by making a relevant object be undetectable or blend into background irrelevance
2) **Repackaging** which hides the real by making a relevant object appear to be something it is not
3) **Dazzling** which hides the real by making the identification of a relevant object less certain by confusing the adversary about its true nature.

Likewise, three potential simulation techniques described include:

1) **Inventing** the false by creating a perception that a relevant object exists when it does not
2) **Mimicking** which invents the false by presenting characteristics of an actual, and relevant object
3) **Decoying** which displays the false by attracting attention away from a more relevant object.

Deception will need to play a key role in smart grid defense mechanisms. Since existing control system architectures are not random, and therefore response characteristics are reproducible, the strength of potential adversaries is amplified. Deception defense mechanisms can greatly increase the difficulty of planning and conducting successful attacks upon a system by portraying control system response characteristics as random to attackers. They can also alert operators to possible threats before any systems are harmed.

Additional security needs include rapid containment, restoration, and recovery strategies for when systems are inevitably compromised. Either software patching or the ability to rapidly identify and isolate the exploited systems must be enabled in order to minimize downtime. This is extremely important since the consequences of an attack are directly proportional to the length of time that the service is disrupted.

4.12. Advanced Metering Infrastructure

4.12.1. Vulnerabilities

The implementation of advanced metering infrastructure (AMI) is widely seen as the first step in the digitalization of the electric grid control systems. Despite the increase in the utilization of AMI, there has been very little assessment or R&D effort to identify the security needs for such systems. Smart meters, however, are extremely attractive targets for exploitation since vulnerabilities can be easily monetized through manipulated energy costs and measurement readings. Currently, in the U.S. alone, it is estimated that $6 billion is lost by electricity providers to consumer fraud in the electric grid. Possible threats to the electrical grid introduced by the use of AMI include:

- Fabricating generated energy meter readings
- Manipulating energy costs
- Disrupting the load balance of local systems by suddenly increasing or decreasing the demand for power
- Gaining control of possibly millions of meters and simultaneously shutting them down
- Sending false control signals
- Disabling grid control center computer systems and monitors
- Disabling protective relays.

As more utilities move toward using Internet protocol (IP)-based systems for wide area communications and the trend of using standardized protocols continues throughout the industry, maintaining the security of such devices will be critical. AMI introduces earnest privacy concerns, as immense amounts of energy use information will be stored at the meter. Breaches into this data could expose customer habits and behaviors. Such arguments have led to the recent moratoriums on AMI installations in numerous Northern California communities and other areas throughout the country. As a result, several key privacy concerns need to be addressed, including those outlined by the National Institute of Standards and Technology (NIST) Cyber Security Working Group. These include:

- Personal Profiling – using personal energy data to determine consumer energy behavioral patterns for commercial purposes
- Real-time Remote Surveillance – using live energy data to determine whether people are in a specific facility or residence and what they are doing
- Identity Theft and Home Invasions – protecting personal energy data from criminals who could use them to harm consumers
- Activity Censorship – preventing the use of energy for certain activities or taxing those activities at a higher rate
- Decisions Based on Inaccurate Data – shutting off power to life-sustaining electrical devices or providing inaccurate information to government and credit-reporting agencies.

In addition, AMI systems will need to be defended against more traditional cyber threats such as mobile/malicious code, denial-of-service attacks, misuse and malicious insider threats, accidental faults introduced by human error, and the problems associated with software and hardware aging.

4.12.2. Security Needs

In order to defend against the vulnerabilities described above, several security features need to be incorporated into the development of AMI, along with new privacy laws to protect consumers. Current privacy laws in the United States are fragmented and vague, and do not specifically address consumer energy usage. Data stored at the meter and transmitted over communication networks must also meet standard cyber security requirements, such as confidentiality, integrity, availability, and non-repudiation.

One security feature alone, such as encryption, will not be able to cover all possible security threats. Since it will be imperative that the industry maintain 100 percent uptime, both physical security of the AMI system hardware, and multiple standard IT security features such as encryption and authentication will be needed. Furthermore, since it will be impossible to protect against all threats, smart meters must be able to detect even the most subtle unauthorized changes and precursors to tampering or intrusion. Additional consideration must also be given to both the cost and impact that the security features will have on AMI system operations. Smart meters will need to be cost effective since millions will need to be purchased and installed to replace antiquated analog devices. Still, they must be sufficiently robust since they will be placed in very insecure locations.

4.13. Current Security Initiatives

Over the last decade and since the terrorist attacks of September 11, 2001, several steps have been taken and initiatives accomplished to enhance the security and reliability of the nation's current electricity infrastructure. These include the Complex Interactive Networks/Systems Initiative (CIN/SI), a joint program sponsored by the Electric Power Research Institute (EPRI) and the Department of Defense (DOD), the EPRI Enterprise Information Security (EIS) program, the EPRI Infrastructure Security Initiative (ISI) (post 9/11), and the North American Electric Reliability Corporation (NERC) initiatives such as the Information Sharing and Analysis Centers (ISACs), public key infrastructure (PKI), and spare equipment database. Information security frameworks for electric power utilities have also been developed by CIGRÈ. A security framework is considered as the skeleton upon which various elements are integrated for the appropriate management of security risk. The different elements considered by CIGRÈ include security domains, baseline controls, and security processes.

4.14. Research and Development Needs

Revolutionary developments in information technology, 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 this critical infrastructure continues to support population growth and economic growth without environmental harm.

4.14.1. Enabling Technologies

During the past 14 years, we have investigated whether there are leading applications of science and technology (S&T) outside the traditional electric energy industry that may apply in meeting and shaping consumer needs. These applications may include entirely new technologies, not part of the portfolio of traditional electricity solutions and not identified in other tasks, which could be potentially available as well. Some technology areas include:

- Materials and devices – including nanotechnology, microfabrication, advanced materials and smart devices
- Meso- and micro- scale devices, sensors, and networks
- Advances in information science: algorithms, AI, systems dynamics, network theory, and complexity theory
- Bioinformatics, biomimetics, biomechatronics, and systems biology
- Enviromatics: development and use of new methodologies and the use of state-of-the-art information technology for improved environmental applications
- Other industries – moving to a wireless world – transportation, telecommunications, digital technologies, sensing, and control
- Markets, economics, policy, and the environment
- End-to-end infrastructure – from fuel supply to end use

Examples of higher-level smart structures and systems that can be built from smart materials and utilized in the grid include:

1) **Flexible AC Transmission (FACTS):**[3] FACTS devices are a family of solid-state power control devices that provide enhanced power control capabilities to high-voltage AC grid operators. FACTS controllers act like integrated circuits – but scaled up by a factor of 500 million in power. By applying FACTS devices, utilities can increase the capacity of individual transmission lines by up to 50% and improve system stability by responding quickly to power disturbances. There is a need to reduce the costs of FACTS technology to provide for broader use. One method for reducing the costs is to replace the silicon-based power electronics with wide band-gap semiconductors such as silicon carbide (SiC), gallium nitride (GaN), and diamond.
2) **High Voltage Direct Current Transmission Systems (HVDC):** These transmission systems are based on the rectification of the generated AC and then inversion back to AC at the other end of the transmission line. Modern systems are based on thyristor valves (solid-state power control devices) to perform the AC/DC/AC conversions. Conventional HVDC transmission systems have been built with power transfer capacities of 3000 MW and 600 kV. A new class of HVDC converter technology has been introduced in the last few years, referred to as voltage source converters (VSC), and it is based on gate turn-off switching technology or insulated gate bi-polar transistors, IGBT. These devices have higher switching frequency capability. HVDC transmission is used in long distance bulk power transmission over land, or for long submarine cable crossings. Altogether, there are more than 35 HVDC systems operating or under construction in the world today. The longest HVDC submarine cable system in operation today is the 250 km Baltic Cable between Sweden and Germany.
3) **Dynamic Line Rating:** The maximum power that can be carried by a transmission line is ultimately determined by how much the line heats up and expands. The "thermal rating" of a line specifies the maximum amount of power it can safely carry under specific conditions without drooping too much. Most thermal ratings today are static in the sense that they are not changed through the year. For such ratings to be reliable, they must be based on worst-case weather conditions, including both temperature and wind velocity. Dynamic line ratings use real-time knowledge about weather or line sag to determine how much power can be transmitted safely. Typically, a dynamically monitored line can increase its allowable power flow (ampacity) by 10–15% over static ratings.

In the future, smart materials and structures are expected to show up in applications that span the entire electric power system, from power plant to end user. Smart materials, in their versatility, could be used to monitor the integrity of overhead conductor splices, suppress noise from transformers and large power plant cooling fans, reduce cavitation erosion in pumps and hydroturbines, or allow nuclear plants to better handle structural loads during earthquakes.

[3] FACTS devices are used for the dynamic control of voltage, impedance and phase angle of high voltage AC transmission lines. The main types of FACTS devices are:

1. **Static Var Compensators (SVC's)**, the most important FACTS devices, have been used for a number of years to improve transmission line economics by resolving dynamic voltage problems. Their accuracy, availability, and fast response enable SVC's to provide high performance steady state and transient voltage control compared with classical shunt compensation. SVC's are also used to dampen power swings, improve transient stability, and reduce system losses by optimized reactive power control.
2. **Thyristor controlled series compensators (TCSCs)** are an extension of conventional series capacitors created by adding a thyristor-controlled reactor. Placing a controlled reactor in parallel with a series capacitor enables a continuous and rapidly variable series compensation system. The main benefits of TCSCs are increased energy transfer, dampening of power oscillations, dampening of subsynchronous resonances, and control of line power flow.

   STATCOMs are GTO (gate turn-off type thyristor) based SVC's. Compared with conventional SVC's (see above) they do not require large inductive and capacitive components to provide inductive or capacitive reactive power to high voltage transmission systems. This results in smaller land requirements. An additional advantage is the higher reactive output at low system voltages where a STATCOM can be considered as a current source independent from the system voltage. STATCOMs have been in operation for over 10 years.

Unified Power Flow Controller (UPFC). Connecting a STATCOM, which is a shunt connected device, with a series branch in the transmission line via its DC circuit results in a UPFC. This device is comparable to a phase shifting transformer but can apply a series voltage of the required phase angle instead of a voltage with a fixed phase angle. The UPFC combines the benefits of a STATCOM and a TCSC.

4.15. An Example of a Smart Infrastructure – A Smarter and More Secure I-35W Bridge:

Within less than a year after the August 2007 collapse of the I-35W bridge in Minneapolis, Minnesota, a city of sorts on the south side of the former took shape, complete with a host of heavy-duty equipment, temporary on-site areas for casting and other tasks, and crews constantly at work. The days and months that followed required extraordinary efforts from many, including alumni of our infrastructure systems engineering program. They incorporated a sensor network into the new I-35W bridge (at less than 0.5% of total cost) which provides full situational awareness of stressors, fatigue, material, and chemical changes to measure and understand precursors to failures and to enable proactive and *a priori* corrective actions.

Analogously, customized and cost-effective advancements noted above are both possible and essential to enable smarter and more secure electric power infrastructures. For example, advanced technologies discussed which are now under development or under consideration hold the promise of meeting the electricity needs of a robust digital economy. 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.

However, considerable technical challenges as well as several economic and policy issues remain to be addressed. At the core of the power infrastructure investment problem lies two paradoxes of restructuring, one technical and one economic. Technically, the fact that electricity supply and demand must be in instantaneous balance at all times must be resolved with the fact that new power infrastructure is extraordinarily complex, time-consuming, and expensive to construct. Economically, the theory of deregulation aims to achieve the lowest price through increased competition. However, the market reality of electricity deregulation has often resulted in a business-focused drive for maximum efficiency to achieve the highest profit from existing assets and does not result in lower prices or improved reliability. Both the technical and economic paradoxes could be resolved by knowledge and technology.

From a broader perspective, in a single century, electricity became the foundation and prime mover of our modern society. Not just as a clean and convenient form of energy, but as the toolmaker's dream. Electricity opened the doors of invention to new technologies of incredible precision, intelligence and communication, and to new forms of instrumentation and innovation. Given economic, societal, and quality-of-life issues and the ever-increasing interdependencies among infrastructures, a key challenge before us is whether the electricity infrastructure will evolve to become the primary support for the 21st century's digital society – a smart grid with self-healing capabilities – or be left behind as a 20th century industrial relic.

Acknowledgement

This work is supported by the National Science Foundation under grant number 0831059, and grants from EPRI, Honeywell Labs, and the Sandia National Laboratories' Grand Challenge LDRD 11-0268.

Suggestions for Further Reading

1. M. Amin, B.F. Wollenberg, Toward a smart grid: power delivery for the 21st century. *IEEE Power and Energy Magazine*, **3**:5 (2005), 34–41.

   This paper provides a vision and approach to enable smart, self-healing electric power systems that can respond to a broad array of destabilizers.
2. M. Amin, Special issue on energy infrastructure defense systems. *Proceedings of the IEEE*, **93**:5 (2005).

   This issue is devoted to the defense of energy infrastructure, including topics such as software, applications and algorithmic developments, the use of sensors and telecommunication to increase situational awareness of operators/security monitors, signals and precursors to failures, infrastructure defense plans, wide-area protection against rare events and extreme contingencies, and rapid/robust restoration.
3. M. Amin, Modeling and control of complex interactive networks. *IEEE Control Systems Magazine*, **22**:1 (2002), 22–27.

   This paper provides a description of the issues dealing with the modeling of critical national infrastructures as complex interactive networks.
4. P. Kundur, *Power System Stability and Control*, EPRI Power System Engineering Series (New York: McGraw-Hill, Inc., 1994).

   This book provides an in-depth explanation of voltage stability, covering both transient and longer-term phenomena and presenting proven solutions to instability problems.

References

1. Amin M. U.S. electrical grid gets less reliable. *IEEE Spectr* 2011; 48(1): 80.
2. Amin M, Stringer J. The Electric Power Grid: Today and Tomorrow, *MRS Bull* 2008; 33(4): 399–407.
3. Amin M, Schewe PF. Preventing blackouts. *Sci Am* 2007; 60–67.

4. Amin M. North America's electricity infrastructure: Are we ready for more perfect storms? *IEEE Secur Priv* 2003; 1(5): 19.
5. Amin M. Security Challenges for the Electricity Infrastructure. special issue of the *IEEE Comput Mag Secur Priv* 2002.
6. Amin M. Toward self-healing energy infrastructure systems cover feature in the *IEEE Comput Applications Power* 2001; 14(1): 20–28.
7. Amin M. Toward Self-Healing Infrastructure Systems. *IEEE Comput Mag* 2000; 33(8): 44–53.
8. Boukarim GE, Wang S, Chow JH, Taranto GN, Martins N. A comparison of classical, robust, and decentralized control designs for multiple power systems stabilizers. *IEEE Trans Power Syst* 2000; 15(4): 1287–1292.
9. Bykhovsky, Chow JH. Dynamic data recording in the New England power system and an event analyzer for the northfield monitor presented at the VII SEPOPE Conf., Curitiba, Brazil, 2000.
10. Canizares A, Alvarado FL. Point of collapse and continuation method for large AS/DC systems. *IEEE Trans Power Syst* 1993; 8(1).
11. Cheng X, Krogh BH. Stability constrained model predictive control for nonlinear systems, in *Proc. 36th IEEE Conf Decision Control* 1998; (3): 2091–2096.
12. Chow JH, Cheung KW. A toolbox for power system dynamics and control engineering education. *IEEE Trans Power Syst* 1992;7(4): 1559–1564.
13. Christie R. Power system test case archive. [Online]. Available:http://www.ee.washington.edu/research/pstca
14. Cihlar TC, Wear JH, Ewart DN, Kirchmayer LK. Electric utility system security presented at the Amer Power Conf, 1969.
15. Clemente J. The security vulnerabilities of smart grid. *J Energy Secur* 2009.
16. Corredor PH, Ruiz ME. Against all odds. *IEEE Power Energy Mag* 2011; 9(2): 59–66.
17. U.S. Department of Energy, *GridWorks: Overview Electric Grid* 2005–08.
18. DyLiacco TE. The adaptive reliability control system. *IEEE Trans Power App Syst* 1967; 517–561.
19. Edison Electric Institute, *Meeting US Transmission Needs* 2005–07.
20. Electric Power Research Institute (EPRI), Complex Interactive Networks/Systems Initiative: Final Summary Report. Overview and Summary Report for Joint EPRI and U.S. Department of Defense University Research Initiative 2003; 155.
21. EPRI, Electricity technology roadmap: synthesis module on power delivery system and electricity markets of the future, EPRI, Palo Alto, July 2003.
22. EPRI, *Electricity Technology Roadmap: 1999 Summary and Synthesis*, Technical Report, CI-112677-V1, 160 pp. EPRI, Palo Alto, July 1999 http://www.epri.com/corporate/discover_epri/roadmap/index.html
23. Ericsson GN. Information security for electric power utilities (EPUs)-CIGRE developments on frameworks, risk assessment, and technology. *IEEE Trans Power Delivery* 2009; 243: 1174–1181.
24. Fink LH, Carlsen K. Operating under stress and strain. *IEEE Spect* 1978; 48–53.
25. Flatabo N, Ognedal R, Carlson T. Voltage stability condition in a power transmission system calculated by sensitivity methods. *IEEE Trans Power Syst* 1990; 5(4): 1286–1293.
26. Gama C, Anguist L, Ingestrom G, Noroozian M. Commissioning and operative experience of the imperatriz TCSC for damping power oscillation in the Brazilian north-south interconnection presented at the VII SEPOPE Conf, Curitiba, Brazil, 2000.
27. Gao B, Morison GK, Kundar P. Voltage stability evaluation using modal analysis. *IEEE Trans Power Syst* 1992; 7(4): 1529–1542.
28. Ghandhari M, Andersson G, Hiskens IA. Control Lyapunov function for controllable series devices presented at the VII SEPOPE Conf, Curitiba, Brazil, 2000.
29. Glover JD, Sarma MS. Power system analysis and design. Boston, MA: PWS, 1993.
30. Hauer JF. Robust damping control for large power systems. *IEEE Control Syst Mag* 1989; 9(1): 12–18.
31. Hauer JF, Trudnowski DJ, Rogers GJ, Mittelstadt WA, Litzenberger WH, Johnson JM Keeping an eye on power system Dynamics. *IEEE Comput Appl Power* 1997; 10(4): 50–54.
32. Hingorani NG. Flexible AC transmission. *IEEE Spectr* 1993, 30(4): 40–45.
33. Kessel P, Glavitsch H. Estimating the voltage stability of a power system. *IEEE Trans Power Del* 1986; PWRD-1(3): 346–354.
34. Kirby B. Reliability management and oversight. DOE National Transmission Grid Study 2002.
35. Lerner JE. What's wrong with the electric grid? *Ind Physicist* 2003; 9(5): 8–13.
36. McDaniel P, McLaughlin S. Security and privacy challenges in the smart grid. *IEEE Secur Priv* 2009; 7(3): 75–77.
37. McQueen MA, Boyer WF. Deception used for cyber defense of control systems in 2nd Conference on Human System Interactions, Catania, Italy, 2009; 624–631.
38. NIST, National Institute of Standards and Technology, Guidelines for smart grid cyber security, The Smart Grid Interoperability Panel - Cyber Security Working Group, NISTIR 7628, August 2010.
39. NIST, National Institute of Standards and Technology, Smart Grid Cyber Security Strategy and Requirements, The Smart Grid Interoperability Panel-Cyber Security Working Group, DRAFT NISTIR 7628, 2010–02.
40. Newaz G, Bigg D, Eiber R. Structural Composite Cores for Overhead Transmission Conductors, EPRI Report EM-5110, Research Project 2426–9. 1987-04.
41. Pai MK. Voltage stability conditions considering load characteristics. *IEEE Trans Power Syst* 1992; 7(1): 243–249.
42. Pavella M, Murthy PG. Transient stability of power systems: Theory and practice. New York: Wiley, 1994.
43. Pierce HE Jr, Colborn HW, Coleman DW, Marriage EA, Richard JC, Rindt LJ, Rubino LJ, Stagg GW, Traub TP, Vandergrift J, Winn CE, Young CC. Common format for exchange of solved load flow data. *IEEE Trans Power App Syst* 1973; PAS-92(6): 1916–1925.
44. Pratt R, et al. The smart grid: An estimation of the energy and CO2 benefits, Pacific Northwest National Laboratory, PNNL-19112. 2010-01.
45. Schewe PF. The grid: A journey through the heart of our electrified world. Washington, DC: Joseph Henry Press, 2007.
46. Schulz RP, Price WW. Classification and identification of power system emergencies. *IEEE Trans Power App Syst* 1984; PAS-103(12): 3471–3479.
47. Schulz RP, VanSlyck LS, Horowitz SH. Classification and identification of power system emergencies in *Proc IEEE PICA Conf* 1989; 49–55.

48. Siljak DD. Decentralized Control of Complex Systems. New York: Academic, 1990.
49. Taylor CW. Power system voltage stability. NewYork: McGraw-Hill, 1994.
50. Zaborszky J, Whang KW, Prasad KV. Monitoring, evaluation and control of power system emergencies in *Proc Systems Engineering Power Conf*, Davos, Switzerland, 1979, Eng. Found. Rep. CONF-790 904-P1.