Scanning the Issue

Special Issue on Energy Infrastructure Defense Systems

This special issue of the PROCEEDINGS OF THE IEEE is devoted to defense of energy infrastructure; papers present the state of the art on several key areas, including hardware, software, applications and algorithmic developments, 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, along with rapid/robust restoration. In-depth surveys of existing remedial action schemes, emergency control techniques, and rapid restoration along with tutorial-type papers are included.

Any complex dynamic infrastructure network typically has many layers and decision-making units and is vulnerable to various types of disturbances. Effective, intelligent, distributed control is required that would enable parts of the networks to remain operational and even automatically reconfigure in the event of local failures or threats of failure.

The events of 11 September 2001 focus new attention on security of infrastructure in the United States. Electricity, water, telephone, the Internet, and other physical and logistic networks are all subject to threat by aggressors and all have vulnerabilities that are difficult to absolutely defend. The report on the northeastern blackout of August 2003 by the U.S.–Canada Power System Outage Task Force 2003 places the focus directly on the infrastructure of electric power. This blackout was not instigated by terrorists, but it was caused by multiple failures of infrastructure elements in the transmission system.

Competition and deregulation have created multiple energy producers that share the same energy-distribution network, one that now lacks the carrying capacity or safety margin to support anticipated demand. Investments in maintenance, research, and development continue to decline in the North American electrical grid.

Both the importance and difficulty of protecting energy infrastructure against natural disasters and physical attacks have long been recognized. In 1990, the Office of Technology Assessment (OTA) of the U.S. Congress issued a detailed report, *Physical Vulnerability of the Electric System to Natural Disasters and Sabotage*, concluding: “Terrorists could emulate acts of sabotage in several other countries and destroy critical [power system] components, incapacitating large segments of a transmission network for months. Some of these components are vulnerable to saboteurs with explosives or just high-powered rifles.” The report also documented the potential cost of widespread outages, estimating them to be in the range of $1–$5/kWh of disrupted service, depending on the length of outage, the types of customers affected, and a variety of other factors.

This vulnerability has significantly increased in recent years, in part because the system is operating closer to its capacity and in part because terrorist attacks are no longer hypothetical. During the fifteen years since the OTA report, the situation has become even more complex. Accounting for all critical assets includes thousand of transformer, line reactors, series capacitors, and transmission lines. Protection of *all* the widely diverse and dispersed assets is impractical because there are so many assets involved, including:

- over 230 000 miles of high-voltage (HV) lines (230 kV and above);
- over 6644 transformers in the Eastern Interconnection; over 6,000 HV transformers in the North American Interconnection;
- interdependence with gas pipelines, compressor stations, dams, rail lines, and telecommunication equipment (monitoring and control of the system).

It is important to note that all threats to security either travel through the power network itself or via the communication and information systems, including:

- natural disasters (such as storms, earthquakes, forest fires, and grassland fires), or conventional attacks, including truck bombs, small airplanes, gunshots;
- hijacking of control;
- biological contamination (real or threat);
- overreaction to isolated incidents or threats;
- cyber/Internet attacks (over 30,000 hits a day at an independent system operator’s Web site);
- more sophisticated modes of attack, including, for example, “suitcase”-sized electromagnetic pulse (EMP) weapons.

Additional factors that place increased stress on the energy infrastructure include dependencies on adjacent power grids (increasing because of deregulation), telecommunications, markets, and computer networks. Furthermore, reliable electric service is critically dependent on the whole grids ability

Digital Object Identifier 10.1109/JPROC.2005.847256

to respond to changed conditions instantaneously. As is true of other critical infrastructures, increased use of electronic automation raises significant issues regarding the adequacy of operational security: 1) reduced personnel at remote sites makes them more vulnerable to hostile threats; 2) interconnection of automation and control systems with public data networks makes them accessible to individuals and organizations, from any worldwide location using an inexpensive computer and a modem; 3) use of networked electronic systems for metering, scheduling, trading, or e-commerce imposes numerous financial risks implied by use of this technology.

In this special issue, we provide nonsensitive overviews of key areas and present selected security aspects of operational systems, without discussing potentially harmful or sensitive material. We begin with an overview in the first paper, "Scanning the Technology: Energy Infrastructure Defense Systems," which provides the context in which we manage and operate the system while focusing on the lessons learned as well as challenges associated with accomplishing security, quality, and reliability missions, including recent hardware, software, applications, and algorithmic developments.

We provide an overview of a continental-scale infrastructure, a multiscale, multilevel hybrid system. In "Wide-Area Protection and Emergency Control," coauthored by Working Group C-4 of the Power System Relaying Committee of the IEEE Power Engineering Society, Begovic *et al.* show that for deployment of a well-coordinated overall defense plan, it is necessary to implement and coordinate various schemes and actions, spanning different periods. The varying nature and types of extreme disturbances coupled with their anticipated infrequent occurrences make it desirable to take automated actions to stabilize the system, which may include system separation in a controlled and coordinated manner. Inadequacy of a well-coordinated overall defense plan hinders localization of the disturbance.

With advances in satellites, communications, and computer technologies, several utilities have installed or are in the process of installing phasor measurement units (PMUs). These devices are also known by other names, such as digital frequency recorders (DFRs) and dynamic swing recorders (DSRs). Some older units do not have global positioning system (GPS) clocks and therefore their data is not synchronized with other monitors. PMUs have been installed at the American Electric Power (AEP) service area, in the Western Electricity Coordinating Council (WECC) under the WAMS project, and in the New York area; in New England, Independent System Operator–New England (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, which has not been the case in the past. 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 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 state transition—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.

In "WACS—Wide-Area Stability and Voltage Control System: R&D and Initial Online Implementation," the authors present a state-of-the art approach by the Bonneville Power Administration (BPA) and Washington State University, who are designing and implementing a wide-area stability and voltage control system termed WACS. WACS provides a flexible platform for rapid implementation of generator tripping and reactive power compensation switching for transient stability and voltage support of the large power system. Features include synchronized positive sequence phasor measurements, digital fiber optic communications from many 500-kV substations, an embedded real-time system controller, and output communications for generator tripping and 500-kV capacitor/reactor bank switching. WACS includes both fast and slow subsystems. The fast proportional control subsystem for transient stability operates in a time frame of hundreds of milliseconds based on voltage measurements from many substations, and the slow subsystem operates in a time frame of a few seconds based on many voltage and generator plant reactive power measurements that are combined using fuzzy logic.

As background, widely used BPA and WECC emergency controls termed remedial action schemes (RAS) are presented. RAS is based on *direct detection* of predefined outages, with high-speed binary (transfer trip) signals to control centers for logic decisions, and then to power plants and substations for generator tripping and capacitor/reactor bank switching. Disadvantages of RAS include control only for predefined events and very high cost (tens of millions of dollars, hundreds of line-loss logic units and communications circuits).

In contrast with RAS, WACS employs strategically placed sensors to react to the power system *response* to disturbances. WACS is a networked control system that can act as either feedback control or single-action feedforward control. As feedback control, the need for discrete action is determined and commanded, the power system response is observed, and further discrete action such as generator tripping or capacitor bank switching is taken if necessary. The WACS platform may also be used for wide-area continuous modulation control of generators and transmission-level power electronic devices.

Another key thrust is designing a power system to have an adequate level of service from the point of view of reliability and security, a complex task considering the definition of adequate service by itself and the multiple risks and situations that could occur.

"Designing a Reliable Power System: Hydro-Québec's Integrated Approach" describes efforts underway at the Hydro-Québec power system, which is one of the most extensive and complex systems in North America. Its main infrastructure is made up of more than 11 000 km of 735-kV lines, and relies largely on dynamic shunt compensation (SVC), series compensation, and on a set of RAS to maximize its reliability and security. Operated in parallel with the ac system, a ±450-kV multiterminal direct current line can also be used to interconnect Hydro-Québec's system with its neighbor, in addition to other dc back-to-back converters.

This paper describes the results of evolution and experience gained by Hydro-Québec during the last 30 years in the design and operation of a large and complex power system, comprising many transmission technologies interacting with each other.

In "Strategic Power Infrastructure Defense," Li *et al.* provide a discussion of the fundamental theoretical techniques for the development of power infrastructure defense systems, including:

- the state of the art of multiagent systems;
- cooperative and self-serving agents;
- power infrastructure defense system techniques, e.g., load shedding, reconfiguration;
- system optimization, adaptation/learning methods, e.g., vulnerability, costs;
- information and communication systems support;
- future research and development opportunities.

In addition, this paper gives an overview of the vulnerabilities of power networks and articulates a vision for integrated sensing, communications, and control of the power grid. The authors provide a description of the system architecture and mechanisms for control of large networks; some of the pertinent issues are why/how to develop controllers for centralized versus decentralized (via a hybrid multiagent model), and issues involving adaptive operation and robustness to disturbances that include various types of failures. An open issue is: what is the tradeoff between efficiency and robustness?

In the next paper, entitled "A Fast Algorithm for Identification and Tracing of Voltage and Oscillatory Stability Margin Boundaries," Zhou and Ajjarapu discuss the pertinent area of voltage collapse and oscillatory instability that are inherently nonlinear phenomena related to bifurcation. Substantial research has been conducted to help understand and analyze the mechanism of these types of instability based on bifurcation theory. This paper presents a framework using a differential manifold approach that combines identification and tracing of both saddle node and Hopf bifurcation margin boundaries without calculating any eigenvalues. For a given base case, they first identify either saddle node or Hopf bifurcation. Then, for any given control change scenario, they further trace the change in saddle node or Hopf bifurcation margins. The manifold-based methodologies presented in this paper facilitate the development of fast margin monitoring and control algorithms.

Next, in the paper "Use of Satellite Technologies for Power System Measurements, Command, and Control," Holbert *et al.* analyze the use of wide-area measurement technologies including satellite-based methods for the command and control of power systems. The methods studied include the GPS and low earth orbit satellites (LEOS). As indicated earlier, the deregulation of the electric power industry is placing increased demands on power transmission system utilization; thus, increased loading of transmission facilities is an impetus for accurate dynamic thermal overhead electrical conductor ratings. The accuracy of dynamic thermal ratings is critically dependent on the measurement accuracy of the input variables to the particular prediction model. To appreciate the potential of wide-area measurements coupled with rapid communications, consider a stressed electric power network suffering from interarea oscillations. These oscillations result in large portions of the system separating from the rest of the system following disturbances. Controls based on local signals are the primary means of mitigating these oscillations because of the large geographical size and the reliability of local measurements. However, local controllers are tuned in a suboptimal fashion to damp both interarea and local plant modes. An alternative technique to provide effective damping of the interarea mode is desirable. Analysis of the interarea phenomenon has shown that certain signals measured at electrical centers of the group of generators separating from the rest of the system provide more effective control.

As an example, these signals could be measured by a GPS-based, wide-area measurement system and then transmitted using low earth orbit satellites to an optimally located FACTS controller to effectively damp the oscillations. In this paper, a supervisory-level power system stabilizer (SPSS) using wide-area measurement is suggested. The robustness of the proposed controller is capable of compensating for the nonlinear dynamic operation of power systems and uncertain disturbances. The coordination of the robust SPSSs and local PSSs is implemented based on the principles of multiagent system theory. The basic concept of wide-area control for power system stabilization is that *multiarea measurements* are used to damp *interarea oscillations*. The performance of the robust controller as an intelligent power system stability agent is studied using a 29-machine, 179-bus power system example. Simulation results show that a multiagent control structure can effectively damp system oscillations under a wide range of operating conditions. With a *local agent* working in the SPSS, a multiagent system may be designed to adapt to the partial failure of local controllers to maintain satisfactory system performance. The combination of agent technology and satellite capability is suggested for advanced power system command and control.

Today's grid relies far too heavily on narrowly programmed protection devices that have contributed to worsening the severity and impact of power outages. These devices, which came into play during last year's blackout, typically perform with simple "ON/OFF" logic, which acts locally while destabilizing a larger regional interconnection.

A key reason indicated by NERC is the detrimental role played by the protection systems during large disturbances, which tend to worsen the perturbations and propagate through overtripping of unfaulted system components due to hidden failures.

With its millions of relays, controls, and other components, the parameter settings and structures of the protection devices and controllers in the electricity infrastructure can be a crucial issue. It is analogous to the poem "for want of a nail… the kingdom was lost." That is, relying on an "inexpensive 25-cent chip" and narrow control logic to operate and protect a multibillion dollar machine is folly when so much is at stake. While seemingly expensive, redundancies and the ability to detour needed power around problems are absolutely essential to the modern grid.

In "Catastrophic Failures in Power Systems: Causes, Analyses, and Countermeasures," De La Ree *et al.* indicate that the present practice in power transmission planning and online security analysis often neglects the impact of the protection systems. In addition, the aim is to mitigate the vulnerability of the system to the loss of a single piece of equipment only by carrying out an N-1 security analysis. Consequently, the risk of cascading failures leading to blackouts and brownouts is neither assessed nor managed. Hidden failures in protection systems have been identified as key contributors in the cascading of power system wide-area disturbances. This paper describes a methodology to evaluate the effects of hidden failures based upon regions of vulnerability and areas of consequence in protection systems. The mechanisms of the hidden failures as well as the development of the regions of vulnerability from the hidden failures are shown. A number of the regions of vulnerability in a sample 179 test system are represented as physical areas. Two scenarios evaluate the consequences of the unwanted disconnections of the transmission lines caused by hidden failures. The development of an index of severity, which combines the magnitude of the regions of vulnerability and the consequences of unwanted disconnections caused by hidden failures, is needed. This index would identify the critical protection systems, whose unwanted operations would result in a significant loss of the power system integrity and/or a large cascading event.

The authors describe methodologies together with algorithms that assess the risk of catastrophic failures in electric power networks. A catastrophic failure is defined as the one that results in the outage of a sizable amount of load. It may be caused by dynamic instabilities in the system or the exhaustion of the reserves in transmission due to a sequence of line trippings leading to voltage collapse. Only the latter case is being considered. The aim of these algorithms is to identify the weak links of the system, which are defined as those branches of the network whose tripping due to a fault lead to a catastrophic failure with the highest probabilities. The paper also explores various ways to consolidate these weak links and thereby decrease the risk of catastrophic failures. These include the development of a hidden failure monitoring and control system that supervises adaptive digital relays located in sensitive spots across the system. These relays will perform dynamic load shedding during an emergency state in conjunction with an adaptive splitting of the system that prevents the cascading failures from spreading throughout the network.

In "Designing the Next Generation Real-Time Control, Communications and Computation for Large Power Systems," Tomsovic *et al.* address the issues involved in the overlaid communication and control system that enables economic and secure operation of power infrastructure. This multilayered infrastructure has evolved over several decades. The monitoring of the grid is still done by a hierarchical design with polling for data at scanning rates in seconds that reflects the conceptual design of the 1960s. This design was appropriate for vertically integrated utilities with limited feedback and wide-area controls; however, the thesis of this paper is that the changing environment, in both policy and technology, requires a new look at the operation of the power grid and a complete redesign of the control, communication and computation infrastructure. Several examples of novel control and communication regimes for such a new infrastructure are presented.

In the next paper, "Design Aspects for Wide-Area Protection Systems," Zima *et al.* introduce a sophisticated wide-area platform for wide-area monitoring, protection, emergency control and optimization purposes. These features impose strict constraints (design considerations) on development of such a system. The hardware includes:

- PMUs;
- communication links;
- central unit—PC and software;
- data preprocessing package;
- basic services;
- specific individual applications;
- GUI;
- packages containing model/data of the supervised power system and for coordination with other software packages.

In "Wide-Area Protection and Power System Utilization," Bertsch *et al.* describe basic principles and philosophy for wide-area protection schemes, also called RAS or system protection schemes (SPS), as a means to improve the capability of existing electric power systems and transmission corridors. In the areas of power system automation and substation automation, there are two parallel trends that lead to different directions: centralization and decentralization. More functions are being moved from local and regional control centers toward the central or national control center. At the same time, more "intelligence" and "decision authority" is moving closer to the actual power system. In addition, there is more functional integration within the same hardware, which raises discussions concerning reliability and security. The main purpose of this paper is to sort out the terminology used in this area, describe pertinent application areas and related requirements, illustrate different design principles— "top-down," "bottom-up," hierarchy, flat, etc., for different applications—and discuss suitable levels of complexity, capability, capacity, and flexibility.

In "Area-wide System Protection Scheme Against Extreme Contingencies," Lachs describes the steps that were taken in the creation of the planning resources; a plan that attempts to be intrinsically simple, reliable, of modest cost, and able to be practically implemented. The underlying objective is to devise timely automatic responses to extreme contingencies that can sustain the integrity of the interconnected grid. The author provides a tutorial on the current approaches and insights into the severe contingencies and emergency strategies. Future introduction of numerous energy storage devices within power systems, often within distribution networks, will open the door to self-healing arrangements. This opportunity will be created as the strategies for responding to extreme contingencies can be effective in directing actions of inverters associated with each energy storage device.

Next, in "Overcoming Communications Challenges in Software for Monitoring and Controlling Power Systems," Birman *et al.* begin with the premise that the evolution of electric power systems is predicated on the extensive use of computer-mediated control for such purposes as monitoring the overall state of the grid, protection, setting power pricing, planning production levels, and implementing producer–consumer load-following contracts. There is a widespread presumption that this will entail deployment of a dedicated but Internet-based infrastructure. However, such an approach overlooks the limitations associated with the current Internet. Moreover, while the Internet is often described as if it is routed around congestion instantly, in practice there can be delays of many minutes between when an overload occurs and when routing adapts. For such reasons, the Internet infrastructure could be said to be intrinsically ill-matched to the needs of critical applications having extreme reliability and real-time needs. The problem is further complicated if we consider higher level software operating on an end-to-end basis. While there are many off-the-shelf products that could be used in the future electric power control network, existing products scale poorly and are fragile. There are very few large-scale success stories involving complex real-time control and monitoring applications, and the ones to which one could point normally operate in isolated environments, are carefully configured through a costly manual process, and have fairly low data rates.

Thus, the authors consider a new communications technology offering scalability, predictable real-time properties, and robustness to the sorts of disruptions common in large communications networks, such as congestion and link or router failure. They propose that Astrolabe, developed as a response to military monitoring and control requirements, for large-scale monitoring and systems management, could respond to this need. Astrolabe runs over either TCP or UDP, but routes information around congestion or failure, without waiting for Internet routing protocols to sense and react to problems. The authors compare the needs of emerging electric power systems control and protection algorithms with the communication properties available from the Internet or from the kinds of off-the-shelf software used today in the most demanding settings, such as stock markets and air traffic control systems.

The paper by Shahidehpour and Wiedman, "Natural Gas Infrastructure Protection for Supplying the Electric Power Plants," focuses on the interdependencies with markets and gas pipelines. The restructuring of electricity has introduced new risks associated with the security of the natural gas infrastructure on a significantly large scale, which entails changes in physical capabilities of pipelines, operational procedures, sensors and communications, contracting (supply and transportation), and tariffs. The authors discuss the essence of protecting the natural gas infrastructure for supplying the ever-increasing number of gas-powered units and its impact on the reliability of the electric power systems infrastructure.

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

I hope that this Special Issue will be of interest to many in various fields of electrical engineering, including power systems and electronics, infrastructure security, systems science, and controls who have a particular interest in sensing, modeling, and control of complex infrastructures, electric power systems, energy markets, and other interactive infrastructures. I express my gratitude to all authors, the referees, members of the editorial office, managing editor, and the editor-in-chief of the PROCEEDINGS OF THE IEEE for their contributions and continued interest in this special issue. I gratefully acknowledge feedback and support from numerous colleagues at the Electric Power Research Institute (EPRI), universities, industry, and government agencies who served as reviewers for this special issue and have provided their tireless efforts and leadership.

MASSOUD AMIN, *Guest Editor*
Center for the Development
of Technological Leadership
University of Minnesota
Minneapolis, MN 55454 USA

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

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

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