guest editorial

Manimaran Govindarasu and Peter W. Sauer

smart grid & security

protecting the cyberphysical systems

THERE IS A MAJOR GROWTH IN electrical and computer engineering research focused squarely on what has become known as the smart grid. While formal definitions of the smart grid do exist, the concept has grown to include technologies that span virtually all areas of electrical and computer engineering impacting energy sustainability, consumer response, electrification of transportation, and related areas. This is primarily due to the strong dependence on communication, control, and computing capabilities that support new growth in electric power and energy resources and technologies. The emergence of cyberphysical systems broadly captures the essence of this interdependence and has provided a rich theoretical basis for characterizing the challenges associated with maintaining critical assets while optimizing performance. Unfortunately while modern communication, control, and computing technologies offer tremendous opportunities to improve electric power system response and resilience to failure, they also render the grid vulnerable to intentional attacks from internal or external parties. The need for secure networks includes the expansive information technology (IT) infrastructure that is at the heart of power system operation and protection. With the emergence of the advanced metering infrastructure (AMI), issues of customer privacy and demand response are also key topics associated with the smart grid. This special issue includes invited articles that address the basic communication needs and cybersecurity issues

Digital Object Identifier 10.1109/MPE.2011.943142
Date of publication: 13 December 2011

associated with smart grid technologies.

Daniel Nordell of Xcel Energy gives a view of the many aspects of security and reliability in a complex large-scale electric power system.

Faycal Bouhafs, Michael Mackay, and Madjid Merabti in the United Kingdom discuss the challenges that the variety of smart grid components present for applications that go deep into the consumer environment and involve the customers in operating decisions.

Massoud Amin and Tony Giacomoni of Minnesota present opportunities and challenges for the security of operations including both resilience and privacy.

Julie Hull, Himanshu Khurana, Tom Markham, and Kevin Staggs of Honeywell in Minnesota address specific cybersecurity issues with the modern electric grid. Beginning with the diversity of communication infrastructures and the history of SCADA systems, the article includes a discussion on minimizing cyberattacks as well as detecting and responding to attacks that do occur. It includes information on how to design a secure system and what is being done today (best practices).

David Anderson, Chuanlin Zhao, Carl Hauser, Vaithianathan Venkatasubramanian, Dave Bakken, and Anjan Bose of Washington State University present a simulator (GridSim) that is described as being able to simulate in real time the electromechanical dynamic behavior of the power grid together with the Information Technology infrastructure that overlays the grid and the control systems. The purpose of the simulator is to design and test new wide-area control and protection schemes.

Chen-Ching Liu (now with Washington State University), Alexandru Stefanov, and Junho Hong (of University College Dublin) together with Patrick Panciatici of RTE France describe a SCADA testbed at UC Dublin for studying cybervulnerabilities and mitigation strategies.

Rakesh Bobba, Jeff Dagle, Erich Heine, Himanshu Khurana (now with Honeywell), William Sanders, Pete Sauer and Tim Yardley of the University of Illinois focus on the challenges of Wide Area Measurement Systems, NASPINet, and Security.

Collectively, these contributions establish the technical need for secure communications and present the challenges for cybersecurity in the rapidly emerging smart grid. The concepts and ideas provide a foundation for future research and development in the equipment and software components that will enable the future grid. Work in this area requires strong collaboration between expertise in communications, computing, control, and electric power systems.

Acknowledgments

The guest editors thank the editor-in-chief of *IEEE Power & Energy Magazine*, Mel Olken, for coordinating the preparation and publication of this special section.