Guest Editorial
Special Section on Cyber-Physical Systems and Security for Smart Grid

CYBER-PHYSICAL system (CPS) is an integration of computation, communication, and control that is embedded in the physical process. CPS has led to the emergence of a new generation of engineering systems. Although there are many important CPS systems in practice, one of its most complex domains is the smart grid whose function is to distribute reliable and efficient electric energy with a high degree of sustainability. While the smart grid aims to enhance the capabilities and response of the generation, transmission, distribution, and use of energy systems, the cyber challenge lies in the realization of the power grid to control and monitor physical behavior securely and efficiently. These research challenges, along with effective design architectures, will continue to confront the research community over the next several years.

This special section contains several important papers that address some of the critical challenges described above. While acknowledging its limited coverage, the section offers a range of interesting smart grid contributions such as wide-area monitoring systems and control, communication and networking, demand and response, and security and privacy. Let us begin our excursion with these contributions.

The first part of the section consists of several papers that are concerned with privacy and cybersecurity. The first paper "Evaluation of the Precision-Privacy Tradeoff of Data Perturbation for Smart Metering" by Mraco Savi, Cristina Rottondi, and Giacomo Verticale investigates the role of data perturbation and data aggregation in the definition of a privacy-friendly smart grid architecture. This paper formalizes a privacy attack and analyzes the tradeoff between the aggregation set size, the precision of time-series energy consumption measurements, and the privacy level. The authors also show how data perturbation can be consistently improved under the assumption of time-correlation of energy consumption measurements.

In the case of demand response, a tradeoff exists between the costs and the degree of privacy. This tradeoff is studied in this paper authored by Jiyun Yao and Parv Venkitasubramaniam, entitled "The Privacy Analysis of Battery Control Mechanisms in Demand Response: Revealing State Approach and Rate Distortion Bounds." In this paper, the authors address privacy protection challenges in the CPS of smart grid from the consumers' perspective. In particular, this paper is concerned with a class of battery charging policies to derive achievable privacy-cost savings tradeoffs using a Markov process model for user demand and instantaneous electricity prices. The next paper in the privacy category "Preventing Occupancy Detection From Smart Meters" by Dong Chen, Sandeep Kalra, David Irwin, Prashant Shenoy, and Jeanie Albrecht, deals with privacy concerns with respect to smart meters as a potential barrier to the advancement of smart grids. In their contribution, the authors present a new approach called combined heat and privacy that modulates the thermal energy storage in electric water heaters to mask occupancy detection.

Smart meters are also serving as the crucial interfaces through which the cyber, physical, and social domains of smart grid can interact with each other, thus facing varieties of threats. The next paper "A Collaborative Intrusion Detection Mechanism against False Data Injection in Advanced Metering Infrastructure" by Xiaoxue Liu, Peidong Zhu, Yan Zhang, and Kan Che proposes a collaborative intrusion detection mechanism against false data injection attack. The authors present a new concept of "spying domain" to protect data in smart meters, which is based on a collaborative intrusion detection mechanism against false data injection attack. The impact of specific cyberattack on the power system is also studied in this paper "Cyber-Physical Simulation for Analyzing Impact of Cyber Events on the Power Grid" by Ren Liu, Ceeman Vellaithurai, Saugata Biswas, Thoshitha Gamage, and Anurag Srivastava. In this contribution, the authors develop a reconfigurable cyber-physical testbed for real-time end-to-end system simulation to assess the impact of three possible cyberattacks.

The transition from traditional power systems, which would require integration of cyber communications and control systems into smart grid infrastructures, can have a profound impact on the operation, reliability, and efficiency of the grid. To constitute secure data acquisition and prevent false data injection attacks is investigated in this paper "Empirical Development of a Trusted Sensing Base for Power System Infrastructures" by Ali Mazloomzadeh, Osama Mohammed, and Saman Zonouz. In this paper, the authors approach is based on encrypting analog ac signals at data acquisition points, which is normally done at phasor measurement units (PMUs) after the measurements are sampled and digitalized at the A-to-D devices. Through pushing the encryption to within the sensors, the proposed framework reduces the size of trusted computing bases for the entire smart grid infrastructure and hence increase its trustworthiness. Bear in mind that

Date of current version August 19, 2015.
Digital Object Identifier 10.1109/TSG.2015.2464911

trustworthy operation requires comprehensive cyber-physical security assessment of potential threats, including cyber-induced and cyber-enabled disruptions of physical components. In the next paper by Katherine R. Davis *et al.* titled "A Cyber-Physical Modeling and Assessment Framework for Power Grid Infrastructures," the authors propose an online framework to assess the operational reliability impacts during threats to the grids cyber infrastructure. In particular, they leverage the analysis outcomes to enhance power system contingency rankings through consideration of cyber-side vulnerabilities. They believe this framework to be an important step toward understanding and analyzing complex cyber-physical systems.

The last paper in the cybersecurity "Detecting False Data Injection Attacks in AC State Estimation" by Chaojun Gu and Mehul Motani deals with detecting false data injection attacks on power system state estimation. It should be pointed out that in state estimation methods, such as weighted least square state estimation, false data injection attacks can impact the bad data detection process. The authors of this paper propose a method to combat false data injection attacks by tracking the dynamics of measurement variations. Their method is based on Kullback–Leibler distance, which calculates the distance between two probability distributions derived from measurement variations.

As microgrids are becoming a key component in the evolution of the power grid, this special section offers two papers addressing some of the microgrid challenges. The first paper "A Secure Communication Architecture for Distributed Microgrid Control" by Velin Kounev, David Tipper, Attila Yavuz, Brandon M. Grainger, and Gregory F. Reed sets out an architecture for securing communications between the distributed control elements of a microgrid. This includes a first of its kind security model and protocols to meet the real-time communication needs of microgrids. In addition, this paper discusses the implementation and performance of the proposed security scheme and its advantages. The use of a wireless communication network is investigated in the next paper entitled "Multi-Terminal Hybrid Protection of Microgrids Over Wireless Communications" by Taha Selim Ustun and Reduan H. Khan, which proposes a hybrid protection system for microgrids. The authors use both adaptive and differential protection at different parts of the microgrid in order to create protection zones. They conclude that zone creation with smart decision making helps to cultivate microgrids operational performance.

As distributed generators are being widely deployed in today's power grid, diversifying the generation mix in today's power grid will result in significant long-term benefits such as sustainable and economical use of available natural resources and increased energy security. Nonetheless, due to the inherent generation variability of renewable generators, their widespread integration has not yet become a reality. This is the main theme of the first paper titled "Distributed Optimization of Dispatch in Sustainable Generation Systems via Dual Decomposition" by Pirathayini Srikantha and Deepa Kundur. The authors propose a distributed scheme that offloads power dispatch decisions to participating generation systems which react to local conditions with the help of lightweight communication signals sent by the utility. This strategy can enhance security and privacy while enabling the seamless plug-and-play integration of heterogeneous generation systems. The second paper in this category "Goal-Based Holonic Multi-Agent System for Operation of Power Distribution Systems" is authored by Anil Pahwa *et al.* It is mainly concerned with large-scale integration of rooftop solar photovoltaic (PV) generation at the home level. The authors propose a goal-based holonic multiagent system for control of reactive power at PV installations in individual homes for optimal operation of the system, as well as for state estimation of system leveraging different measurements available from smart meters at homes.

Another important issue, which has been touched upon in this special section, is the wide-area monitoring and control of power grid systems, especially in conjunction with the increasing need for deployment of phasor measurement unit (PMU). The first paper in this category "A PMU Scheduling Scheme for Transmission of Synchrophasor Data in Electric Power Systems" by Kyatsandra Nagananda, Shalinee Kishore, and Rick S. Blum. This paper is mainly concerned with PMU scheduling for efficient transmission of phasor data on the grid. The proposed scheme is claimed to be fully governed by the measure of electrical connectedness between buses in the grid and is independent of the PMU placement problem. The authors demonstrate the performance benefits by coupling the scheduling policy with a fault detection algorithm, which is used to detect changes in the susceptance parameters in the grid. The next paper "Distributed Optimization Algorithms for Wide-Area Oscillation Monitoring in Power Systems Using Inter-Regional PMU-phasor data concentrator (PDC) Architectures" by Seyedbehzad Nabavi, Jianhua Zhang, and Aranya Chakrabortty proposes three distributed cyber-physical architectures by which different utilities jointly estimate power system oscillation modes using synchrophasor data through a wide-area communication network. In their investigations, the authors consider both synchronous and asynchronous communications, and provide recommendations on interphasor data collector communication protocols to improve the numerical stability of their proposed algorithms. Synchrophasor measurement and communication for distribution generation grid is the topic of the next paper entitled "Scalable Synchrophasors Communication Network Design and Implementation for Real-time Distributed Generation Grid." The authors, Hamid Gharavi and Bin Hu, presented the design and implementation of a hierarchical synchrophasor network testbed based on an emulation platform. In addition, they propose an efficient method to reduce bandwidth, as well as provide capabilities for control at each hierarchical level. For radial and loop feeders, they also present a tree-based wireless multihop routing algorithm.

The cyber-physical infrastructure underlying the modern power grid would require developing a measurement-based disturbance localization algorithm for large-scale power systems. In this paper, "A Real-Time Attack Localization Algorithm for Large Power System Networks

Using Graph-Theoretic Techniques" by Thomas. R. Nudell, Seyedbehzad Nabavi, and Aranya Chakrabortty, an algorithm that utilizes advanced concepts from graph theory to localize disturbances was proposed. Their proposed algorithm is capable of capturing the most up-to-date wide-area network configuration without relying on a static model of the network as used in most conventional monitoring systems.

The next paper by Kara Emre, Mario Berges, and Gabriela Hug-Glanzmann titled "Impact of Disturbances on Modeling of Thermostatically Controlled Loads for Demand Response" investigates one of the most important challenges in cyber-physical systems, which is keeping the physical process under control through accurately modeling the system dynamics. In particular, the authors focus on modeling the dynamics of thermostatically controlled load (TCL) populations in order to engage them as demand response providers to the smart grid. This paper presents a mathematical model that captures the end-user's interactions with individual TCLs and disturbances to their operation. The model creates no additional computational burden within a state-of-the-art linear-time-invariant technique.

The final paper in our collection is authored by Jiang-Hong Liu and Chia-Chi Chu. It is titled "Iterative Distributed Algorithms for Real-Time Available Transfer Capability Assessment of Multi-Area Power Systems." This paper describes a computational framework for energy management systems in modern smart grids. Specifically, the available transfer capability calculations are formulated as a nonlinear optimal power flow problem by studying iterative decomposition-coordination approaches based on constrained augmented Lagrangian methods.

Acknowledgment

The Guest Editors would like to thank all the invited authors for their valuable contributions, as well as the reviewers for their time and effort in providing valuable feedback to the authors. They would also like to thank the IEEE Transactions on Smart Grid, especially Dr. M. Shahidehpour, Editor-in-Chief at the time approved the inclusion of this special section with the current Editor-in-Chief, Dr. J. Wang.

Hamid Gharavi, *Guest Editor*
National Institute of Standards and Technology
Gaithersburg, MD, USA

Hsiao-Hwa Chen, *Guest Editor*
National Cheng Kung University
Tainan, Taiwan

Christian Wietfeld, *Guest Editor*
TU Dortmund University
Dortmund, Germany

Hamid Gharavi (M'79–SM'90–F'92–LF'13) received the Ph.D. degree in electrical engineering from Loughborough University, Loughborough, U.K., in 1980.

He joined the Department of Visual Communication Research, AT&T Bell Laboratories, Holmdel, NJ, USA, in 1982. He was then transferred to Bell Communications Research (Bellcore) after the AT&T-Bell divestiture, where he became a Consultant of Video Technology and a Distinguished Member of Research Staff. In 1993, he joined Loughborough University, as a Professor and the Chair of Communication Engineering. Since 1998, he has been with the National Institute of Standards and Technology, U.S. Department of Commerce, Gaithersburg, MD, USA. His current research interests include smart grid, wireless multimedia, mobile communications and wireless systems, mobile *ad hoc* networks, and visual communications. He holds eight U.S. patents and has over 100 publications related to the above topics.

Mr. Gharavi was a recipient of the Charles Babbage Premium Award from the Institute of Electronics and Radio Engineering in 1986 and the IEEE CAS Society Darlington Best Paper Award in 1989. He served as a Distinguished Lecturer of the IEEE Communication Society. He was a Guest Editor for a number of special issues, including the Proceedings of the IEEE Special Issue on Smart Grid: The Electric Energy System of the Future in 2011, Sensor Networks and Applications in 2003, and Wireless Multimedia Communications in 1999. He was the Technical Program Committee Co-Chair for IEEE SmartGridComm in 2010 and 2012. From 2010 to 2013, he served as the Editor-in-Chief for the IEEE Transactions on Circuits and Systems for Video Technology. He is currently the Editor-in-Chief of IEEE Wireless Communications and an Editorial Board Member of IEEE Access. He served as an Editorial Board Member of the Proceedings of the IEEE from 2003 to 2008. He was a Core Member of Study Group XV (Specialist Group on Coding for Visual Telephony) of the International Communications Standardization Body CCITT (ITU-T).

Hsiao-Hwa Chen (S'89–M'91–SM'00–F'10) received the B.Sc. and M.Sc. degrees in electrical engineering from Zhejiang University, Hangzhou, China, in 1982 and 1985, respectively, and the Ph.D. degree in electrical engineering from the University of Oulu, Oulu, Finland, in 1991.

He is currently a Distinguished Professor with the Department of Engineering Science, National Cheng Kung University, Tainan, Taiwan. He has authored or co-authored over 400 technical papers in major international journals and conferences, six books, and over ten book chapters in the area of communications.

Dr. Chen was a recipient of the Best Paper Award from the IEEE Wireless Communications and Networking Conference 2008 and the IEEE Radio Communications Committee Outstanding Service Award in 2008. He served as the General Chair, the Technical Program Committee Chair, and the Symposium Chair for several international conferences. He served or is serving as an Editor or/and a Guest Editor for numerous technical journals. He is the Founding Editor-in-Chief of the *Security and Communication Networks Journal*. He is currently the Editor-in-Chief for IEEE WIRELESS COMMUNICATIONS. He is a Fellow of the Institute of Engineering and Technology and an Elected Member at Large of the IEEE Computer Society.

Christian Wietfeld (M'05–SM'12) received the Dipl.-Ing. and Dr.-Ing. degrees in electrical engineering from Rheinisch-Westfälische Technische Hochschule (RWTH) Aachen University, Aachen, Germany, in 1992 and 1997, respectively.

He is currently a Full Professor and the Head of the Communication Networks Institute, Technical University of Dortmund, Dortmund, Germany. For over 20 years, he has initiated and contributed to national and international research projects on mobile and wireless data communication systems in academia such as RWTH Aachen and TU Dortmund, and industry such as Siemens, Munich, Germany. Since 2008, he has been actively contributing to the research on cyber-physical energy systems as part of various national and European research efforts (e.g., German E-Energy Program, DFG FOR 1511, and EU FP7 SmartC2Net). He has published over 165 peer-reviewed publications and patents.

Mr. Wietfeld was a recipient of the International Telecommunications Union-Telecommunication Standardization Sector Outstanding Contribution Award for his contributions to the standardization of next generation mobile network architectures. He is the Chair of IEEE's German sister organization, the Verband der Elektrotechnik, Elektronik, und Informationstechnik/Informationstechnische Gesellschaft Committee on Communication Networks and Systems, and has co-founded the IEEE GLOBECOM Workshop on Wireless Networking for Unmanned Autonomous Vehicles.