# Guest Editorial: Resilience in Energy Industries—Recent Advances, Open Challenges, and Future Directions

THE transformation of energy infrastructure is making the resilience a fundamental topic for the definition of future configuration of the energy systems. This is due to the increased penetration of renewable energy sources (RES), the distributed energy management, the change in the power demand, the integration between energy and mobility sectors, the progressive liberalization of energy markets, the increased probability of extreme weather events, and the occurrence of errors in the interaction between humans and machines.

Resilience is the capacity of critical infrastructure systems to proactively maintain a safe level of operational normalcy in response to anomalies, including threats of a malicious and unexpected nature. Threats to normal operation are those elements that destabilize control and communications system networks. These threats include human error and malicious human attacks, complex latencies, and interdependencies. For instance, control systems need to provide greater human in the loop recognition based upon the roles and responsibilities of the individual. This ensures that the human interaction provides the required and most accurate state awareness information for the unique requirements of an individual formulating a judgment. In addition, control system performance indices are not just physics based, but include event-based cyber security measures, as cyber exploitation can degrade systems and require some human response to mitigate. Ultimately, the control system architecture must engender a holistic design that includes all performance measures affecting the resilience of the infrastructure.

Once the resilience measures are defined based upon performance, both passive and active resilience enhancement measures can be proposed and tested. Passive measures include all those precautions implemented in the planning phase, aiming at reducing the overall failure probability of the system. These measures are often related to the identification of optimal topological configurations and in the preventive identification of critical features. These types of features include the analysis of the optimal topological features for the reduction of systemic risks, the definition of the optimal positioning of generation and loads, when applicable, and the improvement of the resilience of multilayered infrastructures (in which one or more of the considered layers is or are composed by a power system or its subsystems). On the other hand, the active resilience enhancement measures include all those actions and devices that allow the active management of the system during its operation. These systems include the definition of the optimal management schemes of RES, energy storage systems or backup systems, the implementation of measurement and/or control systems, and the implementation of islanding procedures.

Digital Object Identifier 10.1109/TII.2019.2918383

Also, it should be interesting to investigate passive approaches to improve the impact of active resilience enhancement measures. As an example, this can include an optimized placement of monitoring systems or the optimal placement of energy storage systems, which can be identified during the planning phase in order their ability to control the system, if and when needed.

Finally, the evaluation of the cost efficiency of the resilience enhancement measures should be propaedeutic to the efficient implementation of such measures. This step should estimate the costs associated to the proposed resilience enhancement measures, and evaluate their implementation on the base of a cost benefit analysis.

In this framework, this special section on "Resilience in Energy Industries—Recent Advances, Open Challenges, and Future Directions" of the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS addresses a number of relevant issues associated to resilience of energy critical infrastructure. Seven high-quality contributions to this special section have been selected for publication in a strict peer-review process. They concern different topics related to the improvement of resilience in energy infrastructure. They can be clustered in two main classes: active resilience enhancement measures and passive resilience enhancement measures. The first one considers solutions aimed to improve the resilience of power system by means of a hardware approach. This is based on the proper integration of energy storage systems or on the management of generation of RES in critical environmental condition or on the correct positioning of supporting energy resources in case of critical events. The passive resilience consists in software algorithm aimed to prevent cyber attacks associated both with the energy market and/or with the massive use of information and communication technologies in the power system. Considering this classification, the special session has been organized in order to report first the hardware-based actions involving the infrastructure, its devices, and its energy management. The goal is to report the proposed solutions for counteracting at the origin the hardware causes of unpredictable fatal fails on the power system. Subsequently, this special section presents two classes of solutions to make power system more resilient: the ones dealing with cyber attacks exploring vulnerabilities of the Internet of Things technologies, and the ones helping to neutralize negative effects of the electricity market on the energy management in power systems.

## I. Active Resilience Proposed Actions

In order to increase the flexibility and, subsequently, the reliability and the resilience of power systems, Alharbi *et al.* investigate on the advantages related to the implementation of planning criteria for energy storage systems [item 1) in the Appendix]. The comparison between the installation of new energy storage systems and used electric vehicle battery, according to second life battery concept, has been developed, considering the proposed planning tool. Particularly, the planning process is aimed to determine the optimal decisions regarding the sizing, the operation, and the installation time, taking into account a new set of mathematical relations of battery energy storage system (BESS) degradation and optimal year of replacement. The proposed case of study highlights the advantages obtainable under different scenarios.

In this contest, the availability of electric vehicles able to manage energy in real time, when they are connected to charging stations, is fundamental. In fact, the expected exploitation of e-mobility represents an interesting opportunity for the implementation of demand management algorithm devoted to the reinforcement of future power system also in term of resilience. Therefore, the development of control algorithms aimed to optimize energy management of electric vehicles is strategic.

Regarding this topic, Liu *et al.* present an online energy management controller for plug-in hybrid electric vehicles, based on driving conditions recognition using genetic algorithms (GAs) [item 2) in the Appendix]. Through scenarios based on four types of driving conditions, GAs are applied offline for finding optimal controls. When put in production, the approach recognizes driving conditions online. Testing included simulations (where demonstrated that the approach being superior to charge-depleting/charge-sustaining technique), and hardware-in-the loop experiment to validate the strategy real time.

The unpredictable power perturbations and the fluctuations in power system associated to RES represent one of the main concerns in the transition toward the distributed energy models. Therefore, the actions aimed to minimize power perturbation generated by RES can be considered a viable solution to improve the power quality and hence a form of active action to improve resilience of RES-based power systems. In this contest, Seyedmahmoudian *et al.* developed a method called adaptive radial movement optimization (ARMO) to diminish the effect of the partial shading (PS) problem in the maximum power point tracking for photovoltaic systems with additional dynamic applications. The main advantages of ARMO are its improved tracking speed and a significant reduction in output fluctuations during the tracking period. Experimental comparisons to other computational intelligence approaches were made for different introductions of PS and varying load conditions. The methodology proved to be successful in rapidly achieving a stabilized output.

An original solution to improve the resilience of the power system during critical events, acting on the hardware configuration of the power system, has been proposed by Darani *et al.* in [item 3) in the Appendix]. They provide a unique perspective on optimized response to a disaster based upon automated mobile and autonomous energy sources formed into a temporary and adaptive microgrid. The author's approach includes a GA optimization in microgrid resource positioning, considering an operating field with obstacles. The approach is applied to a dc distribution system and provides several test cases to validate the concept of prepositioned robotic sources to address loss of power after a catastrophic event.

## II. Passive Resilience Proposed Actions

Regarding passive resilience actions on the power systems, Hong *et al.* propose a new concepts for detecting and mitigating cyber attacks on power systems resorting to cyber-physical security solutions [item 4) in the Appendix]. A specific coordination of protections aimed to change their settings referring to real-time power system analysis has been proposed to counteract cyber intrusions. The validation of the proposed attack mitigation functions has been performed on hardware-in-the-loop test bench, reproducing real-time power system and considering realistic intrusion scenarios.

Barreto and Càrdenas investigate the resilience of the electricity market infrastructure in case of implementation of demand response systems [item 5) in the Appendix]. In particular, they compare the centralized direct load control system, and decentralized dynamic prices system considering attack model aimed to defraud and damage the system. This paper proves that the decentralized systems are more resilient. However, decentralized dynamic prices system introduces critical issues in distinguishing attacks from system failures making difficult for the defender detecting the attacks. The authors propose the introduction of penalties for the users in order to discourage the attackers.

Zhang *et al.* presented multilayer data-driven cyber-attack detection for industrial control systems (ICSs) in paper [item 6) in the Appendix]. In this paper, the authors addressed cyber security of ICSs. The proposed approach based on the defense in depth is developed utilizing network traffic data, host system data, and measured process parameters. Importantly, real-time ICS testbed data were used for demonstrating the proposed detection system. Five types of attacks and four classical classification approaches were used as a secondary line of defense in event of intrusion prevention layer failing. Autoassociative kernel regression model was studied to strengthen early attack detection, showing that the approach detects physically impactful cyber attacks before significant consequences occur.

## Acknowledgment

The Guest Editors would like to express their deep gratitude to all the authors who have submitted their valuable contributions and to the numerous and highly qualified anonymous reviewers. They think that the selected contributions, which represent the current state-of-the-art in the field, will be of great interest to the industrial electronics community. They would like to thank Prof. K. Luo, Editor-in-Chief for the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS (TII), for giving them the opportunity to organize this special section and for all the encouragement, help, and support given throughout the process, and the TII staff for their professional support and assistance during the whole preparation of this special section.

A. DAMIANO, *Guest Editor*
Department of Electrical and Electronic Engineering
University of Cagliari
09123 Cagliari, Italy

C. RIEGER, *Guest Editor*
Idaho National Laboratory
Idaho Falls, ID 83415-3545 USA

V. VYATKIN, *Guest Editor*
Department of Computer Science, Electrical and Space Engineering
Luleå University of Technology
97187 Luleå, Sweden

M. MANIC, *Guest Editor*
Computer Science Department
Virginia Commonwealth University
Richmond, VA 23284 USA

## APPENDIX
## RELATED WORK

1) T. Alharbi, K. Bhattacharya, and M. Kazerani, "Planning and operation of isolated microgrids based on repurposed electric vehicle batteries," *IEEE Trans. Ind. Inform.,* vol. 15, no. 7, pp. 4319–4331, Jul. 2019.
2) T. Liu, H. Yu, H. Guo, Y. Qin, and Y. Zou, "Online energy management for multimode plug-in hybrid electric vehicles," *IEEE Trans. Ind. Inform.,* vol. 15, no. 7, pp. 4332–4341, Jul. 2019.
3) S. A. Darani, C. D. Majhor, W. W. Weaver, R. D. Robinett, III, and O. Abdelkhalik, "Optimal positioning of energy assets in autonomous robotic microgrids for power restoration," *IEEE Trans. Ind. Inform.,* vol. 15, no. 7, pp. 4342–4351, Jul. 2019.
4) J. Hong, R. F. Nuqui, A. Kondabathini, D. Ishchenko, and A. Martin, "Cyber attack resilient distance protection and circuit breaker control for digital substations," *IEEE Trans. Ind. Inform.,* vol. 15, no. 7, pp. 4352–4361, Jul. 2019.
5) C. Barreto and A. A. Càrdenas, "Impact of the market infrastructure on the security of smart grids," *IEEE Trans. Ind. Inform.,* vol. 15, no. 7, pp. 4362–4369, Jul. 2019.
6) F. Zhang, H. A. Dias Edirisinghe Kodituwakku, W. Hines, and J. Coble, "Multilayer data-driven cyber-attack detection system for industrial control systems based on network, system, and process data," *IEEE Trans. Ind. Inform.,* vol. 15, no. 7, pp. 4370–4380, Jul. 2019.

**Alfonso Damiano** (M'11) received the M.S. (*Laurea*) degree in electrical engineering from the University of Cagliari, Cagliari, Italy, in 1992.

In 1994, he joined the Department of Electrical and Electronic Engineering, University of Cagliari, as an Assistant Professor. Since 2018, he has been a Full Professor of Electrical Machines and Energy Management with the University of Cagliari. In 2012, during his involvement in the Italian strategic national research project on critical infrastructures Crisis Lab, he was a Visiting Professor with the Institute for Advanced Studies of Lucca, Lucca, Italy. Since 2014, he has been involved, as a Scientific Coordinator, in several international research projects regarding energy storage, smart grids, and e-mobility as European Project Horizon 2020 Netfficient, European Project Horizon 2020 SIM4NEXUS, and European Project FP7 ACCUS. Since 2013, he has been involved as a main Scientific Advisor in the development and implementation of two pilots of renewable energy sources based microgrid supported by novel energy storage management systems; the project is funded by the European Community. Since 2013, he has been a Scientific Coordinator of Sardinian Regional Renewable Energy Laboratory, Sardinia, Italy. He is the coauthor of more than 160 papers published in international conference proceedings and journals. His research interests include management and control of electric vehicles, microgrid, and energy storage systems.

Prof. Damiano is a Reviewer for several international conferences and journals and a member of IEEE Industrial Electronics Society's Energy Storage and Resilience and Security for Industrial Applications Technical Committees. He was the recipient of two IEEE awards. In 2013, the project "Smart City—A Labelled Municipalities," where he has been the main Scientific Advisor, received from European Commission the "Sustainable Energy Europe and ManagEnergy Award in 2014".

**Craig Rieger** (SM'08) received the B.S. and M.S. degrees in chemical engineering from Montana State University, Bozeman, MT, USA, in 1983 and 1985, respectively, and the Ph.D. degree in engineering and applied science from Idaho State University, Pocatello, ID, USA, in 2008.

He is the Chief Control Systems Research Engineer and a Directorate Fellow with Idaho National Laboratory (INL), Idaho Falls, ID, pioneering interdisciplinary research in the area of next-generation resilient control systems. In addition, he has organized and chaired 11 Institute of Electrical and Electronics Engineers technically cosponsored symposia and one National Science Foundation Workshop in this new research area, and authored more than 50 peer-reviewed publications. He has 20 years of software and hardware design experience for process control system upgrades and new installations. He has also been a Supervisor and Technical Lead for control systems engineering groups having design, configuration management, and security responsibilities for several INL nuclear facilities and various control system architectures.

**Valeriy Vyatkin** (M'03–SM'04) received the Ph.D. degree in computer systems and Dr.Sc. degree in applied computer science from Taganrog Radioengineering Institute, Taganrog, Russia, in 1992 and 1999, respectively, the Dr.Eng. degree in electrical engineering from the Nagoya Institute of Technology, Nagoya, Japan, in 1999, and the Habilitation degree in engineering from the Ministry of Science and Education, Saxony-Anhalt, Germany, in 2002.

He is on joint appointment as Chair of Dependable Computations and Communications with Luleå University of Technology, Luleå, Sweden, and Professor of Information Technology in Automation with Aalto University, Espoo, Finland. He is also a Codirector of the International Research Laboratory "Computer Technologies," ITMO University, Saint Petersburg, Russia. Previously, he was a Visiting Scholar with Cambridge University, Cambridge, U.K., and had permanent appointments with The University of Auckland, Auckland, New Zealand; Martin Luther University, Halle, Germany, as well as in Japan and Russia. His research interests include dependable distributed automation and industrial informatics; software engineering for industrial automation systems; artificial intelligence, distributed architectures, and multiagent systems in various industries, including smart grid, material handling, building management systems, datacenters, and reconfigurable manufacturing.

Dr. Vyatkin was the recipient of the Andrew P. Sage Award for the Best IEEE Transactions Paper in 2012. He is the Chair of IEEE Industrial Electronics Society Technical Committee on Industrial Informatics.

**Milos Manic** (S'96–M'04–SM'06) received the Dipl.Ing. and M.S. degrees in electrical engineering and computer science from the University of Niš, Niš, Serbia, in 1991 and 1997 respectively, and the Ph.D. degree in computer science from the University of Idaho, Moscow, ID, USA, in 2003.

He is currently a Professor with the Computer Science Department and Director of VCU Cybersecurity Center, Virginia Commonwealth University, Richmond, VA, USA. He has given more than 30 invited talks around the world, authored more than 180 refereed articles in international journals, books, and conferences, and holds several U.S. patents. He completed more than 30 research efforts in the area of data mining and machine learning applied to cyber security, critical infrastructure protection, energy security, and resilient intelligent control.

Dr. Manic was the recipient of the R&D 100 Award for Autonomic Intelligent Cyber Sensor in 2018. He is an Officer of IEEE Industrial Electronics Society, Founding Chair of IEEE Industrial Electronics Society Technical Committee on Resilience and Security in Industry, and General Chair of IEEE Industrial Electronics Society in 2018 and IEEE Conference on Human System Interactions in 2019.