Guest Editorial: Special Section on Resilient Control of Cyber-Physical Power and Energy Systems

I. Introduction

OUR power and energy systems are becoming more and more integrated and interconnected. The increasing integration of edge devices and dependence on cyber infrastructure provides both the potential for benefits and risks. The integration enables more dynamic and flexible control paradigms while at the same time increasing the cyberattack surface and uncertainty of behavior. Control methodology in this new world must be designed for resilience and must have the ability to withstand, react, and respond to both physical faults and cyber-induced threats [1]. Understanding system resilience under adverse conditions requires studying control performance and how cyber infrastructure can integrate with and support the overall resilience of the system.

As the distributed energy resources and demand-side control increase in the power grid, the industrial Internet of Things and their security will become increasingly important. As the push to enhance power distribution operations intensify and end-customers play a more integral role in distribution systems, their inverters and a multitude of IoT devices—including home energy management systems, thermostat controls, water heater controls, battery-based smart chargers, and solar panels—will proliferate as controllable assets. These deployments will continue to push controls to the edge of the system, which provides opportunities to use new control paradigms for increased flexibility and resilience of the distribution system [2]. However, these benefits can only be realized if the increased attack surface of the devices and their communication pathways are secure [3].

To ensure a net positive resilience in the face of the increasing dependence on IoT infrastructure, research must prioritize architectural and operational security. Concurrently, maintaining resilience within the cyber-physical power and energy system (CPPES) hinges on reliable sensor data for real-time monitoring, control, and decision-making. Any disruption or compromise of sensor functionality can lead to suboptimal operation and reduced efficiency, and potentially result in operation failure or safety hazards. Building resilient sensing or state estimation systems will enhance system-wide resiliency [4]. Another aspect is the computation resources for monitoring or control within the CPPES. The CPPES will benefit from hardware and algorithmic designs that allow computing resources to self-adapt and continue critical operations when its functionality or computation capacity is compromised by cyberattacks or degraded under faults. Resilient design considerations also suggest an evolution to more distributed, agent-based designs that minimize dependencies and interdependencies, reduce the potential for brittle failures from unrecognized degradation, and provide the framework for self-adaptation [5].

II. Section at a Glance

We received 26 paper submissions, and following a thorough peer review process, only six manuscripts were chosen to be featured in this Special Section of the IEEE Transactions on Control Systems Technology. These selected papers cover a range of cyber-physical resiliency topics: distributed controls utilizing IoT technologies, distributed methods for fault diagnosis and resilient state estimation, and resilient planning and investment decisions utilizing game theoretic approaches. The application domains explored in the featured papers include microgrids, power system substations, and marine engines.

The first two papers focus on grid resilience through the IoT. In [A1], a distributed microgrid control approach is developed to utilize IoT technologies. A distributed state machine algorithm is defined to utilize the IoT communication infrastructure for consensus algorithms to coordinate grid-forming dispatch and transition functions. The performance of the approach is demonstrated on a modified Banshee distribution network model implemented in a hardware-in-the-loop to integrate an implementation of their algorithms running on Beaglebone Black development boards.

While the first paper explores the use of IoT to improve system resiliency, the second paper focuses on improving the resiliency of the IoT foundations to limit the risks for applications to the grid. As the number of IoT devices increases and is needed to coordinate decisions, it will become increasingly important to ensure the devices to efficiently and securely communicate. In [A2], a new approach for securely establishing a group key for distributed communication is presented to optimize the efficiency for lower bandwidth wireless communication commonly used in IoT applications. Dynamic key generation with Shamir's secret sharing algorithm is used to reduce the number of transmitted packets necessary for group key initialization and renewal. The speed efficiency is evaluated from the context of smart grid applications and demonstrated to require fewer communication frames than the existing approaches.

To enable resilient sensing, Kougiatsos and Reppa [A3] presented a model-based distributed architecture for sensors fault detection and isolation in a marine internal combustion engine. Modeling the engine with a nonlinear differential-algebraic equations (DAE) of interconnected subsystems, a local sensor fault detection agent was developed for each subsystem. The agent utilized state and algebraic residuals that are compared with adaptive thresholds. The sensor fault

Digital Object Identifier 10.1109/TCST.2024.3403515

isolation is achieved through a bilevel approach consisting of local and global decision logic layers. The effectiveness of the approach was demonstrated using key performance metrics, including minimum detectable sensor fault magnitude, and missed detection rate.

The second paper on resilient sensing focuses on the co-design of hardware and state estimation algorithm for a sensor estimation system. If computational nodes are lost or processing capacity is diminished due to cyberattacks, Croteau et al. [A4] present an approach to self-adapt a bank of Kalman filters and reprogram the new structure on surviving field-programmable gate arrays (FPGAs) during run time. The method was demonstrated on a prototype system to estimate the kinematics of a maneuvering unmanned surface vehicle.

While the other papers focus more on operational resilience concerns, the final two papers focus on planning and making investment decisions to enable a more resilient system response. In [A5], a new metric is defined to enable the risk analysis and assessment of the resilience of transmission system substations. The new metrics incorporate vulnerability and amount of defender knowledge to evaluate optimal investment strategies to achieve resilience. The new metric is validated through simulations on research transmission models.

In [A6], resilience strategies are studied to improve the grid defensive posture. Game theory techniques are used to study attacker-defender models where mean-field degree-based epidemic models are used to define the behavior of malware propagation across IoT-enabled power grids. Resilient strategies are found by searching for Nash equilibriums of the game that stymie the effect of the botnet. Case studies are presented using the IEEE 39 bus transmission model.

III. Conclusion

The Special Section on Resilient Control of CPPESs sheds light on the critical importance of developing resilient control methodologies in the face of increasing integration and interconnectivity in power and energy systems. The research presented in this Special Section showcases innovative approaches to enhancing system resilience under adverse conditions, including cyber-induced threats and physical faults.

By exploring distributed controls utilizing IoT technologies, fault diagnosis methods, resilient state estimation techniques, and game theoretic approaches for planning and investment decisions, the selected papers offer valuable insights into addressing the complex challenges of ensuring the resilience of cyber-physical systems in the power and energy domain. These contributions not only advance the theoretical understanding of system resilience but also provide practical implications for improving the operational efficiency and security of power and energy systems.

Moving forward, future research endeavors should focus on further exploring the synergies between cyber infrastructure and control methodologies to improve the resilience of power and energy systems. In the near term, this entails the emergence of new control tools and theoretic paradigms tailored to tackle emerging challenges. Efforts would aim to create resilience planning tools and cyber-layer middleware, along with agnostic tools, to strengthen the resilience of next-generation power and energy systems against evolving cyber threats. Long-term efforts would consider the framework for applying distributed control that recognizes and adapts to threats, minimizing the complexity of the operation through agent-based architectures that provide a solid foundation for greater autonomy [6].

Acknowledgment

The Guest Editors extend their gratitude to all the authors for their contributions through their submissions. We also express our sincere appreciation to the diligent reviewers who meticulously evaluated the several papers submitted, ensuring the quality and rigor of this special section. Additionally, we wish to acknowledge the past Editor-in-Chief of this journal, Prof. Andrea Serrani, for entrusting us with the responsibility to organize this special section. His unwavering support and invaluable guidance have been instrumental throughout the preparation of this contribution.

Veronica Adetola, *Guest Editor*
Pacific Northwest National Laboratory
Richland, WA 99352 USA
veronica.adetola@pnnl.gov

Thomas W. Edgar, *Guest Editor*
Pacific Northwest National Laboratory
Richland, WA 99352 USA
thomas.edgar@pnl.gov

Sai Pushpak Nandanoori, *Guest Editor*
Pacific Northwest National Laboratory
Richland, WA 99352 USA
saipushpak.n@pnnl.gov

Quanyan Zhu, *Guest Editor*
New York University
Brooklyn, NY 11201 USA
qz494@nyu.edu

Masoud Abbaszadeh, *Guest Editor*
GE Vervona Research Center
Niskayuna, NY 12309 USA
abbaszadeh@ge.com

Craig Rieger, *Guest Editor*
TRECS Consulting, LLC
Pocatello, ID 83201 USA
sliderbot@gmail.com

References

[1] C. G. Rieger, D. I. Gertman, and M. A. McQueen, “Resilient control systems: Next generation design research,” in *Proc. 2nd Conf. Hum. Syst. Interact.*, May 2009, pp. 632–636, doi: 10.1109/HSI.2009.5091051.

[2] (2020). *Power Systems in Transition*. [Online]. Available: https://www.iea.org/reports/power-systems-in-transition

[3] *Secure Communications: Interoperability in the Power Grid*, Dept. Energy, Washington, DC, USA, 2023.

[4] G. Chen, Y. Zhang, S. Gu, and W. Hu, “Resilient state estimation and control of cyber–physical systems against false data injection attacks on both actuator and sensors,” *IEEE Trans. Control Netw. Syst.*, vol. 9, no. 1, pp. 500–510, Mar. 2022, doi: 10.1109/TCNS.2021.3113265.

[5] C. G. Rieger, K. L. Moore, and T. L. Baldwin, “Resilient control systems: A multi-agent dynamic systems perspective,” in *Proc. IEEE Int. Conf. Electro-Inf. Technol.*, May 2013, pp. 1–16, doi: 10.1109/EIT.2013.6632721.

[6] A. M. Farid, “Multi-agent system design principles for resilient coordination & control of future power systems,” *Intell. Ind. Syst.*, vol. 1, no. 3, pp. 255–269, Oct. 2015, doi: 10.1007/S40903-015-0013-X.

Appendix: Related Articles

[A1] H. Tu et al., "An IoT-based framework for distributed generic microgrid controllers," *IEEE Trans. Control Syst. Technol.*, vol. 32, no. 5, pp. 1692–1705, Sep. 2024.

[A2] Y. Hanna, M. Cebe, J. Leon, and K. Akkaya, "Efficient group key management for resilient operation of LoRaWAN-based smart grid applications," *IEEE Trans. Control Syst. Technol.*, vol. 32, no. 5, pp. 1706–1717, Sep. 2024.

[A3] N. Kougiatsos and V. Reppa, "A distributed cyber-physical framework for sensor fault diagnosis of marine internal combustion engines," *IEEE Trans. Control Syst. Technol.*, vol. 32, no. 5, pp. 1718–1729, Sep. 2024.

[A4] B. Croteau, K. Kiriakidis, T. A. Severson, R. Robucci, S. Rahman, and R. Islam, "State estimation adaptable to cyberattack using a hardware programmable bank of Kalman filters," *IEEE Trans. Control Syst. Technol.*, vol. 32, no. 5, pp. 1730–1742, Sep. 2024.

[A5] K. Khanna and M. Govindarasu, "Resiliency-driven cyber–physical risk assessment and investment planning for power substations," *IEEE Trans. Control Syst. Technol.*, vol. 32, no. 5, pp. 1743–1754, Sep. 2024.

[A6] Y. Zhao, J. Chen, and Q. Zhu, "Integrated cyber-physical resiliency for power grids under IoT-enabled dynamic botnet attacks," *IEEE Trans. Control Syst. Technol.*, vol. 32, no. 5, pp. 1755–1769, Sep. 2024.

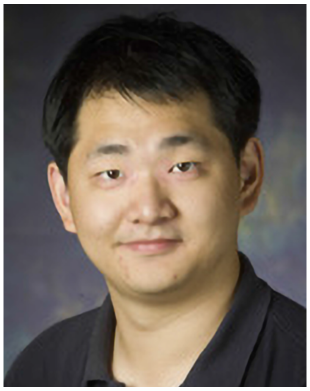
Veronica Adetola is a Chief Research Scientist at the Pacific Northwest National Laboratory (PNNL), Richland, WA, USA. She leads the Resilient Control Methods Team and research and development for cyber-physical systems resilience, sustainable electrification of buildings and industrial systems, and reliable integration of inverter-based distributed energy resources into the power grids. Before joining PNNL in 2019, she worked at the United Technologies Research Center (now Raytheon Technologies), East Hartford, CT, USA, where she made significant contributions and successfully led efforts for multiple UTC businesses and government-funded research programs. She has authored a book, three book chapters, more than 50 journal publications and peer-reviewed conference papers, and holds ten granted U.S. patents. Her expertise includes model predictive control, adaptive and robust control, learning-based control, real-time optimization, and control co-design for various applications.

Dr. Adetola was a Board of Governors Member of the IEEE Control Systems Society in 2019. He is the Vice Chair of the IEEE Control System Society (CSS) Technical Committee on Energy Systems. He currently serves as an Associate Editor for IEEE Transactions on Control Systems Technology.

Thomas W. Edgar is a Chief Cyber Security Research Scientist at Pacific Northwest National Laboratory, Richland, WA, USA. During his time at the laboratory, he has worked in the fields of secure communications protocols, cryptographic trust management, cyber deception, security standards, and scientific approach to security. Most specifically, he is the Principal Investigator for a cyber-physical testbed to enable controlled experimentation in high fidelity environments as well as being a focus area lead on an internal investment overseeing projects for phenomenological understanding of OT systems to improve and validate resilient response. His expertise lies in scientific process, critical infrastructure security, protocol development, cyber deception, and network security. His contributions have resulted in numerous national awards (2017 Research and Development 100 Award and the 2018 Federal Laboratory Consortium for Excellence in Technology for the SerialTap Technology and 2021 Research and Development 100 Award for Shadow Figment Technology), four patents with multiple commercial transfers/licenses, a textbook on "Research Methods for Cyber Security," and contributions that led to the IEEE 1711 part 2 standard.

Sai Pushpak Nandanoori (Member, IEEE) received the B.Tech. degree in electrical and electronics engineering from Pondicherry Engineering College, Pondicherry, India, in 2009, the M.S. degree in dynamical systems and control from Indian Institute of Technology Madras, Chennai, India, in 2013, and the Ph.D. degree in dynamical systems and control from Iowa State University, Ames, IA, USA, in 2018.

He is currently a Staff Research Engineer with Pacific Northwest National Laboratory, Richland, WA, USA. His research interests include developing novel system theoretic methods and data-driven methods using Koopman operator theory to solve challenging problems in the areas of power systems, microgrids, and cyber-physical systems. His work was highlighted in the top 100 downloaded engineering papers published in *Scientific Reports* in 2023.



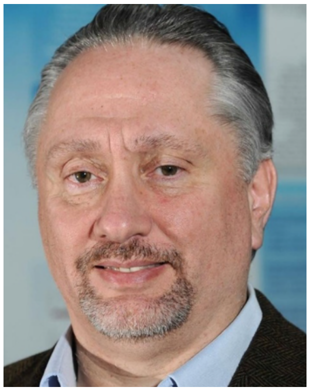
Quanyan Zhu is an Associate Professor with the Department of Electrical and Computer Engineering, New York University (NYU), New York, NY, USA. He also holds affiliations as a Faculty Member with the Center for Urban Science and Progress (CUSP) and the Center for Cyber Security (CCS), NYU. His research interests encompass network optimization and control, resilience of cyber and physical systems, security of industrial control systems, and the Internet of Things.

Dr. Zhu is currently the Technical Committee Chair of Security and Privacy for the IEEE Control Systems Society. He serves as an Associate Editor for IEEE TRANSACTIONS ON AEROSPACE AND ELECTRONIC SYSTEMS and IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING.

Masoud Abbaszadeh received the Ph.D. degree in electrical and computer engineering from the University of Alberta, Edmonton, AB, Canada, in 2008.

He was an Adjunct Professor at the Department of Electrical, Computer and Systems Engineering, Rensselaer Polytechnic Institute, Troy, NY, USA. He is currently a Principal Research Engineer at GE Research Center, Niskayuna, NY, USA, where he leads research and technology development for cyber-physical security and resilience and autonomous systems. He has authored over 150 peer-reviewed articles, nine book chapters, and holds 40 issued U.S. patents with more than 45 additional U.S. patents pending. He has also published two books, an edited volume on cyber-physical systems security and resilience (Springer 2022) and a research monograph on nonlinear optimal control with applications in robotics and energy systems (IET 2022).

Dr. Abbaszadeh is a member of IEEE CSS Conference Editorial Board. He was a recipient of multiple awards at GE Research Center, including the 2018 GE Dushman Award (highest award at GE Research and Development), the 2020 GE Research Control & Optimization Innovation Award, and the 2020 GE Research Technology Award. He is an Associate Editor of IEEE TRANSACTIONS ON CONTROL SYSTEMS TECHNOLOGY.



Craig Rieger backed by years of professional expertise in practical and theoretical control system engineering, he pioneered the resilient control systems research area with an interdisciplinary team at Idaho National Laboratory, Idaho Falls, ID, USA, and several universities. Advancing this threat resilience theme is his current focus as the Managing Director of TRECS Consulting. Prior to establishing his consultancy, he worked for the Idaho National Laboratory in several positions, including a Directorate Fellow, a Chief Control Systems Research Engineer, a Control Systems Lead, and an Instrumentation, Control, and Intelligent Systems Lead.

Dr. Rieger has contributed to a number of publications, including “Resilient Control Systems: Next Generation Design Research,” “A Cyber Resilient Design for Control Systems,” and a recent Wiley IEEE book *Resilient Control Architectures and Power Systems*. He also holds patents in “Systems and Methods for Control System Security.” Although his career has been filled with highlights, he takes the most pride in establishing the interdisciplinary research area of threat-resilient control systems. In light of his team’s achievement, the Region 6 IEEE Director’s Award was presented in 2014.