Tutorial Title:

Emerging Cybersecurity Challenges in Modern Energy Systems – Assessment and Solutions

Organizer:

Subham Sahoo, Aalborg University, sssa@energy.aau.dk

Yan Li, Penn State University, yql5925@psu.edu

Charalambos Konstantinou, King Abdullah University, charalambos.konstantinou@kaust.edu.sa

Abstract:

Cyberattacks on critical infrastructure can have a debilitating effect on national economic security, public health, and safety. The underlying processes of the critical power infrastructure sector controlled by the information and communication technology-based elements employed into power electronic systems, create a close coupling between the cyber and physical components. This transition greatly expands the attack surface of such systems, as cyberattacks targeting commercial-off-the-shelf hardware and software are well-known.

In this context, this tutorial not only aims to establish the scientific know-how comprising a framework from basic to advanced topics on power systems and power electronics security, but also plans to demonstrate its impact on different operation layers from lab-scale resources. The first part of the tutorial will emphasize on providing context on building testbeds for security studies, providing guidance on recognizing weaknesses, which can be valuable to attackers. It then aims at, along with threat modeling and risk assessment strategies, the modeling, resources, and metrics for industrial control systems security studies. Case studies on cyberattacks and defenses will be presented in a hardware-in-the-loop environment using OPAL-RT real-time simulator and EXataCPS emulator. Moreover, different cases of attack strategies will be simulated under nominal and abnormal operating conditions to uncover their system-wide impacts in power systems, as well as illustrate the impact of such attacks. The feasibility of the detection methods leveraging the hardware layer will then be investigated from a system resiliency perspective. The second part of the tutorial will then put spotlight on resiliency metrics against cyber-attacks across much faster dynamics in the microgrid scale. Keeping these issues in view, a stepwise design of software-defined networking (SDN) technique will be introduced to build the communication network, with the objective of enabling the network's real-time configuration ability. Three typical SDN planes will be introduced, namely, data plane, control plane and application plane. Their separation is designed to manage the data traffic and generate extensible functions such as cyberattack detection. Considering the holistic visibility of SDN also makes the system vulnerable to cyberattacks, the model-based programmable cyberattack detection and defense strategies will be introduced to secure the SDN network in microgrids. A demonstration will be provided to showcase the programmable detection and defense strategies. Finally, the third part of the tutorial will generally focus on the impact of cyber attacks on operation management of power electronic systems. Generalization from projections of cyber attacks on stability and reliability of the grid will firstly be carried out using a self-healing

mechanism. Furthermore, different methodologies to model cyber attacks will be explained in detail, which are programmed to be introduced into the systems as faults. To characterize between various malfunctioning events and cyber attacks, the design of anomaly detection tools will be explained. Finally, demonstration videos from experimental prototype will be shown to examine the performance of the self-healing mechanism under different cyber attacks, faults, unstable events. Moreover, its efficacy to restore the system back to normally and protect the physical infrastructure from cyber attacks will be analyzed in detail.

Bio:

Subham Sahoo received his Ph.D. degree in Electrical Engineering at Indian Institute of Technology (IIT), Delhi, New Delhi, India in 2018. After the completion of his PhD, he worked as a postdoctoral researcher in the Department of Electrical and Computer Engineering in National University of Singapore during 2018-19 and in Aalborg University (AAU), Denmark during 2019-2020. He is currently an Assistant Professor in the Department of Energy, AAU, Denmark.

He is a recipient of the Indian National Academy of Engineering (INAE) Innovative Students Project Award for the best PhD thesis across all the institutes in India for the year 2019. He was also a distinguished reviewer for IEEE Transactions on Smart Grid in the year 2020. He is an active contributor and chairs the cybersecurity working group in the IEEE PELS Technical Committee (TC 10) on Design Methodologies. He has delivered 2 tutorials in IEEE APEC 2020 and IEEE IECON 2020. He has also organized the first Industrial/PhD course on Cybersecurity for power electronic systems in AAU in the year 2020.

His research interests are control, optimization, cybersecurity and stability of power electronic dominated grids, physics-informed machine learning tools for power electronic systems.

Yan Li received her Ph.D. degree from University of Connecticut, Storrs, CT, U.S., in 2019. She also received a Ph.D. degree from Tianjin University, Tianjin, China, in 2013. Both are in electrical engineering. She worked as a postdoctoral researcher in the Department of Electrical Engineering and Computer Science in University of Denver during 2013-2014. She is currently an assistant professor at the School of Electrical Engineering and Computer Science in The Pennsylvania State University, University Park, PA, U.S.

She is a recipient of IEEE-PES Outstanding Engineer Award, Connecticut Women of Innovation Award, UConn Outstanding Senior Women Academic Achievement Award, Connecticut Power and Energy Society Rising Star Award. She is an associate editor of IET Energy System Integration and an active reviewer for several journal and conferences, including IEEE Transactions on Power System, IEEE PES General Meeting, and IEEE ITEC. She is a Senior Member of IEEE and a member of INFORM. She has developed a Sustainable Energy course for Penn State undergraduate students, which introduces typical renewable energy, control strategies, and microgrids. A new course, Cyber-Physical Microgrids, is under development.

Her research interests include cyber-physical microgrids, quantum computing, data-driven modeling and control, cybersecurity, software-defined networking, resilience analysis, etc.

Charalambos Konstantinou is an Assistant Professor of Computer Science (CS) and Affiliate Professor of Electrical and Computer Engineering (ECE) at King Abdullah University of Science and Technology (KAUST), Thuwal, Saudi Arabia. He is the PI of the Secure Next Generation Resilient Systems Lab (sentry.kaust.edu.sa) and a member of the Resilient Computing and Cybersecurity Center (RC3) at KAUST. His research interests are in secure, trustworthy, and resilient cyber-physical and embedded IoT systems. He is also interested in critical infrastructures security and resilience, renewable energy integration, and real-time simulation. He received a Ph.D. in EE from New York University and a M.Eng. Degree in ECE from National Technical University of Athens, Greece. Before joining KAUST in 2021, he was an Assistant Professor at Florida State University. Konstantinou is currently the Chair of the IEEE Task Force on Resilient and Secure Large-Scale Energy Internet Systems and the co-Chair of the IEEE Task Force on Cyber-Physical Interdependence for Power System Operation and Control. He has delivered a recent tutorial on 'Industrial Control Systems Security' in Design, Automation, and Test in Europe (DATE) Conference and Exhibition 2021. He is a Senior Member of IEEE, a member of ACM, and an ACM Distinguished Speaker (2021-2024).