Electrical & Computer Engineering

S E M I N A R

Louisiana State University

Data-Driven Approaches for Safe and Secure Cyber-Physical Systems

Paul Griffioen

University of California, Berkeley

Abstract—Cyber-physical systems (CPSs), engineered systems which include sensing, processing, control, and communication in physical spaces, are ubiquitous in modern critical infrastructures including manufacturing, transportation systems, energy delivery, health care, water management, and the smart grid. As the physical, communication, and computational parts of these complex systems become increasingly interconnected and intertwined, it is important to ensure their safety and security in the presence of uncertainties and attacks. In this talk, we present three necessary components for designing safe and secure CPSs: detecting attacks, responding to attacks, and providing safety guarantees for systems with unmodeled dynamics. In particular, we introduce the moving target defense, software rejuvenation, and data-driven reachability, showing how each of these tools leverage knowledge of the underlying physical dynamics to guarantee safety and security. We illustrate our results in a number of example applications and present future research directions for data-driven CPS safety and security.

Bio—Paul Griffioen is currently a postdoctoral researcher in the Department of Electrical Engineering and Computer Sciences at the University of California, Berkeley working with Murat Arcak. He received M.S. and Ph.D. degrees in Electrical and Computer Engineering from Carnegie Mellon University in 2018 and 2022, respectively, where he was co-advised by Bruno Sinopoli and Bruce H. Krogh. He received a B.S. degree in Electrical and Computer Engineering from Calvin College in 2016. His research interests include the modeling, analysis, and design of active detection techniques and response mechanisms for ensuring resilient and secure cyber-physical systems. His research interests also include data-driven analysis and design of high-performance cyber-physical systems that ensure safety while operating under computational constraints.

When: Tuesday, **19 March 2024,** 10:30 - 11:30
Where: Room 3316E Patrick F. Taylor Hall
Info: `https://www.lsu.edu/eng/ece/seminar`