Electrical & Computer Engineering

SEMINAR

Louisiana State University

Combined Knowledge and Data Driven Safety Assurance in Cyber-Physical Systems

Xugui Zhou

University of Virginia

Abstract—Rapid advances in sensing and computing technologies have led to the proliferation of Cyber-Physical Systems (CPS). However, increasing device complexity, shrinking technology sizes, and shorter time to market have resulted in significant challenges in ensuring the reliability, safety, and security of CPS. Significant efforts have been made using techniques such as run-time verification, monitoring, and anomaly detection. However, these approaches cannot maintain high detection accuracy, considering complex system dynamics and unpredictable human behaviors in the control loop, and often detect the occurrence of hazards late, which may not leave enough time for successful mitigation. In addition, there is often a gap between the safety properties checked at run-time and the safety requirements specified at design time, which are usually based on ad-hoc and fixed rules and do not account for the multi-dimensional context in the CPS, including physical processes, the environment, the cyber components that affect the physical processes, and their interactions in both temporal and spatial domains.

In this talk, I will present my research addressing these challenges through a hybrid knowledge and data driven approach to context-aware safety assurance in CPS. First, I will discuss vulnerabilities in safety-critical CPS and introduce a formal framework for control-theoretic specification of safety requirements. Then I will present two combined knowledge and data driven approaches to refining safety specifications for run-time safety monitoring and hazard mitigation, and design-time safety validation. Finally, I will illustrate my visions for the future, engineering the next generation of CPS that are safer and more robust through automatic, adaptive, and trustworthy safety assurance.

Bio—Xugui Zhou is a Ph.D. candidate in Electrical and Computer Engineering at the University of Virginia, advised by Prof. Homa Alemzadeh. Before Joining UVA in 2019, he was a project manager and senior engineer at State Grid and researched power grid protection technology. Prior to that, he obtained his B.Eng in Automation and M.Eng in Control Science and Engineering from Shandong University, China, in 2012 and 2015, respectively. His research interests are at the intersection of computer system security and control system engineering by drawing techniques from formal methods and machine learning. His work has appeared at top-tier venues, including AAAI, DSN, and IEEE TDSC. He has received Rising Star Award in CPS 2023, Carlos and Esther Farrar Graduate Fellowship Award, Google Ph.D. Fellowship Internal Selection, and GTRI Focus Fellowship Award, and is the inventor of three international patents.

When: Thursday, **21 March 2024,** 10:30 - 11:30
Where: Room 3316E Patrick F. Taylor Hall
Info: `https://www.lsu.edu/eng/ece/seminar`