Bio: Luis Garcia is a Postdoctoral Scholar in the Networked and Embedded Systems Laboratory (NESL) in the University of California, Los Angeles (UCLA) Electrical and Computer Engineering Department since 2018. His research interests include the safety and security of learning-enabled cyber-physical systems, malware analysis and reverse engineering, industrial control system security and verification, as well as broad interests in novel applications of machine learning. His research is funded by the U.S. Department of Education Graduate Assistance in Areas of National Need (GAANN) Fellowship. He obtained his Ph.D. in Computer Engineering with a Cyber Security track working on the safety and security of cyber-physical industrial control systems at Rutgers University in 2018.

“Feeling Safe and Secure in a Learning-Enabled Cyber-physical World”

In the current cyberwarfare climate, industrial control systems (ICS) are increasingly becoming focal points of security research as they interconnect, monitor, and control safety-critical processes. ICS comprise a class of cyber-physical systems (CPS) across a wide range of domains, including but not limited to the electric power grid, factory automation, as well as nuclear reactors. As the interconnectivity and accessibility of ICS system components expands, the attack surface for such systems expands as well. Because these ICS control safety-critical physical processes, there is a need for security solutions that have the physical dynamics integrated into the design process in order to ensure safe operation.

In this presentation, I will present my research that investigates the security and verification of ICS at different levels of abstraction. The goal is to bridge the gap between practical security analyses and sound theoretical approaches to verifying cyber-physical systems. In particular, my research will not only leverage the physical properties of an ICS for security purposes, but to also provide fine-grained hybrid systems modelling of embedded cyber-physical systems such as programmable logic controllers (PLCs). I further describe some of my ongoing research that focuses on the safety and security implications of enabling machine learning in the context of safety critical systems.