Speaker: Dr. Christiana Chamon Garcia
Assistant Professor, Virginia Tech

Talk Title: Trustworthy Intelligence for Cyber-Physical Systems: From Hardware Roots of Trust to Resilient AI

Talk Location/Time: ITE 346; Sep. 14 @ 11:15AM-12:15PM

Abstract: Cyber-physical systems increasingly rely on distributed sensing, embedded intelligence, networked control, and machine-learning-enabled decision-making. While these capabilities improve autonomy and efficiency, they also expand the attack surface across hardware, communications, software, and data-driven models. Security failures can therefore propagate beyond the digital domain to affect physical processes, safety, reliability, and mission assurance. This work examines how trustworthy intelligence can be developed for cyber-physical systems by connecting hardware-rooted trust, physical-layer security, stochastic modeling, and robust artificial intelligence. Discussion includes research directions for detecting and characterizing anomalous system behavior under uncertainty; securing sensing, computation, and communication at resource-constrained edge devices; and improving the resilience of AI-enabled monitoring and control against adversarial manipulation, distribution shifts, and synthetic or deceptive data. A central theme is that effective security mechanisms should not treat the physical system as an afterthought: system dynamics, operational context, and measurable physical constraints can provide valuable evidence for authentication, anomaly detection, and attack mitigation. Open challenges in moving from isolated detection algorithms toward adaptive, explainable, and experimentally validated security architectures for critical cyber-physical applications are highlighted.

Bio: Christiana Chamon Garcia received the B.S. degree in electrical engineering from the University of Houston, Houston, TX, USA, in 2017 and the M.S. and Ph.D. degrees in electrical engineering from Texas A&M University, College Station, TX, USA, in 2020 and 2022, respectively. She is currently an Assistant Professor for the Bradley Department of Electrical and Computer Engineering at Virginia Tech, Blacksburg, VA, USA and the director of the Stochastic Noise and Cyber Innovation Lab (SNACIL).

In 2016 she was a Hardware Design Intern and in 2017 a Product Management Intern with Hewlett Packard Enterprise. In 2022, she was an Applications Engineer at Vidatronic Inc, and from 2022 to 2024, she was an Instructional Assistant Professor for the Department of Computer Science and Engineering at Texas A&M University, College Station, TX, USA. Her research interests include stochastic processes, physical unclonable functions, decentralized networks, cyber-physical systems, security in artificial intelligence, engineering education, human-computer interaction, accessibility in engineering and kinesiology, and exercise science.

Dr. Garcia is a 2024 CCI Faculty Fellow, 2023 Future Faculty Diversity Program (FFDP) Fellow, 2023 WISCPROF: Future Faculty in Engineering Workshop Fellow, 2020-2021 Ebensberger Fellow, and a member of ACM, IEEE, and Eta Kappa Nu (HKN).