CONTEXTUAL
ROBOTICS
INSTITUTE

UC San Diego

Building Safe and Secure Cyber-Physical Systems Against All Odds!

Radoslav Ivanov– University of Pennsylvania

Monday, 7th May 2018, at 1pm
Computer Science & Engineering Building, room #1202

Abstract: The increased autonomy of modern Cyber-Physical Systems (CPS) has exposed our limited understanding of systems of such complexity. Multiple deadly accidents in different domains (e.g., automotive, medical, aircraft) have occurred in the last several years, some due to partially known and changing (physiological) models and some due to malicious attacks that disrupt the system operation. In this talk, I will discuss my work on ensuring the safety and security of modern CPS; in particular, my focus is on providing accurate information with guarantees as a necessary condition to closing the loop. In the Medical CPS domain, I have developed parameter-invariant and context-aware detection and estimation approaches with guaranteed performance regardless of the values of unknown patient-specific physiological parameters (e.g., metabolic rate). We have successfully applied these approaches on real-patient data from the Children's Hospital of Philadelphia for the purpose of monitoring the patient's oxygen content during surgery.

In the CPS security domain, my work makes use of the inherent sensor redundancy available in modern CPS in order to argue about the system safety and security even when some components might be under attack. In particular, I have proposed attack-resilient sensor fusion techniques that do not require any assumptions about which particular sensors fail or are under attack in order to detect safety-critical states. We have evaluated the benefit of sensor fusion in a number of automotive CPS applications where the system has access to multiple sensors that can be used to estimate the same state (e.g., velocity can be estimated using encoders, cameras, GPS, etc.).

Bio: Radoslav Ivanov received the B.A. degree in computer science and economics from Colgate University, NY, and the Ph.D. degree in computer and information science from the University of Pennsylvania. He is currently a postdoctoral researcher at the University of Pennsylvania, working with Insup Lee and James Weimer. Radoslav's research interests include the design and control of safe and secure cyber-physical systems, in particular, automotive and medical CPS, and predictive and retrospective analysis of medical patient data.

Hosted by Nikolay Atanasov [natanasov@eng.ucsd.edu]

The **Contextual Robotics Institute** aligns world-class expertise in hardware, software, cognitive science, design, machine learning, materials, security, and more, in order to develop systems that sense the environment around them; learn from experience and situational awareness; and act autonomously to assist humans and serve the public good.

ContextualRobotics.ucsd.edu