Robotics and Flexible Automation Section (ROI)
INVITED LECTURE:

“Securing Autonomy in Contested Environments”

Miroslav Pajić, Duke University, Durham (NC), USA

Abstract: The tight interaction between information technology and the physical world makes autonomous vehicles (AVs) vulnerable to attacks beyond the standard cyber-attacks, illustrating the need to change the way we reason about AV security. In this talk, I will present our recent efforts in this domain, starting from security-aware modeling and vulnerability analysis of neural network-based control systems operating in adversarial environments. Based on the novel notions of attack effectiveness and stealthiness independent of any potentially employed anomaly detector, we developed sufficient conditions for the existence of stealthy effective attacks that force the system into an unsafe operating region, for different levels of runtime information available to the attacker. Further, I will illustrate how such attacks can be launched on various perception architectures in modern AVs, exploiting intrinsic vulnerabilities in heterogenous perception-based sensing (e.g., camera, LiDAR, radar). Finally, I will advocate that we need to strengthen each layer of the autonomy stack before introducing our methods for security-aware planning for AVs operating in unknown stochastic environments, in the presence of attacks.

Short Bio:

Miroslav Pajic is the Dickinson Family Associate Professor in the Department of Electrical and Computer Engineering at Duke University. He also holds a secondary appointment in the Computer Science Department. His research interests focus on the design and analysis of high-assurance cyber-physical systems with varying levels of autonomy and human interaction, at the intersection of (more traditional) areas of embedded systems, AI, learning and controls, formal methods, and robotics. He is currently leading efforts on secure (edge-based) autonomy as part of the AFOSR Center of Excellence on Assured Autonomy in Contested Environments and the new ATHENA NSF AI Institute on Edge Computing.

Dr. Pajic received various awards including the NSF CAREER Award, ONR Young Investigator Program Award, ACM SIGBED Early-Career Researcher Award, IEEE TCCPS Early-Career Award, IBM Faculty Award, ACM SIGBED Frank Anger Memorial Award, the Joseph and Rosaline Wolf Dissertation Award from Penn Engineering, as well as seven Best Paper and Runner-up Awards, such as the Best Paper Awards at the 2017 ACM SIGBED International Conference on Embedded Software (EMSOFT) and 2014 ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS), and the Best Student Paper award at the 2012 IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS). He is an associate editor in the ACM Transactions on Cyber-Physical Systems and ACM Transactions Computing for Healthcare (ACM HEALTH) and was a Chair of the 2019 ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS'19).