2021 NSF CYBER-PHYSICAL SYSTEMS PRINCIPAL INVESTIGATORS' MEETING

CAREER: Foundations for Secure Control of Cyber-Physical Systems

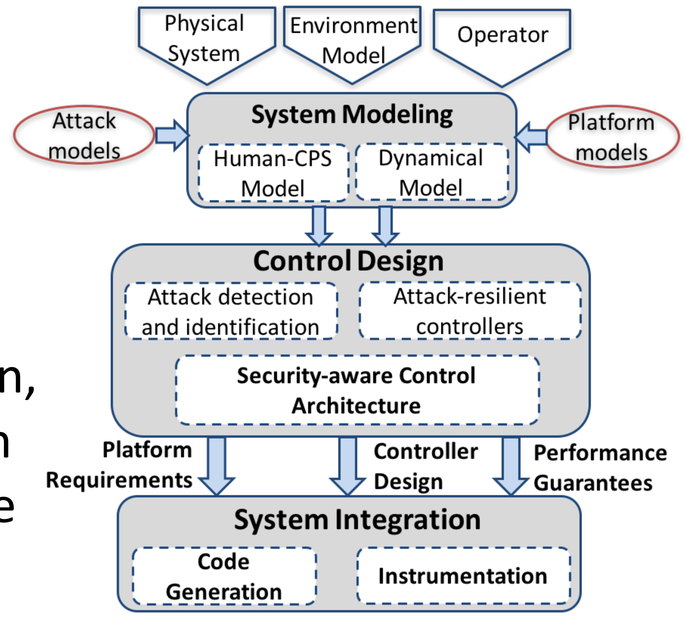
PI: Miroslav Pajic, Duke University

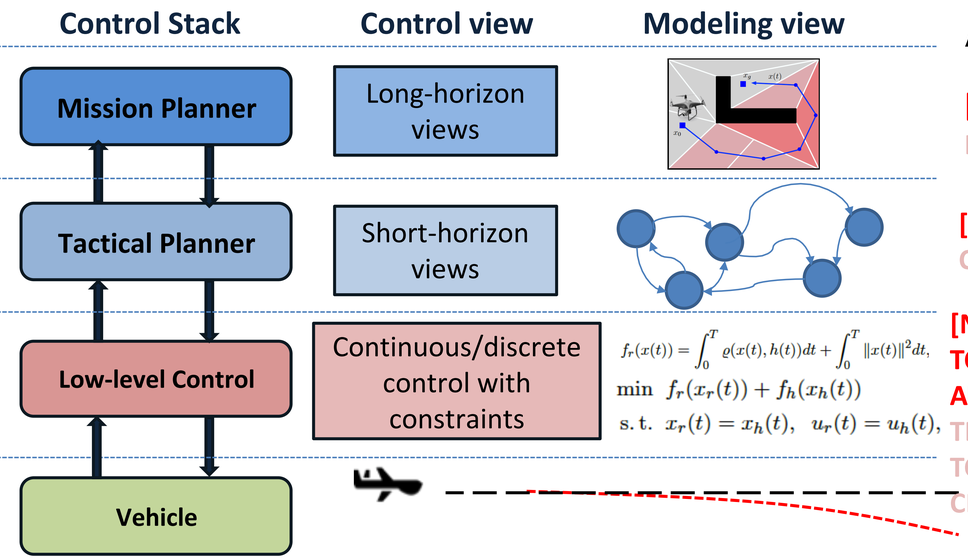
Challenge:

- Develop scientific foundations for secure control of CPS with varying levels of autonomy and human interaction

Solution:

- A mix of resilient control, attack-detection, efficient execution monitoring and system recovery provides safety and performance guarantees even under attack





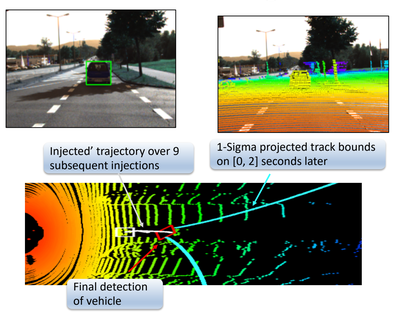
Adding Resiliency

[ICRA21a, ICRA21b, ICRA20, ICRA19, CAV'19a, THMS19]

[AUT21*, TII21, TASE21*, CDC19a, CDC19b, IoTDI19]

[NeurIPS21a*, USENIX Sec22*, TCPS20, TCPS20, ACC20, AUT21b*, AUT21, AUT18, TECS17, RTSS17, TCNS17a, TCNS17b, CSM17, CDC17, CDC18,…]

Tracking Case Study: Vehicle Following



Our Goal: Add resiliency to controls across all levels of control stack

Scientific Impact:

- Recent Contributions
  - Security-aware planning via model-free learning [ICRA21a]
  - SMC for Probabilistic HyperProperties (EMSOFT19,CSF21)
  - Vulnerability Analysis using Adversarial Learning (NeurIPS21*)
  - Control-aware security integration (TCPS20, ACC20,AUT21*, TAC19, …)
  - Security-Analysis of Camera-LiDAR semantic level fusion (USENIX Sec'21*)

- EMSOFT17 Best Paper Award
- EMSOFT19 Best Paper Finalist
- IEEE TCCPS Early-Career Award,
- ACM SIGBED Early-Career Award
- IBM Faculty Award, …

Broader Impact:

- Outreach & educational activities at Duke
- Tech transfer: Intel and NATO CMRE

Award #: CNS 1652544
Award Date: 03/15/2017-02/28/2022
PI: Miroslav Pajic
Email: miroslav.pajic@duke.edu