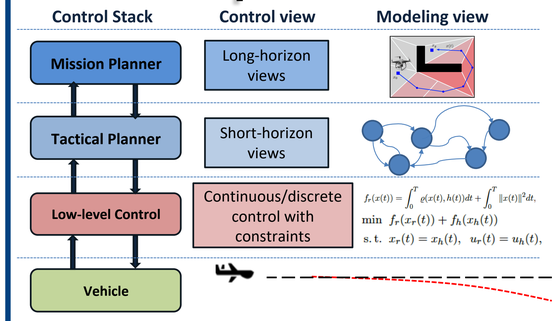
CAREER: Foundations for Secure Control of Cyber-Physical Systems

Miroslav Pajic
Department of Electrical and Computer Engineering, Duke University

CNS 1652544

1 Cyber-Physical Security Techniques



Adding Resiliency

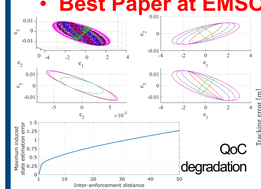
[ICRA21a, ICRA21b, ICRA20, ICRA19, CAV'19a, THMS19]

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

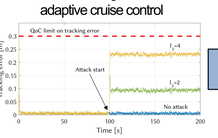
[NeurIPS21a*, USENIX Sec22*, TCPS20, TCPS20, ACC20, AUT21b*, AUT21, AUT18, TECS17, RTSS17, TCNS17a, TCNS17b, CSM17, CDC17, CDC18,...]

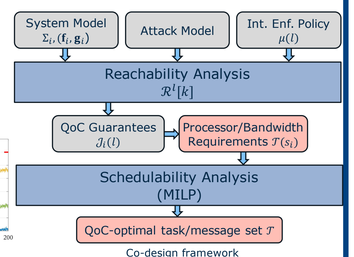
Recent Contributions

- Security-aware planning via model-free learning [**ICRA21a**]
  - Use high-assurance reinforcement learning for 2-player stochastic games [**ICRA21b**, **NeurIPS21b***]
- Statistical Model Checking for Probabilistic HyperProperties (**EMSOFT19 - Best Paper Award Finalist, CSF21**)
- Vulnerability Analysis for Complex CPS using Adversarial Learning [**NeurIPS21***]
  - Framework for analysis of control degradation for different threat models
- Control-aware **intermittent** integrity enforcement [**TCPS20, ACC20, AUT21*, TAC19**, **CDC17, CDC18**]
- Security Analysis of Camera-LiDAR Semantic-Level Fusion [**USENIX Sec22***]
- Security-Aware Scheduling
  - **Best Paper at EMSOFT'17**

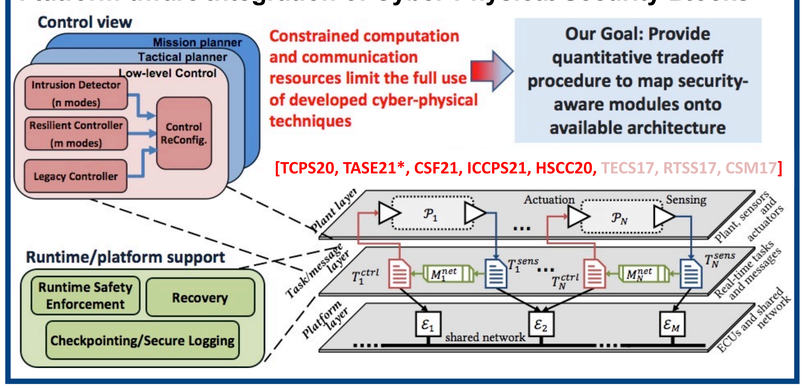


Reachable regions for a adaptive cruise control





Platform-aware Integration of Cyber-Physical Security Blocks



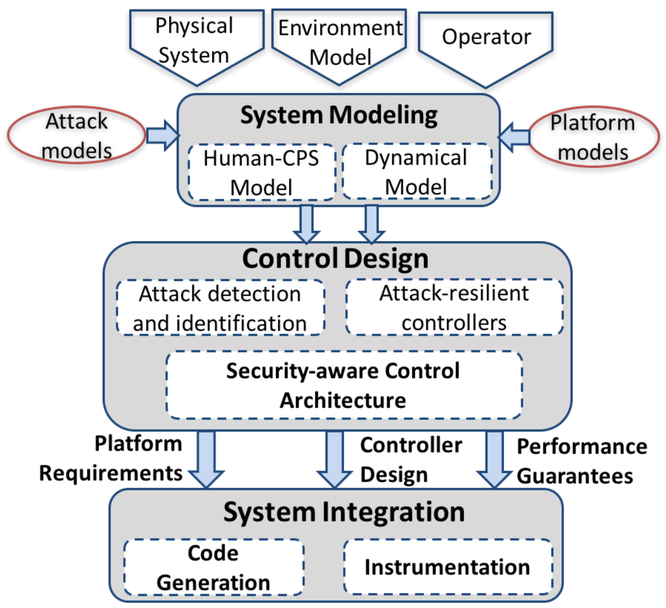
Constrained computation and communication resources limit the full use of developed cyber-physical techniques

Our Goal: Provide quantitative tradeoff procedure to map security-aware modules onto available architecture

[TCPS20, TASE21*, CSF21, ICCPS21, HSCC20, TECS17, RTSS17, CSM17]

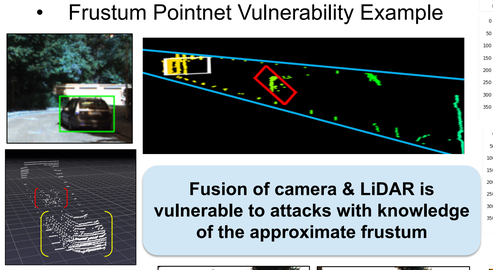
* Project Overview

- ***Goals of the project***: to develop the scientific foundation for secure control of cyber-physical systems (CPS)
- **High-assurance CPS design framework** in which the mix of resilient control, attack-detection, efficient execution monitoring and system recovery provides safety and performance guarantees even in the presence of attacks

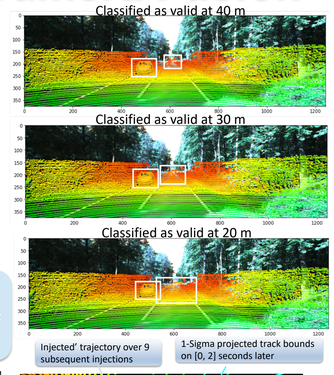


3 Attacks on LiDAR-Camera Fusion

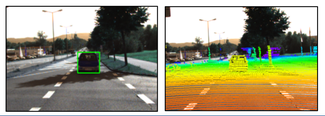
- Stealthy attacks on LiDAR
  - Visualizations in Camera Frame
- Attacks on Camera-Lidar Fusion
  - Frustum Pointnet Vulnerability Example

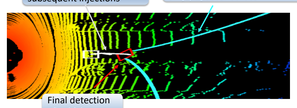


Fusion of camera & LiDAR is vulnerable to attacks with knowledge of the approximate frustum



Tracking Case Study: Vehicle Following





2 Secure Control of Human-CPS

- How to build human-aware cyber-physical systems?

Model-Based Methodology

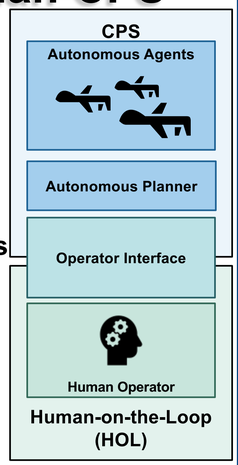
- Use formal methods to model system dynamics
- Capture human factors using data-driven models [**THMS19, HCI18**]
- Formalize requirements, and develop a framework to synthesize protocols [**CAV19, ICRA19**]

Study: Single-Operator Multi-UAV Systems

- ***Operator*** – sets goals, supervise, imagery tasks
- ***Automation*** – planning, trajectory following
- Malicious attacks on UAV sensors (spoofing GPS) to drive the UAV to undesired locations

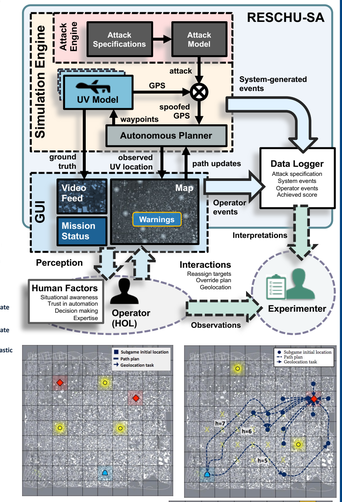
RESCHU-SA Testbed

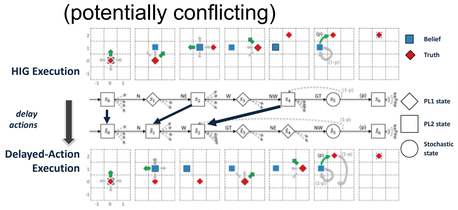
- Simulation environment for multi-UAV command and control
- Supports simulating smart attacks on GPS
- Extendable and open source

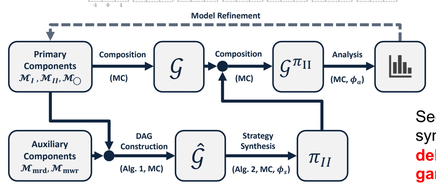


Security-Aware Control

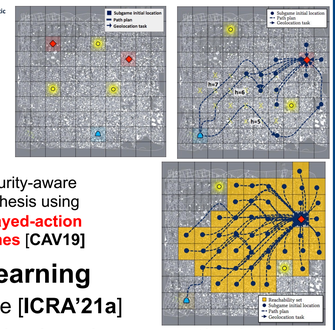
- From data, a Hidden Information game model is obtained
- Synthesis of security-aware HCPS control protocols [**CAV'19, ICRA'19**]
  - Trade-off Analysis – Time vs. Risk (potentially conflicting)







Security-aware synthesis using **delayed-action games** [**CAV19**]



Secure Planning via Model-Free Learning

- Against stealthy attacker with full knowledge [**ICRA'21a**]
- **Problem:** For a given task and the IDS mechanism, learn an optimal control strategy resilient to stealthy attacks on actuators
- Model as a zero-sum SG $\mathcal{G}$ with an LTL winning condition φ capturing
  - the controller task and IDS mechanism
  - the behavior of stealthy attackers
- Reduce the LTL objective $argmax_\mu\, min_\nu\, Pr_{\mu,\nu}(\mathcal{G} \vDash \varphi)$ to $argmax_\mu\, min_\nu\, \mathbb{E}_{\mu,\nu}[G_\varphi^\times]$ $argmax_\mu\, min_\nu\, \mathbb{E}_{\mu,\nu}\left[\sum_{i=0}^{\infty} \gamma^i r_{(i)}\right]$