2021 NSF CYBER-PHYSICAL SYSTEMS PRINCIPAL INVESTIGATORS' MEETING

Against Coordinated Cyber and Physical Attacks: Unified Theory and Technologies

Naira Hovakimyan[1](nhovakim@illinois.edu), Lui Sha[1], Petros Voulgaris[1], Xiaofeng Wang[2]

[1]University of Illinois at Urbana–Champaign, [2]University of Nevada, Reno, [3]University of South Carolina

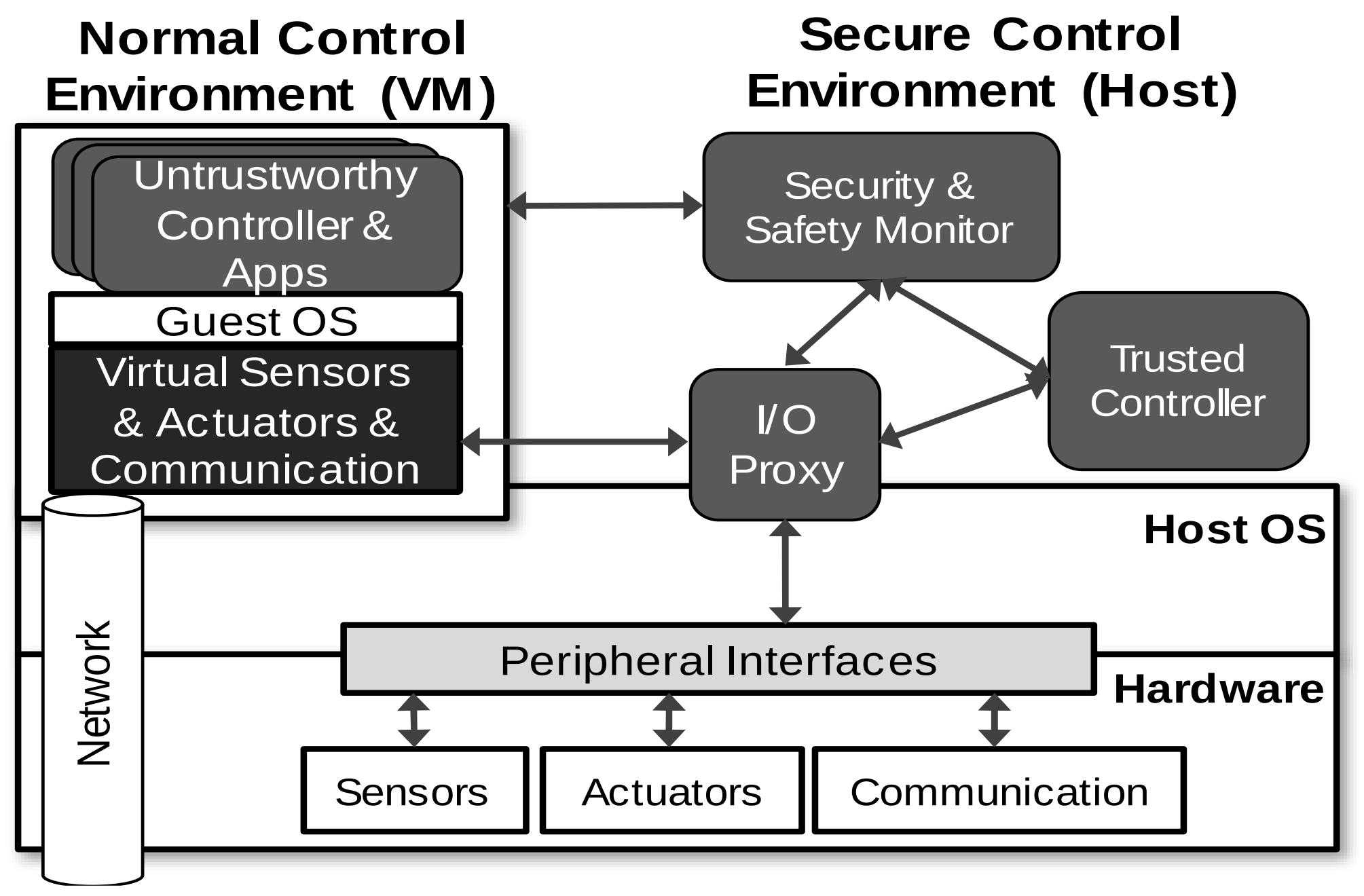
Challenge: Signal processing, robust fault tolerant control (RFTC) theory and software assurance technologies: developed under different assumptions and models

- Software assurance technologies: model-based, require no changes in the profile of the physical dynamics and observations.
- RFTC techniques: compensate for the physical damage, assuming control software and sensor data are not compromised.

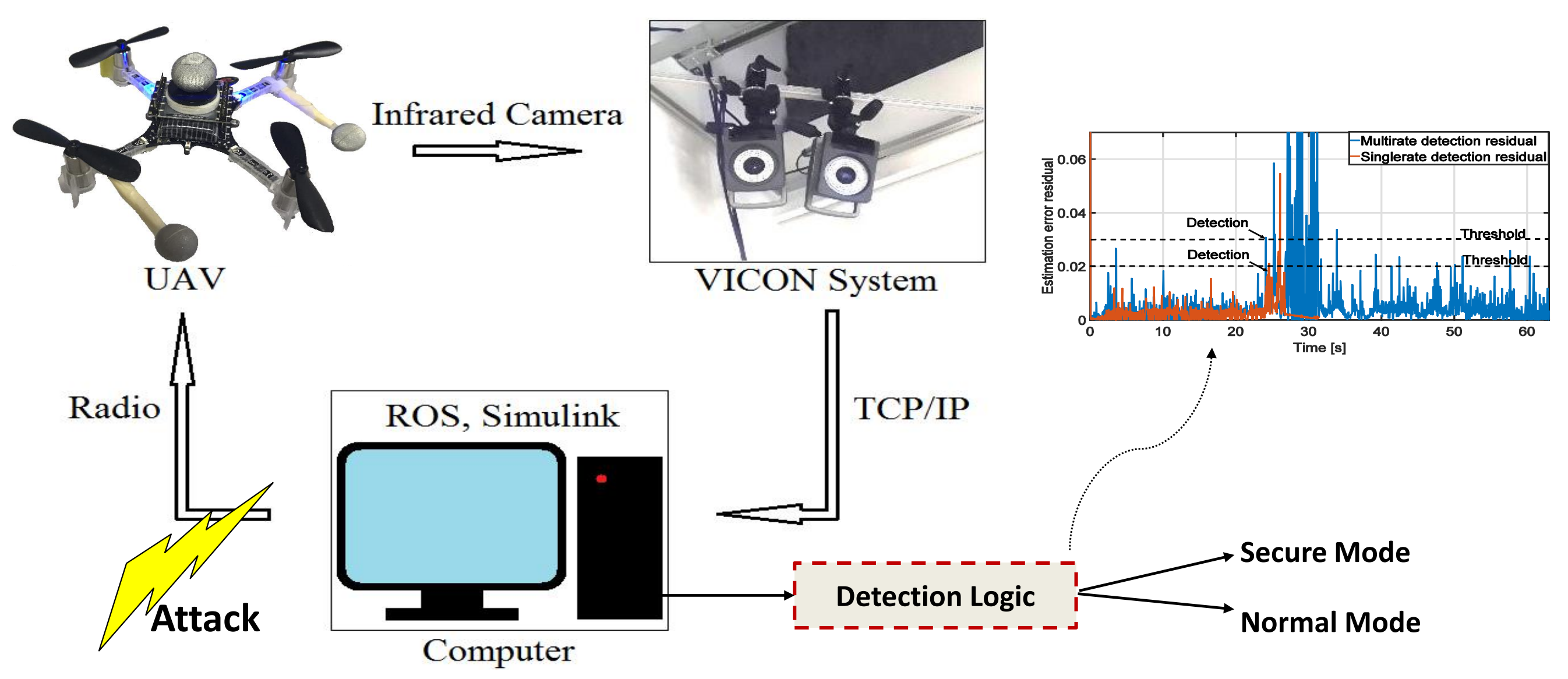
Goal: Unified models and techniques with coherent set of assumptions, supported by integrated technologies that can defend against Coordinated Cyber-Physical Attacks (CCPAs)

CPS Engineering: develop attack-resilient Simplex (ARSimplex) architecture:

- ➢ Normal Control Environment: it runs software components for any normal function.
- ➢ Secure Control Environment: it runs a minimal set of software components that are critically required to control the physical system.
- ➢ Secure Controller: it extends the $\mathcal{L}1$ adaptive control theory to multi-rate sampled-data framework for the purpose of compensation for uncertainties and adaptation to failures, and detection of cyber and physical failures/attacks.

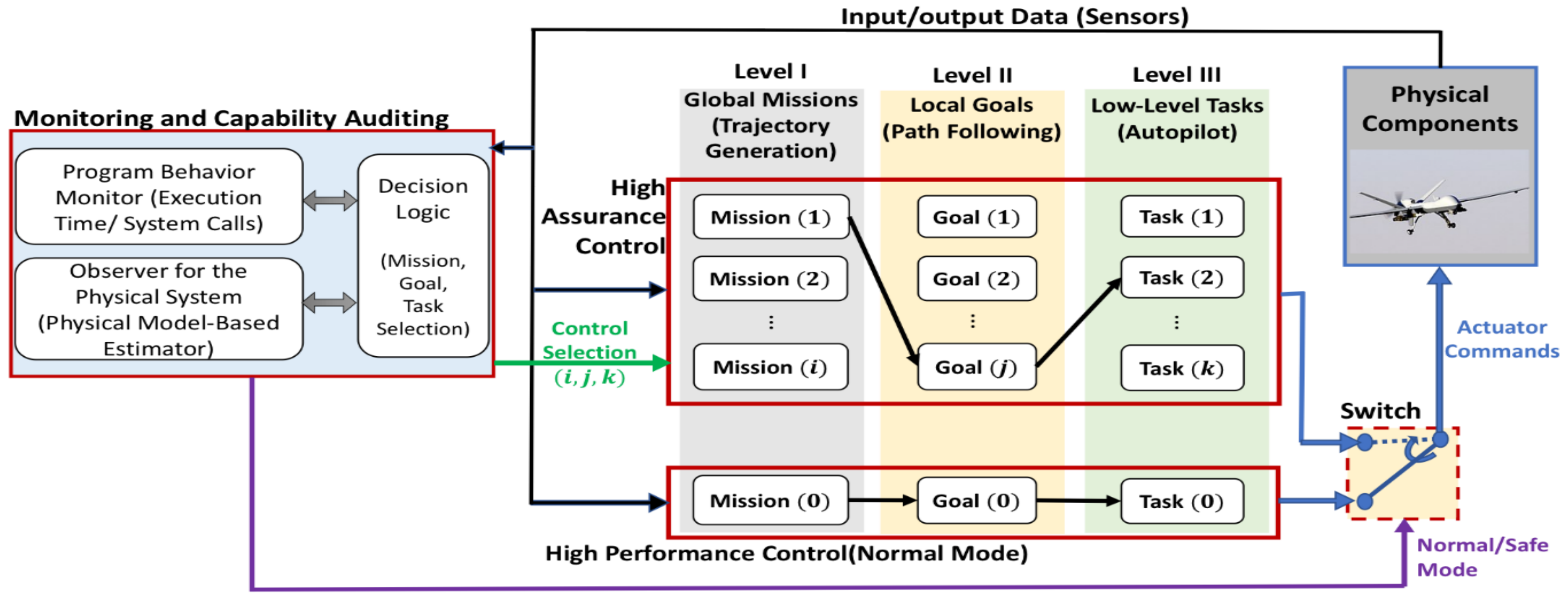

Normal Control Environment (VM)
Secure Control Environment (Host)
Untrustworthy Controller & Apps
Guest OS
Virtual Sensors & Actuators & Communication
Security & Safety Monitor
I/O Proxy
Trusted Controller
Host OS
Network
Peripheral Interfaces
Hardware
Sensors
Actuators
Communication

ARSimplex Architecture .



UAV flight test setup at the Intelligent Robotics Lab (IRL) at UIUC.

CPS Technology: *to address zero-day emergencies due to CCPA*, a multilevel control framework is designed for UAVs' adaptation of high-level missions, local goals, and low-level control tasks to uncertainties.


Input/output Data (Sensors)
Monitoring and Capability Auditing
Program Behavior Monitor (Execution Time/ System Calls)
Observer for the Physical System (Physical Model-Based Estimator)
Decision Logic
(Mission, Goal, Task Selection)
High Assurance Control
Control Selection
(i, j, k)
Level I
Global Missions (Trajectory Generation)
Level II
Local Goals (Path Following)
Level III
Low-Level Tasks (Autopilot)
Physical Components
Mission (1)
Mission (2)
Mission (i)
Goal (1)
Goal (2)
Goal (j)
Task (1)
Task (2)
Task (k)
Mission (0)
Goal (0)
Task (0)
Actuator Commands
Switch
Normal/Safe Mode
High Performance Control(Normal Mode)

CPS Science: characterize the generic conditions for the detectability and the policy of coordinated stealthy attacks: intermittent zero-dynamics attack, cooperative zero-dynamics attack, cyber and physical topology attacks, and Denial-of-Service attack.

[1]UIUC, [2]UofSC,
ECCS-1739732, ECCS-1739886
08/31/2019 – 8/31/2021