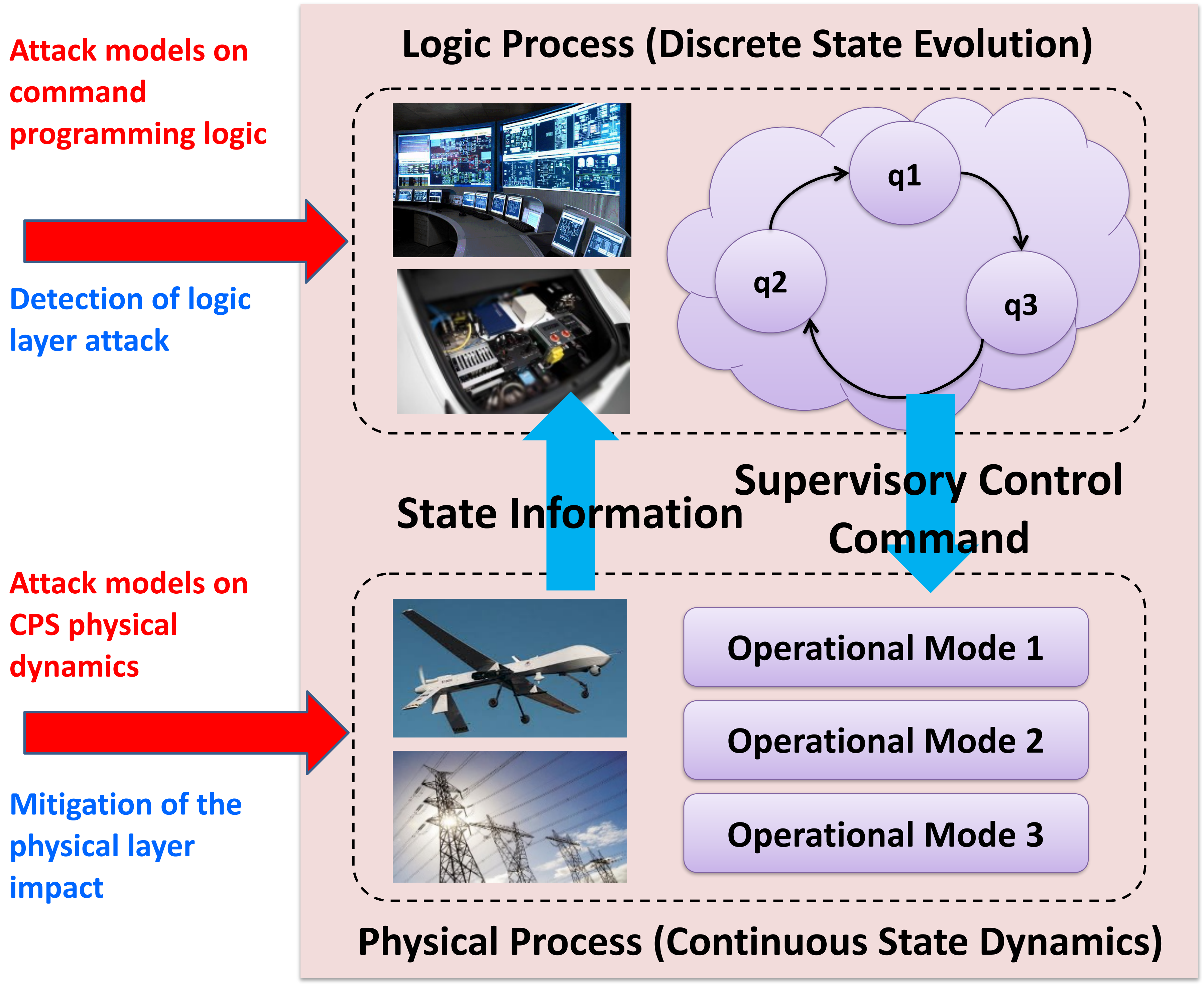
CERIAS
The Center for Education and Research in Information Assurance and Security

Resilient Control Designed for CPS: a Hybrid System Approach

Dawei Sun and Inseok Hwang

In our ongoing research, we model the CPS subject to cyber-attacks as a hybrid system so that it can account for both the switching attack that tampers the discrete state dynamics (logical behavior) and the data injection attack which compromises the continuous state dynamics (physical behavior) of the CPS. Specifically, the identifiability and severity of the joint attacks are first analyzed, and a unified resilient hybrid control scheme is proposed to mitigate the impact of faults/attacks.

Hybrid System Modeling of CPS and Faults/Attacks


Attack models on command programming logic

Detection of logic layer attack

Attack models on CPS physical dynamics

Mitigation of the physical layer impact

Logic Process (Discrete State Evolution)

State Information

Supervisory Control Command

Operational Mode 1

Operational Mode 2

Operational Mode 3

Physical Process (Continuous State Dynamics)

The CPSs are generally designed to operate at different conditions. From this perspective, the hybrid system approach is a powerful tool for CPS security analysis: it can address both **the higher level supervisory control logic** and **physical layer dynamics**. With hybrid system approach, the cyber-attacks that temper the logic behavior of the CPS and the cyber attacks that are modeled on the physical dynamics of the CPS can be analyzed within the unified framework.

Problem Formulation

Abstraction of Hybrid CPS

- **Continuous State Dynamics**

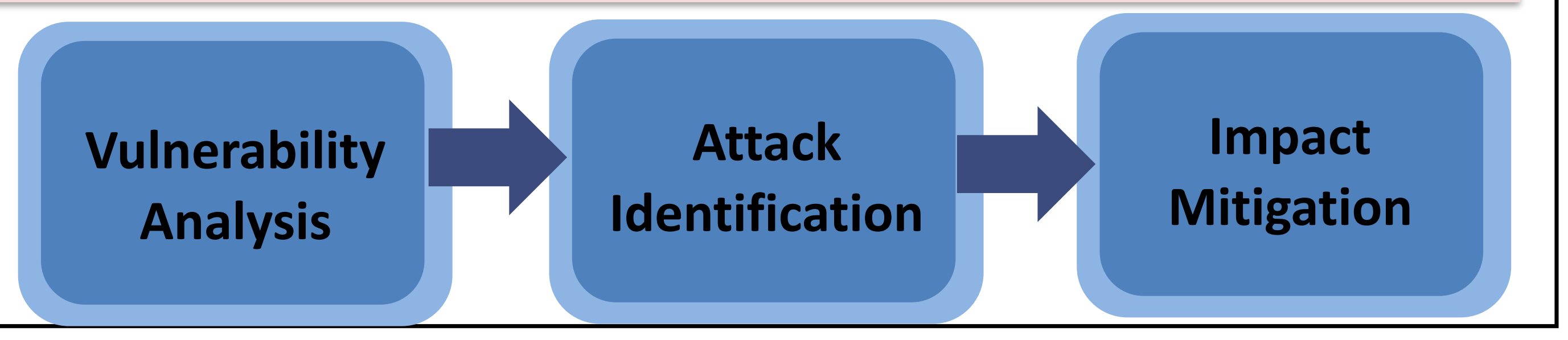
Physical States Control Inputs Attacker's Input

- **Discrete State Dynamics**

Supervisory Control

Attacker's Input

Resilient Scheme Design Process:

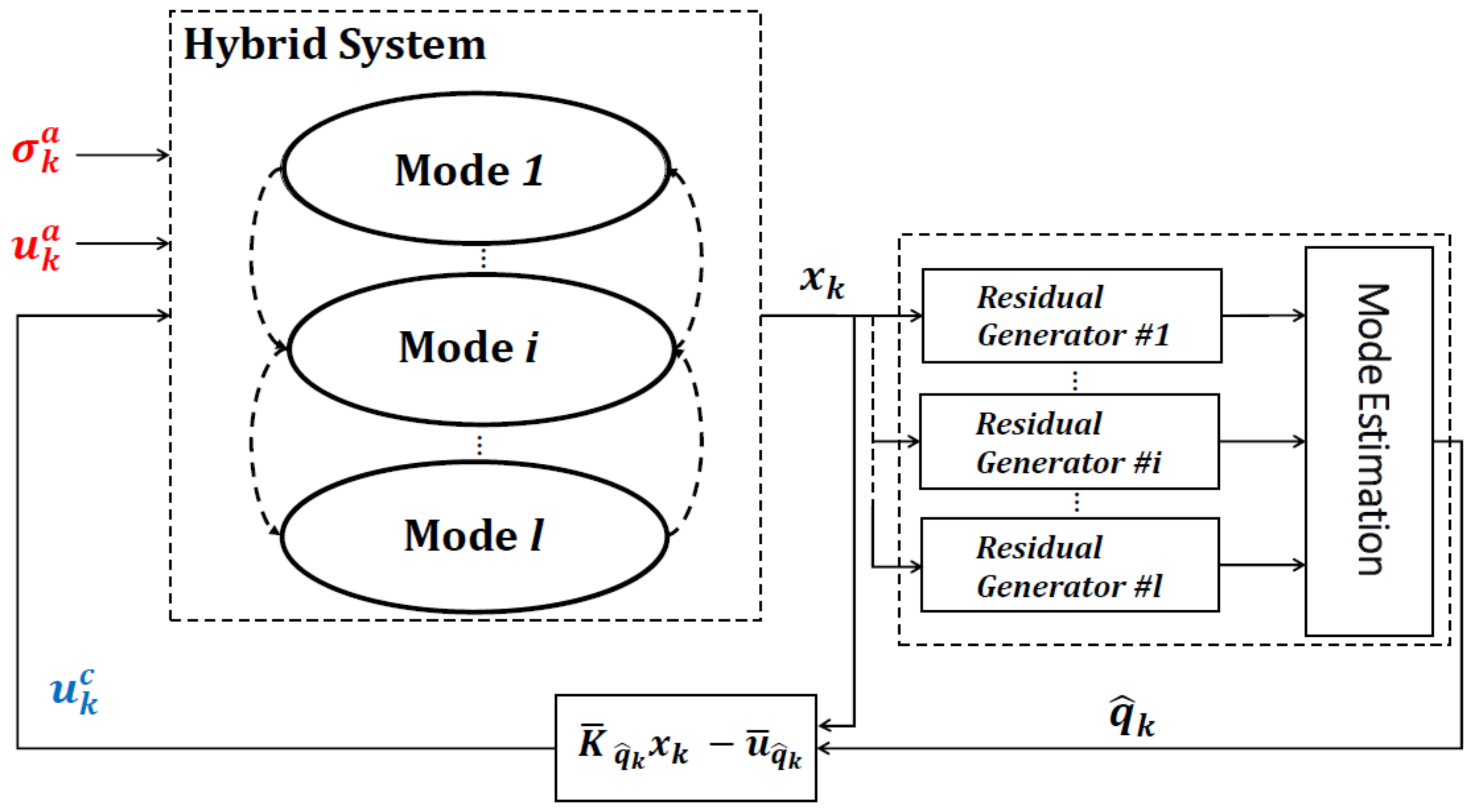

Vulnerability Analysis

Attack Identification

Impact Mitigation

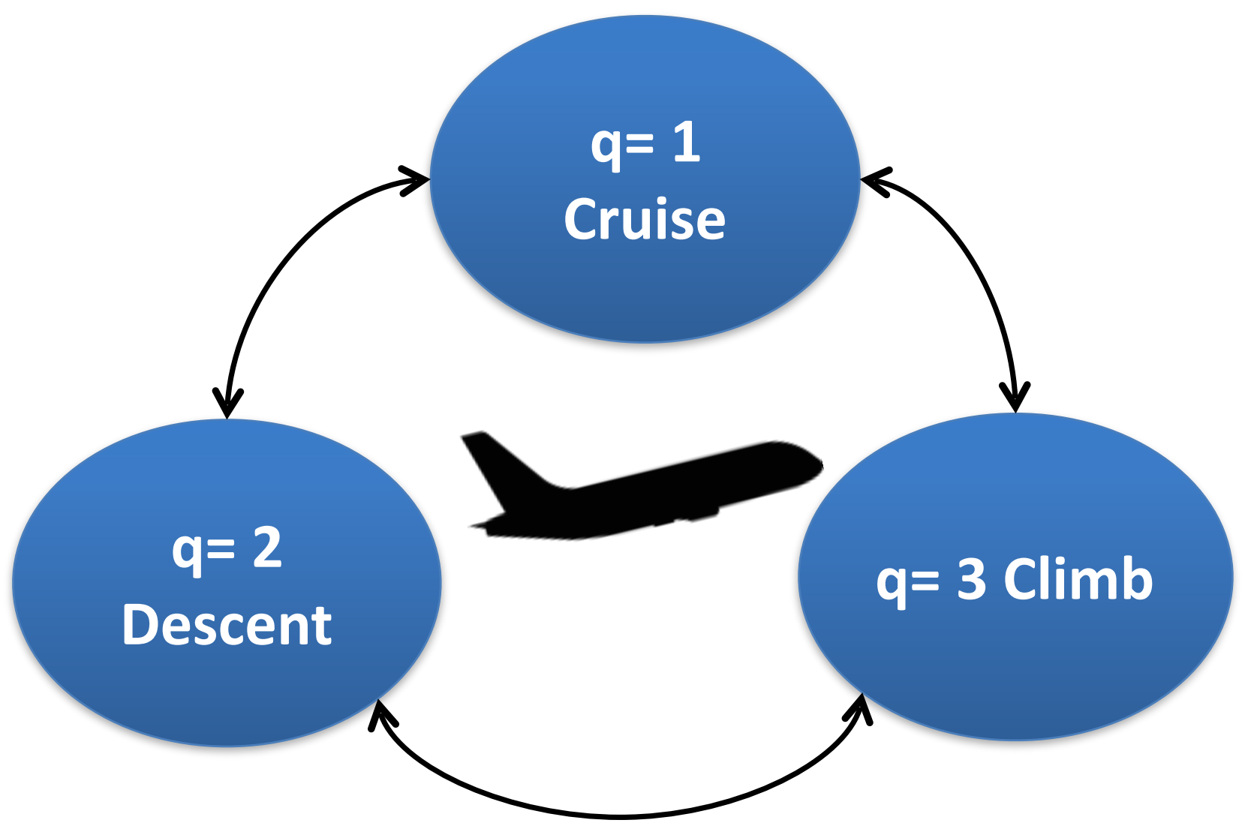
Assured Attack Containment Scheme

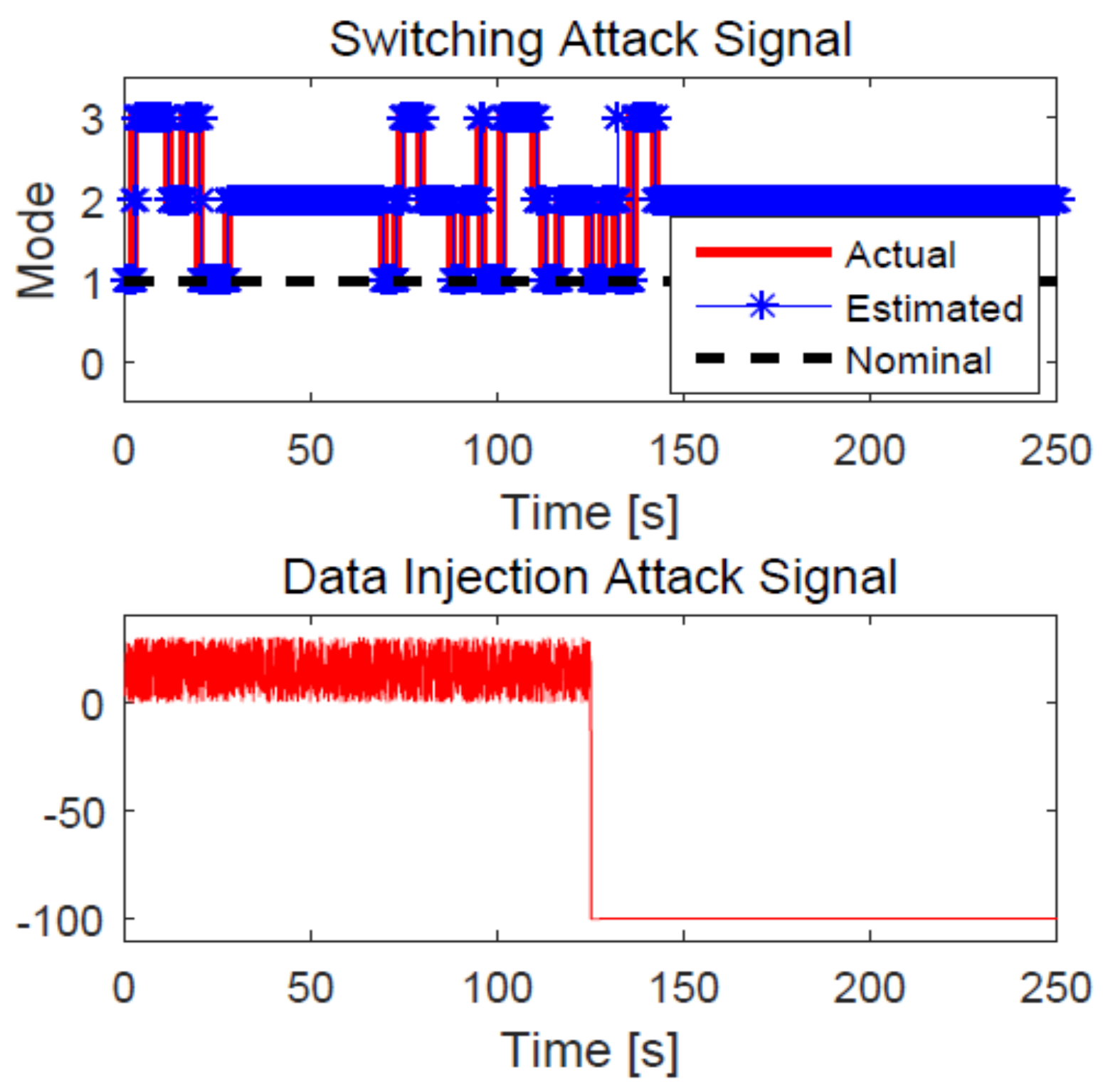
- **Monitoring system design**: based on the analysis of attack, the algorithm is designed to detect and identify the attack
- **Resilient control design**: the resilient control is designed to mitigate the physical impact of the cyber-attack

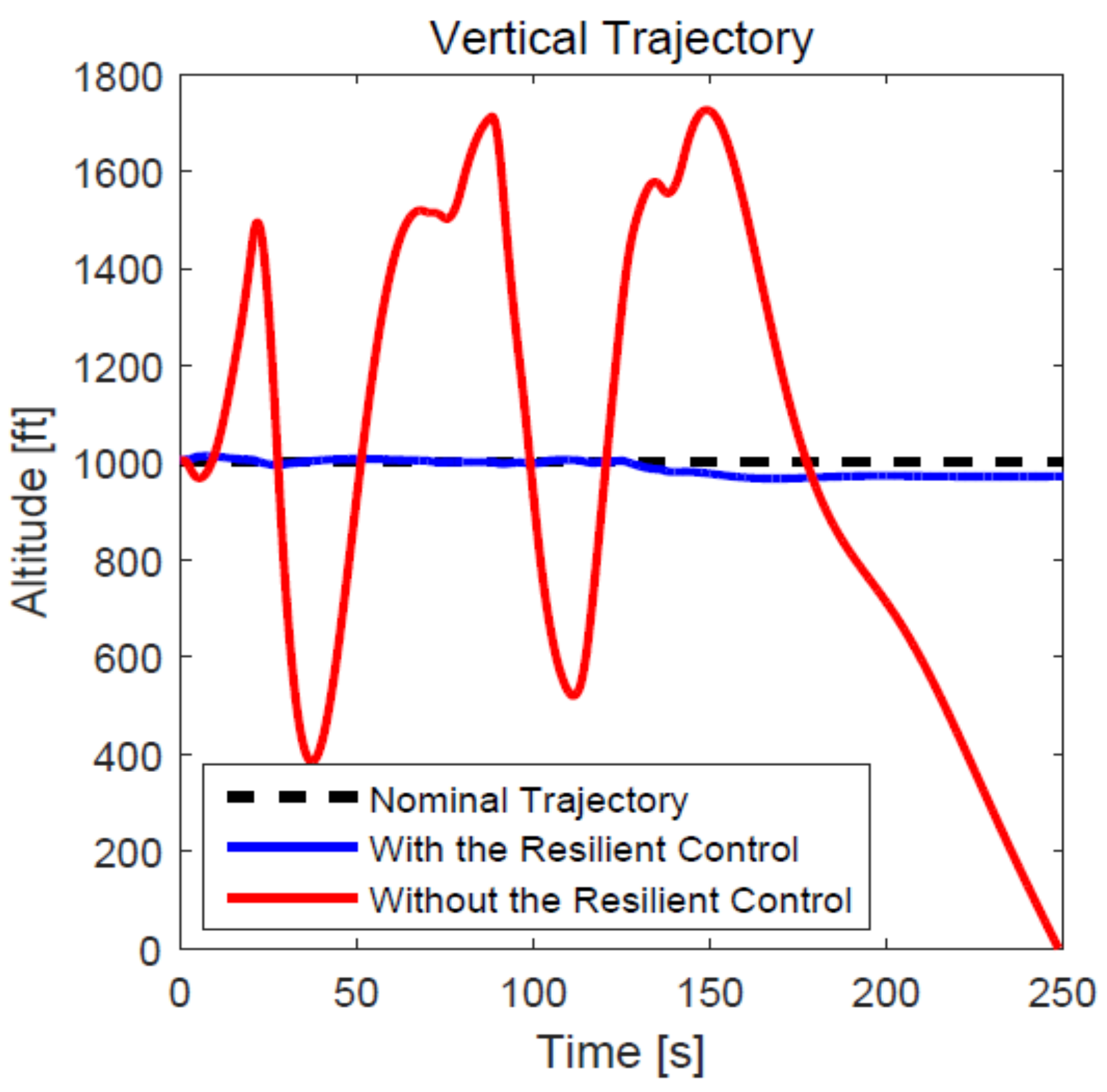


•Example: Unmanned Aircraft System

In the simulated scenario, the attacker injects the fault signal to the UAS motor and adversely switches the flight mode simultaneously. The developed algorithm is able to detect the adverse switchings and mitigate the deviation in the UAS flight trajectory.







PURDUE UNIVERSITY Discovery Park

Acknowledgement: This work is part of the project titled *Towards Cyber-Physical Vetting of Critical Infrastructures* supported by *the Discovery Park Big Idea Challenge*

CERIAS