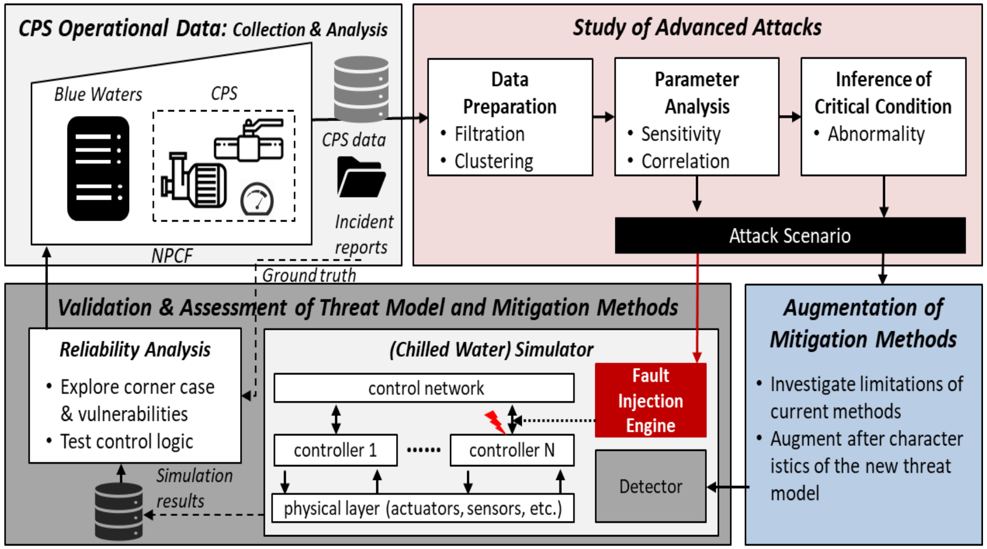
Data-Driven Study of Attacks on Cyber-Physical Infrastructure Supporting Large Computing Systems

Challenge:

- **To detect** attacks deployed with self-learning malware
- **To detect and distinguish** attacks from random failures
- **To devise and validate** the protection mechanisms by using real operational data


CPS Operational Data: Collection & Analysis
Blue Waters
CPS
NPCF
CPS data
Incident reports
Study of Advanced Attacks
Data Preparation
• Filtration
• Clustering
Parameter Analysis
• Sensitivity
• Correlation
Inference of Critical Condition
• Abnormality
Attack Scenario
Ground truth
Validation & Assessment of Threat Model and Mitigation Methods
Reliability Analysis
• Explore corner case & vulnerabilities
• Test control logic
Simulation results
(Chilled Water) Simulator
control network
controller 1
controller N
physical layer (actuators, sensors, etc.)
Fault Injection Engine
Detector
Augmentation of Mitigation Methods
• Investigate limitations of current methods
• Augment after characteristics of the new threat model

Solution: A 4-stage approach

- Analyze CPS operational data
- Study potential innovation in security attacks
- Devise mitigation and detection methods
- Validate, assess, and hardening of the CPS

Scientific Impact:

- ***Scientifically sound methods*** to jointly study reliability failures and malicious attacks against a CPS critical for the uninterruptible operation of a large computing infrastructure.
- ***Demonstration of new advanced attacks*** which take advantage of machine learning to develop and execute an attack strategy
- ***Define principles*** for detecting advanced attacks
- ***A data-driven simulation testbed*** that emulates the CPS behavior and enables experimentation with representative attack scenarios

Broader Impact:

- **Identify advances in security threats** by demonstrating the feasibility of masquerading a security attack as a reliability failure
- **Improve the security of CPSes** and provide an effective methodology for in-depth monitoring for improved resiliency
- **Application of the proposed approach to** CPSes in other domains (e.g., robots, AVs) to eliminate security risks

Award ID: 18-16673

University of Illinois at Urbana-Champaign
Contacts: **Z. Kalbarczyk** (kalbarcz@Illinois.edu) and R. K. Iyer (rkiyer@Illinois.edu)