Indirect Cyber Attacks: Case for Targeted Change of Environmental Control to Compromise Large Computing Infrastructure

Zbigniew Kalbarczyk

In collaboration with: K. Chung, V. Formicola, A. Withers, A. Slagell, R. Iyer

ECE ILLINOIS

ILLINOIS

Threat of Indirect Cyber Attacks against Critical Assets

- **Significant dependency of computing infrastructures (e.g., HPC and cloud) on CPS that monitors and controls operational environment**
  - CPS can become a stepping stone for attacking a target that relies on that CPS services
  - relatively weak CPS security becomes an entry point of an attack
  - limited visibility and control over the CPS from the "dependent" target system
- **Distinguishing attacks from random failures**
  - masquerading a security attack as an accidental failure reduces attack visibility and chances for timely detection
- **Detecting attacks deployed with self-learning malware**
  - in presence of information to learn from the malware can self-develop or evolve
  - hard to detect malware that causes behavior similar to an accidental failure

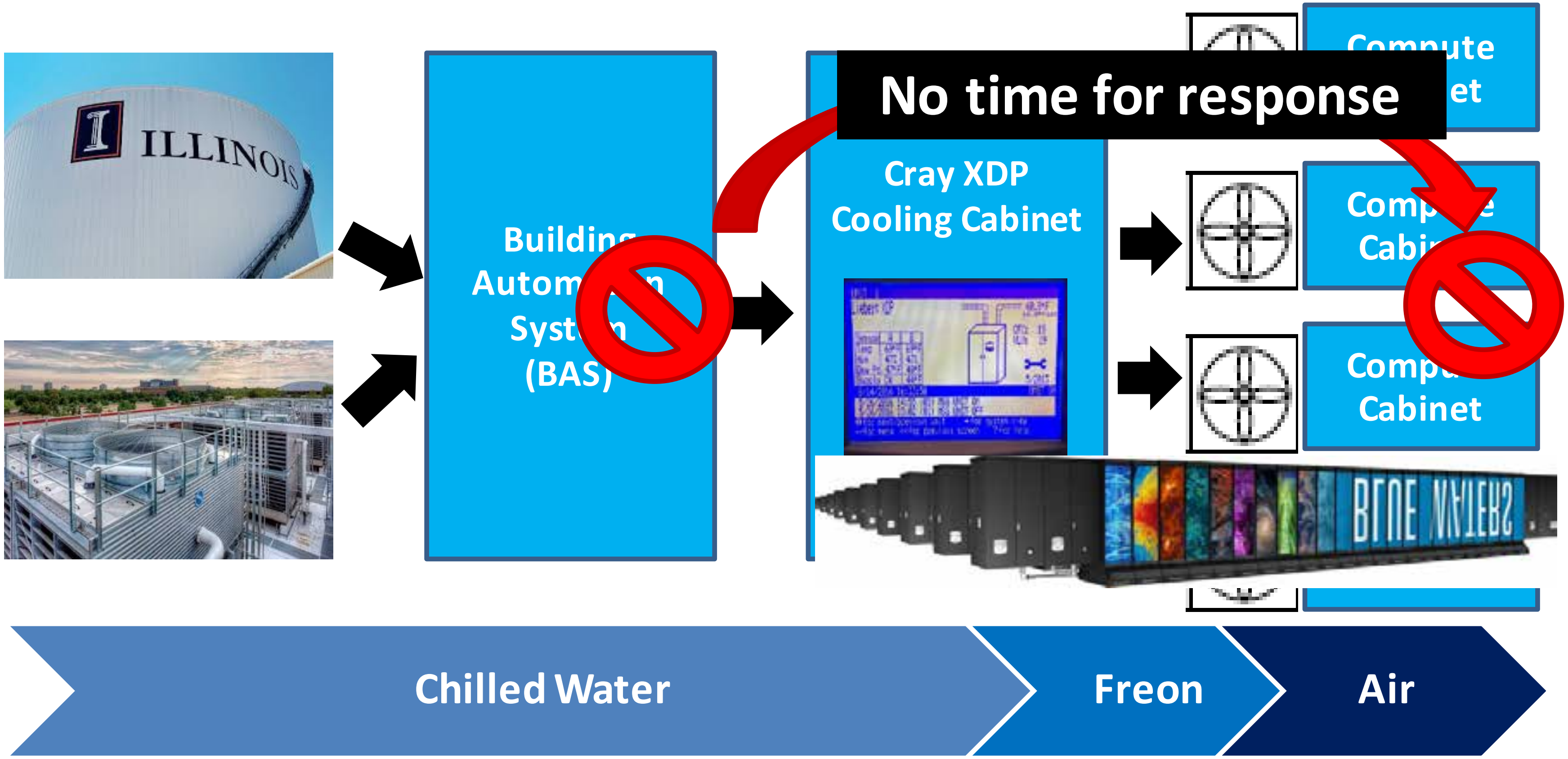
Attack Model

- An indirect attack on a large computing infrastructure through alteration of the CPS responsible for the cooling of the computing assets
  - computing Infrastructure itself well-hardened against attacks
  - relatively weak security of CPS responsible for the environment control

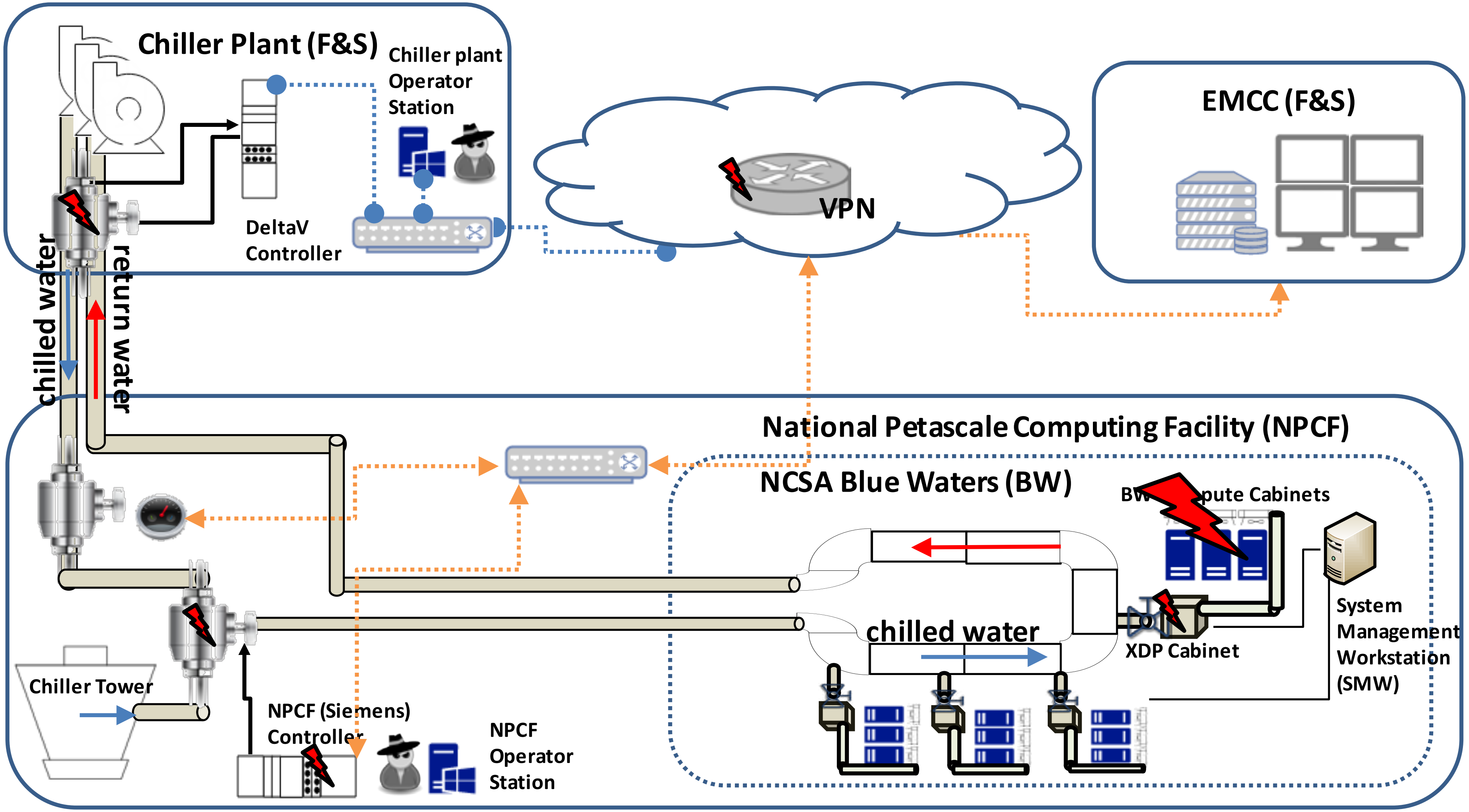
- Masquerade as an accidental failure
  - study data on past accidental failures and make an attack to emulate similar failure scenarios
  - minimize attack traces

Target System

- Blue Waters (BWs), petascale supercomputer at University of Illinois for groundbreaking research (e.g., weather forecast , earthquakes, or genomics)
- Building Automation System (BAS) controlling the environmental parameters of the National Petascale Computing Facility (NPCF, a 20,000 square foot machine room), which houses Blue Waters



Blue Waters Supercomputer and Cooling System

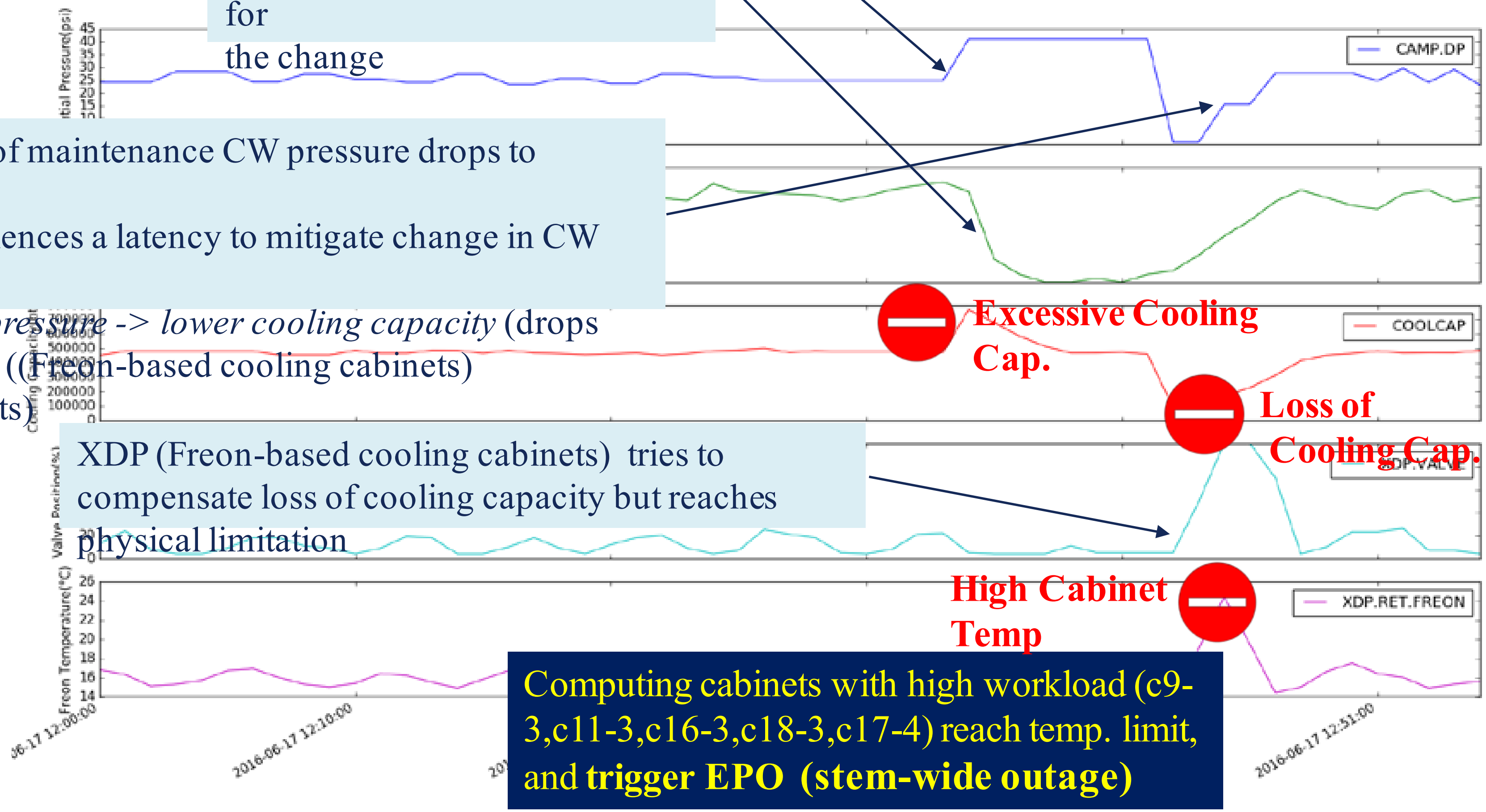


Attack Entry Points

- Compromise operator machines to access facility control system
- Network vulnerable to man-in-the-middle (MITM) attacks
  - an attacker can alter data packets to manipulate the sensors as well as the control commands sent to the cyber-physical system
- Attack set points for the water flow, control water temperature, and hid (from the operator) actual temperature values
  - operational parameters and control logic typically configured through set points and project files located on operator consoles
- Indirect attacks can be performed by targeting the NPCF control system, by aiming at the chilling pumps in the tower and in the inlet water pipe

What the Data on Blue Waters Failures Tell?

Example real failure scenario: **Change in Chilled Water Pressure**



Campus Facilities and Services perform maintenance process cause an increase in CW pressure

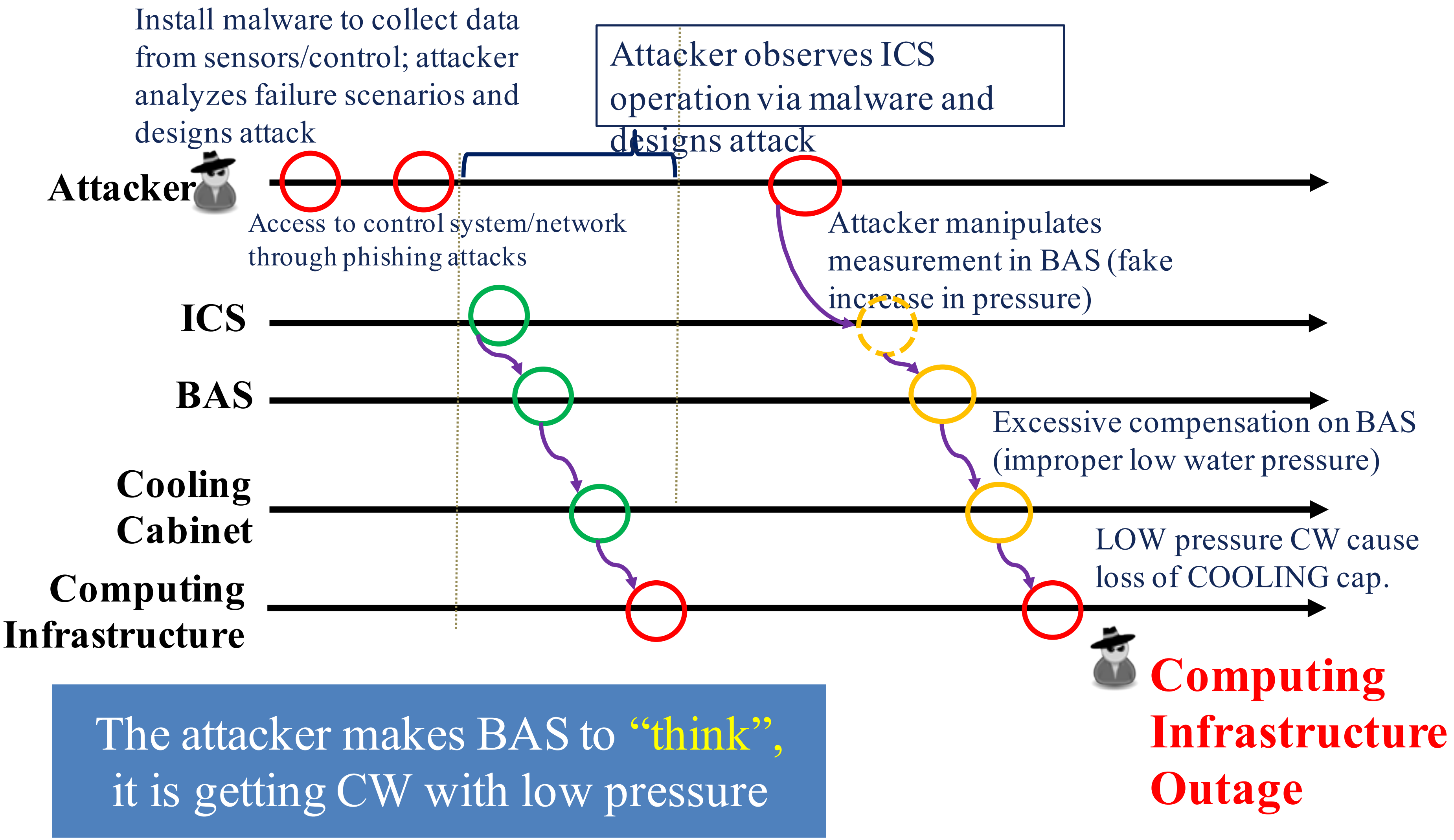
BAS closes the valve to mitigate for
the change

- At the end of maintenance CW pressure drops to normal;
- BAS experiences a latency to mitigate change in CW pressure;
- *lower CW pressure -> lower cooling capacity* (drops below XDP ((Freon-based cooling cabinets) requirements)

XDP (Freon-based cooling cabinets) tries to compensate loss of cooling capacity but reaches physical limitation

Computing cabinets with high workload (c9-3,c11-3,c16-3,c18-3,c17-4) reach temp. limit, and **trigger EPO (stem-wide outage)**

Mimic An Accidental Failure to Masquerade An Attack



Install malware to collect data from sensors/control; attacker analyzes failure scenarios and designs attack

Attacker observes ICS operation via malware and designs attack

Attacker

Access to control system/network through phishing attacks

Attacker manipulates measurement in BAS (fake increase in pressure)

ICS

BAS

Excessive compensation on BAS (improper low water pressure)

Cooling Cabinet

LOW pressure CW cause loss of COOLING cap.

Computing Infrastructure

Computing Infrastructure Outage

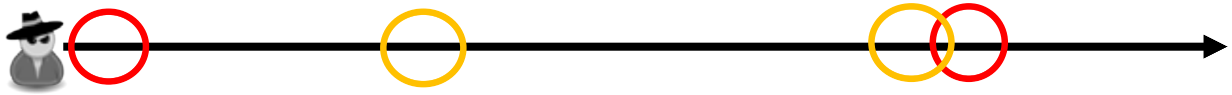
The attacker makes BAS to "think", it is getting CW with low pressure

Simulator

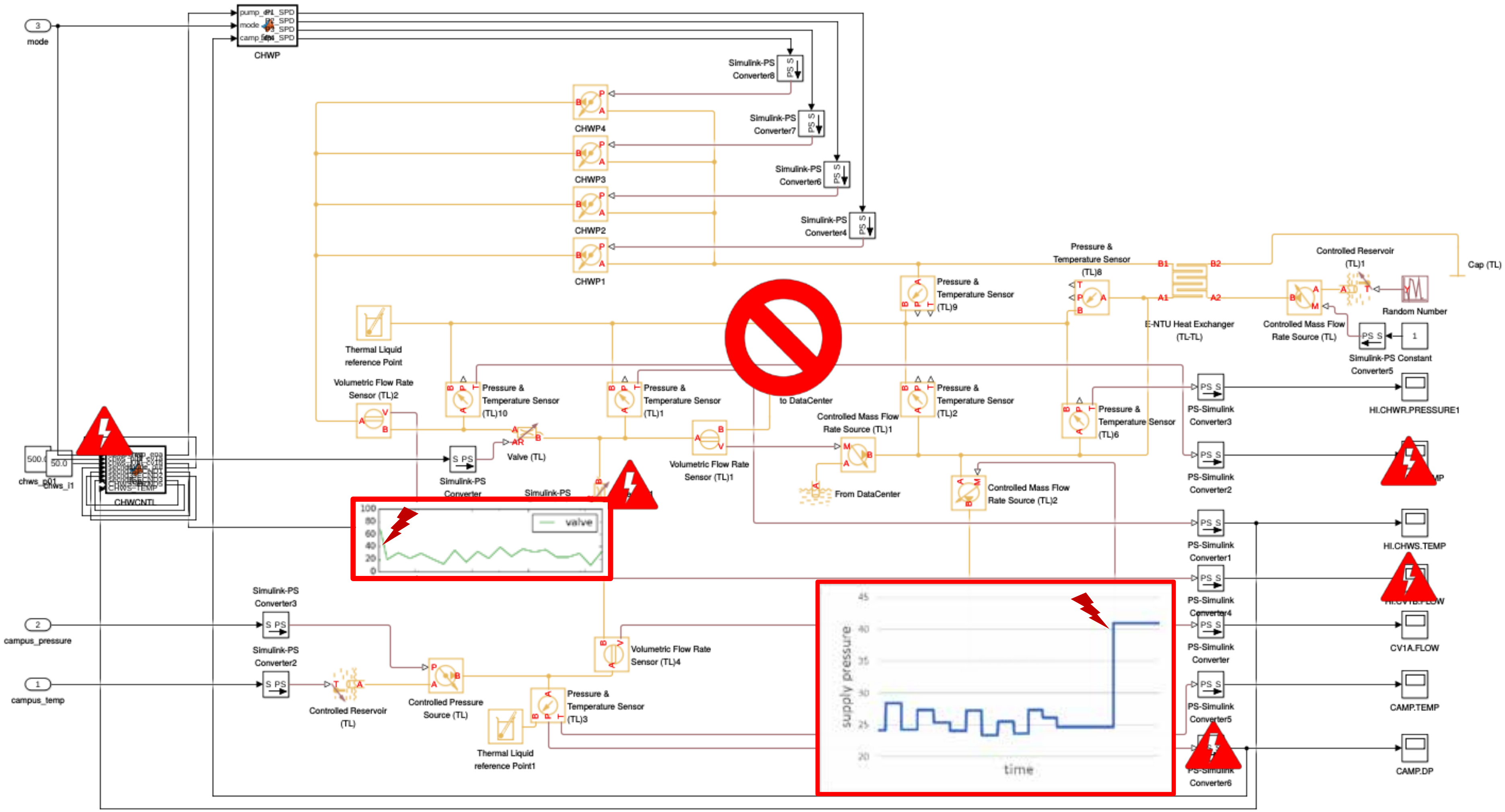
- Model CPS that controls supply of cooling water to the computing infrastructure
    - Metlab based simulator
- Date-driven simulation
    - Data defines physical parameters of the input chill water fed into the cooling system
    - Mimic operation and control flow of a real system
- Enable evaluation of effectiveness of attacks and mitigation mechanisms

Example: Mimic An Accidental Failure to Masquerade An Attack

Attack



Attacker manipulates measurement (fake increase in pressure) [illegible]



mode
campus_pressure
campus_temp
CHWP
CHWP1
CHWP2
CHWP3
CHWP4
Simulink-PS Converter4
Simulink-PS Converter6
Simulink-PS Converter7
Simulink-PS Converter8
Thermal Liquid reference Point
Volumetric Flow Rate Sensor (TL)2
Pressure & Temperature Sensor (TL)10
Pressure & Temperature Sensor (TL)1
Pressure & Temperature Sensor (TL)9
Pressure & Temperature Sensor (TL)8
Pressure & Temperature Sensor (TL)2
Pressure & Temperature Sensor (TL)6
Pressure & Temperature Sensor (TL)3
Valve (TL)
to DataCenter
From DataCenter
Controlled Mass Flow Rate Source (TL)1
Controlled Mass Flow Rate Source (TL)2
Controlled Mass Flow Rate Source (TL)
Volumetric Flow Rate Sensor (TL)1
Volumetric Flow Rate Sensor (TL)4
E-NTU Heat Exchanger (TL-TL)
Controlled Reservoir (TL)1
Controlled Reservoir (TL)
Cap (TL)
Random Number
Simulink-PS Constant Converter5
Controlled Pressure Source (TL)
Thermal Liquid reference Point1
CHWCNTL
chws_p01
chws_i1
PS-Simulink Converter1
PS-Simulink Converter2
PS-Simulink Converter3
PS-Simulink Converter4
PS-Simulink Converter5
PS-Simulink Converter6
HI.CHWR.PRESSURE1
HI.CHWS.TEMP
CV1A.FLOW
CAMP.TEMP
CAMP.DP
valve
100
80
60
40
20
0
supply pressure
45
40
35
30
25
20
time

Summary

- Significant dependency of computing infrastructures (e.g., HPC and cloud) on CPS that monitors and controls operational environment
- Indirect attacks can be launch through the CPS
  - An attack can cause a failure of a computing infrastructure (including a *system-wide outage*) without touching the computing elements but instead manipulating vulnerable cyber-physical infrastructure of the facility
  - An attack masqueraded as an accidental failure
- Self-learning malware plausible way of deploying indirect attacks against computing infrastructures

- Identify design/configuration/implementation flaws
- Drive design of more efficient detection, e.g., monitors/detectors placement
- CPS security should be an integral part of the design process of a computing infrastructure