iTrust
Centre for Research
in Cyber Security

SINGAPORE UNIVERSITY OF
TECHNOLOGY AND DESIGN

Challenges in Avoiding Process Anomalies in Critical Infrastructure

2nd Workshop on Cyber-Physical Systems Se
curity and Resilience (CPS-SR)
Montreal, Canada

Aditya Mathur

Professor and Center Director, iTrust

Center for Research in Cyber Security

Singapore University of Technology and Design

Professor of Computer Science,

Purdue University, West Lafayette, IN, USA

April 15, 2019

Question

To what extent, and how, can we avoid anomalies in operational critical infrastructure?

Tour Guide

A. Context

B. Anomalies

C. Detection

D. Command Validation

E. Experimental Evaluation

F. Next Steps

A. Context

A Distributed CI

Attack point

Level 2

Historian

SCADA

Management Systems

Firewall

NIDS

Switch

Level 1

Controller [PLC]

Controller [PLC]

Controller [PLC]

Level 0

S

A

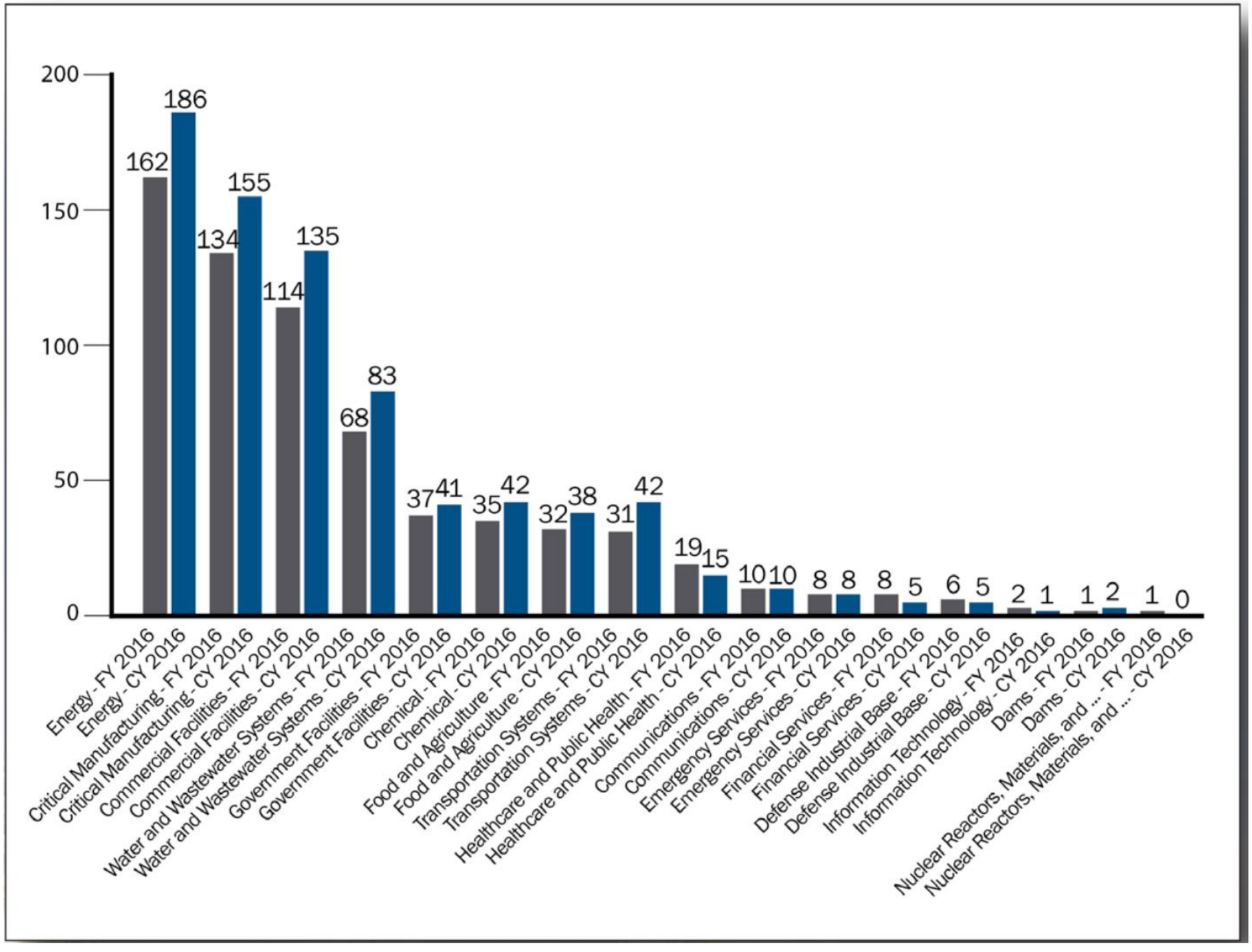
S

A

S

A

ICS-CERT Annual Vulnerability Coordination Report 2016



Tools for Invasion

Ransomware

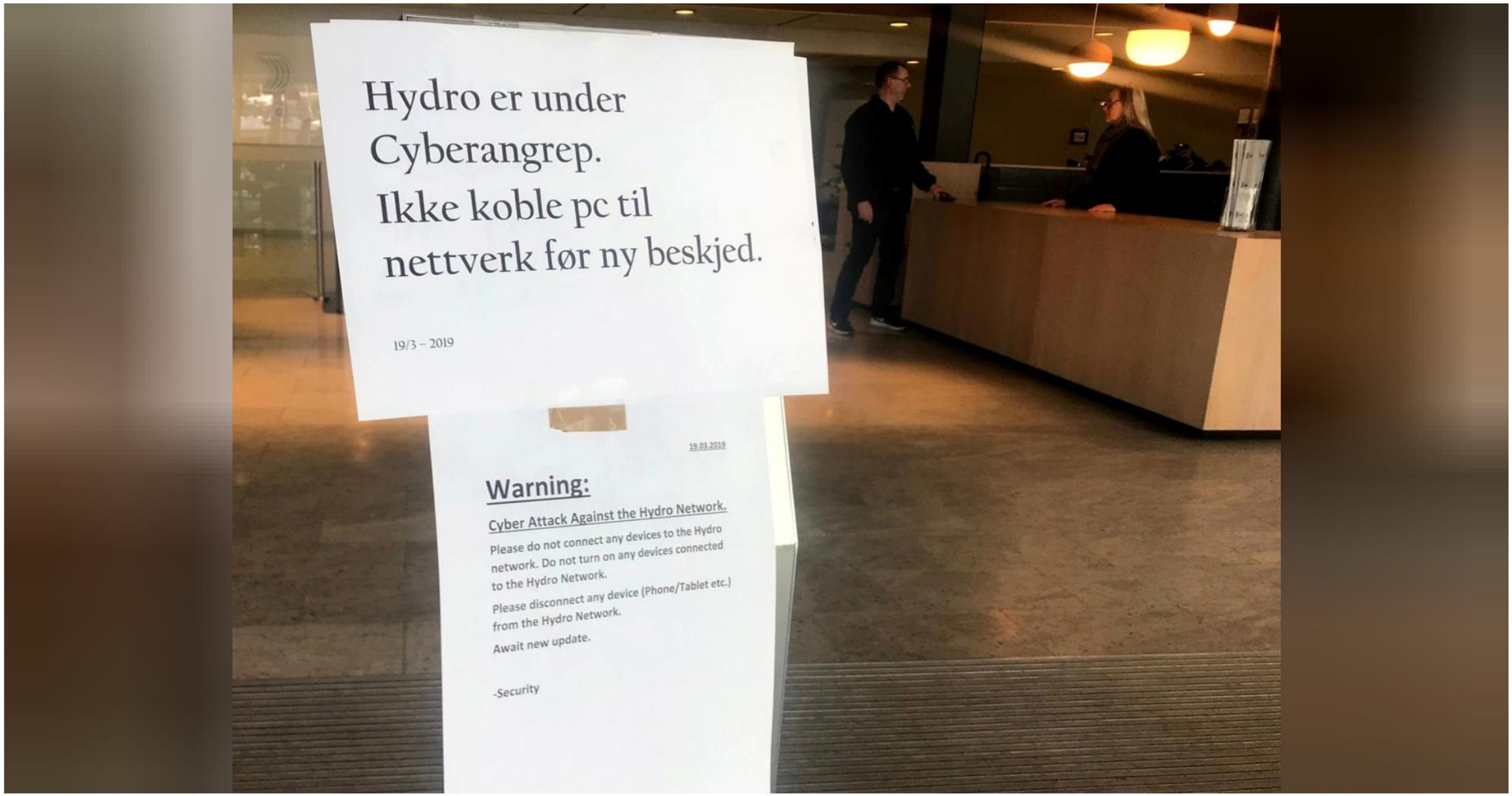
Malware

Virus

Social Engineering! → The Physical and Virtual insider!

Most potent threat

A Recent Successful Attack: 2019 Norsk Hydro



Critical Infrastructure: Interconnection

Water Treatment

Water Distribution

Electric power generation, transmission, distribution, AMI

B. Anomalies

Process anomaly

q_i : plant state at time t=i

Valid state sequence:

$$q_{-k}\, q_{-k+1}\, q_{-k+2} \cdots q_{-1}\, q_0\, q_1\, q_2 \cdots$$

Anomalous state sequence:

$$q_{-k}\, q_{-k+1}\, q_{-k+2} \cdots q_{-1}\, \underbrace{q'_0\, q'_1\, q'_2 \cdots}$$

Anomalous sequence

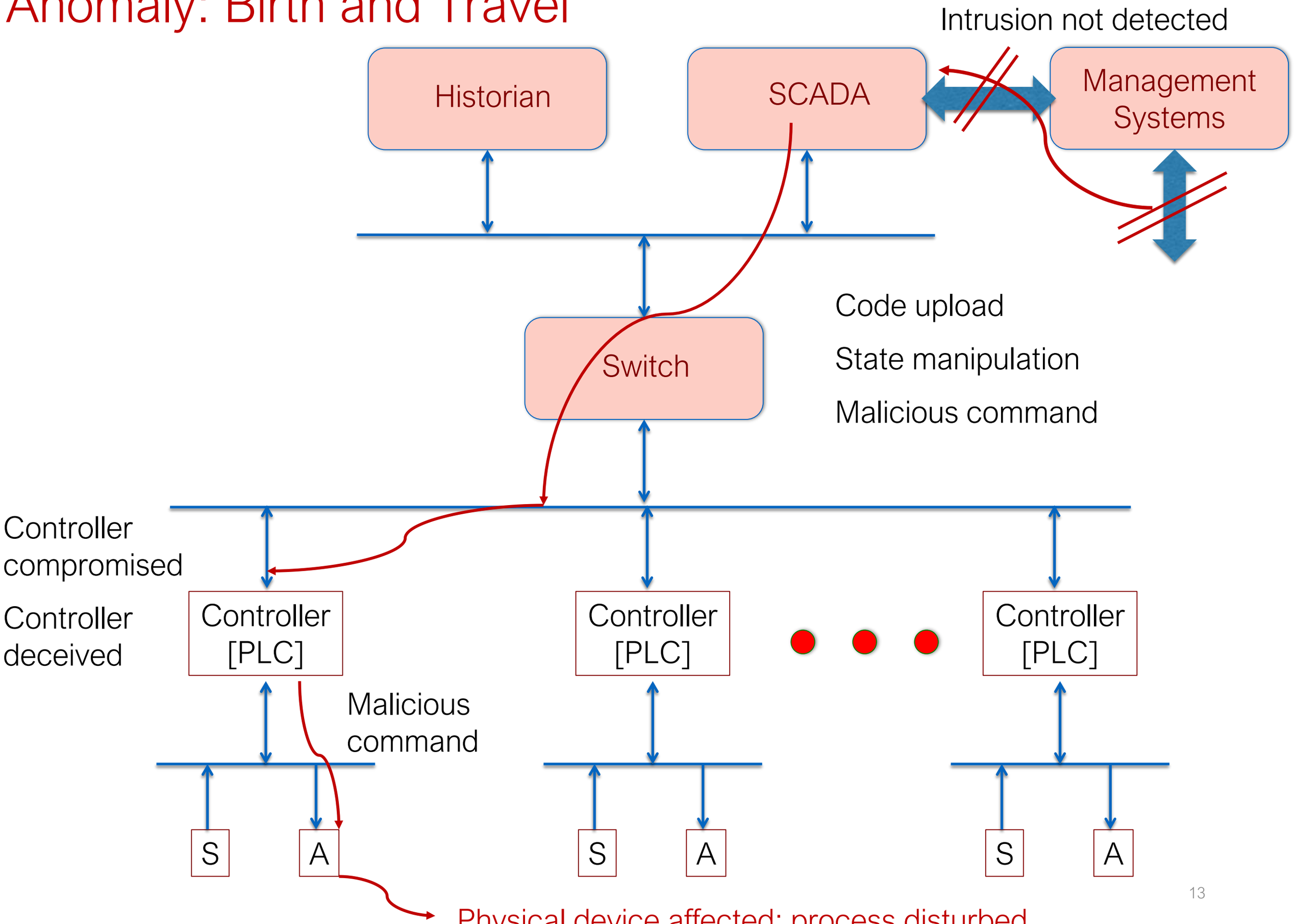
Question:

How to detect anomaly as close to q'_0 as possible?

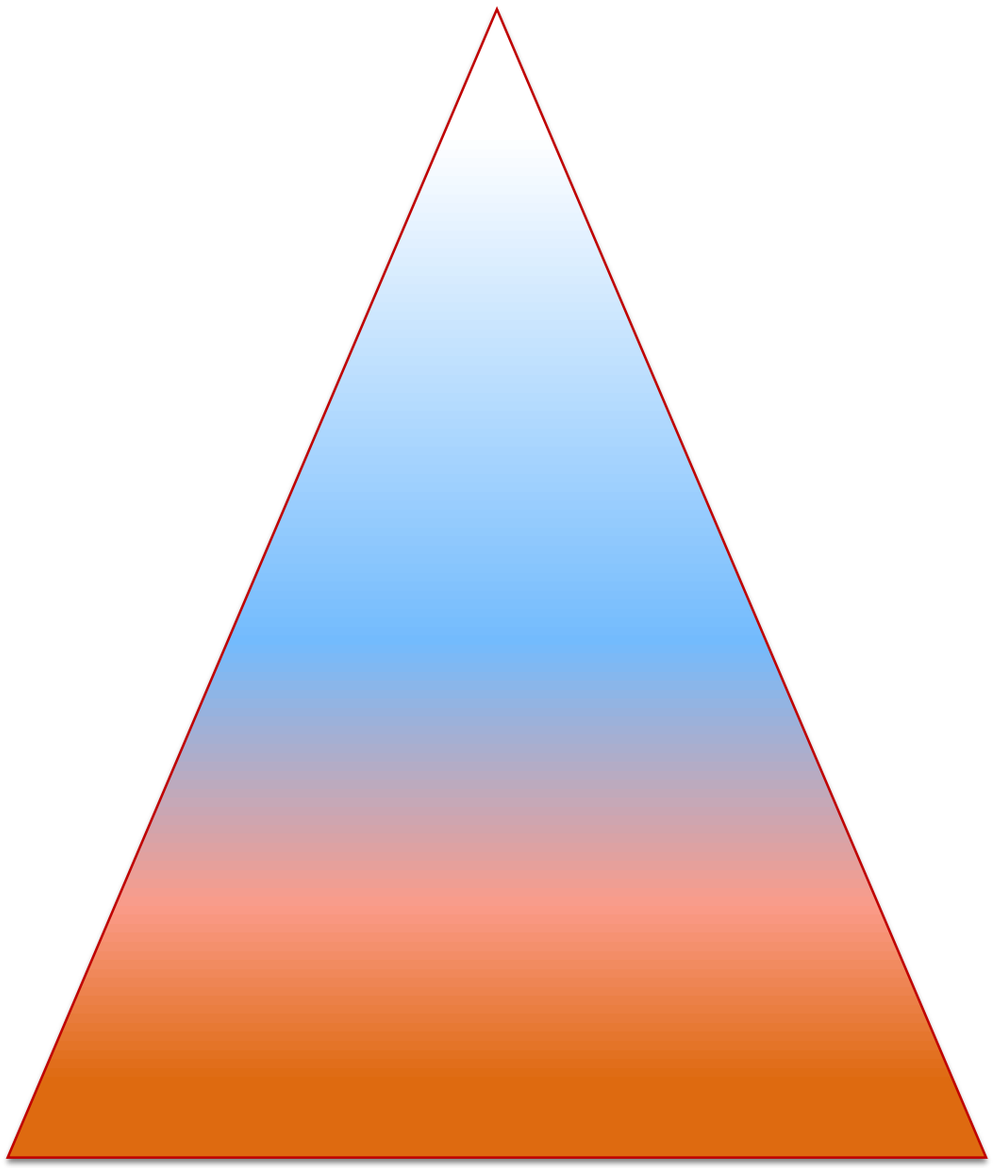
Anomalies: Cause and Avoidance

Component failure	Fault tolerant design
Communications failure	Thorough testing
Programming errors	
Process data manipulated	Secure design
Actuator command manipulated	Firewalls
	IDS

Anomaly: Birth and Travel



The Anomaly Impact Pyramid



None

Mild

Severe

Catastrophic

C. Detection

Requirements

Ultra-high detection rate

- rare for an anomaly to be not detected

Ultra-low rate of false alarm:

- e.g., less than 1-false alarm in 6-months; data collected every second

Timely detection

- Offers “enough” time for an operator to take corrective action and avoid damage

Approaches for Detection

Design Centric

Plant design

- Process Dynamics
  - $\dot{x} = f(x,u,\eta)$
  - $y = g(x, \theta)$

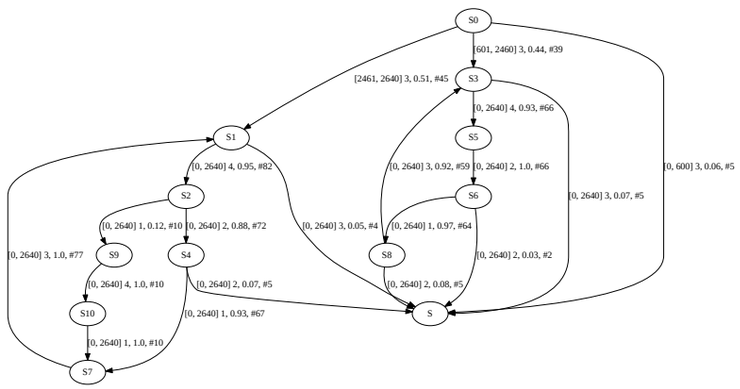
  Fabio et al. 2013
- State Entanglement
  - **if** $(q(c)==v_i)$ $q(S)$;

  Adepu et al. 2016

Data Centric

Plant data

- Machine Learning: Model; Noise



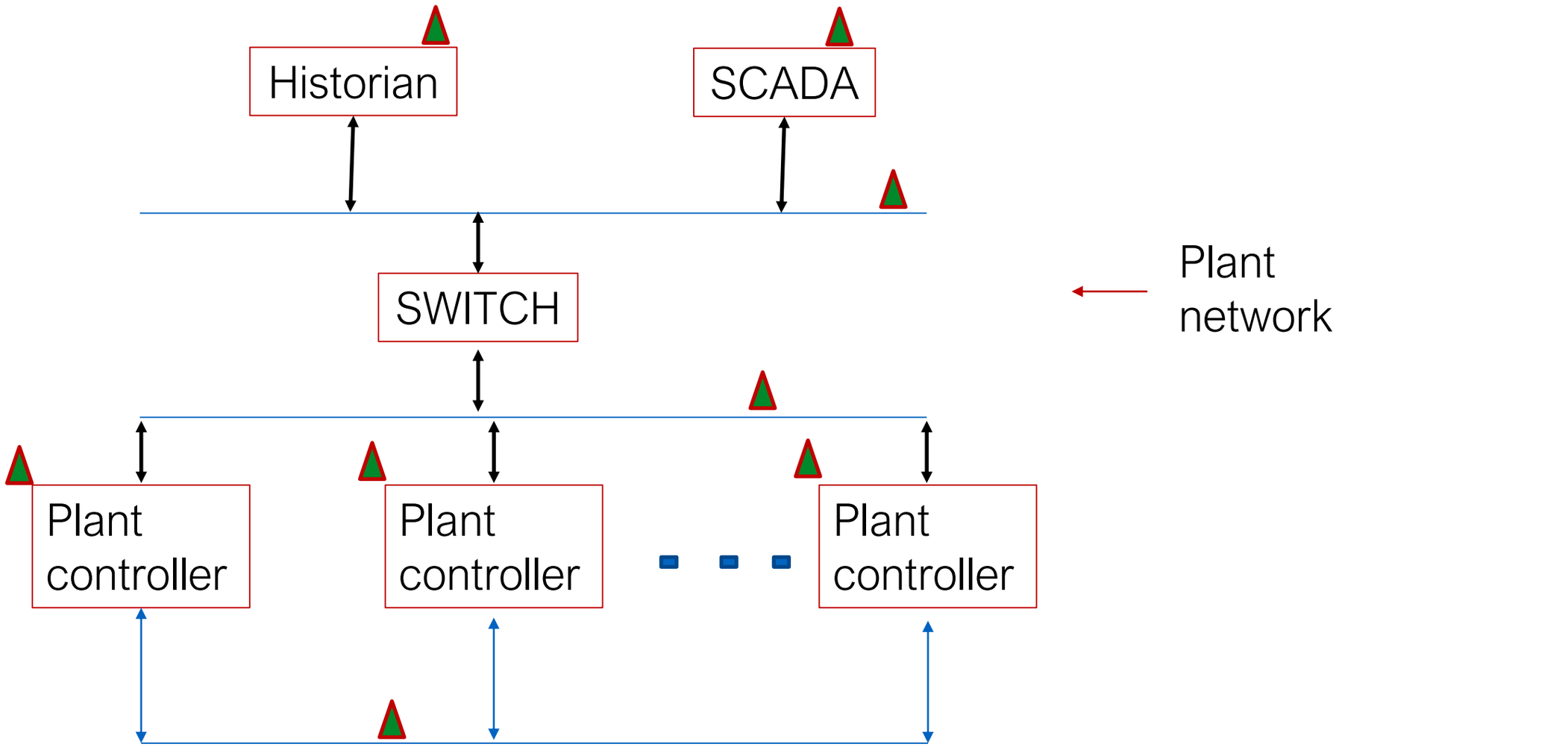
Qin et al. 2018
Mujeeb et al.2018

$Y_k=f(Y_{k-1.} z_1, z_2, \ldots z_n)$

Heng et al. 2019

DAD: Monitor placement

Monitor: A coded version of a set of rules that must hold during normal operation.



Claim

Near perfect anomaly detection is achievable BUT… may not be adequate to protect a plant from severe damage.

D. Command Validation

Definitions

$\omega(t, a)$: A well-formed command sent to actuator a at time t.

$\omega(t, a)$: Valid iff $f(a, \omega, s_k)$, where s_k is plant state when the command is issued.

$f(a, \omega, s_k)$: actuator function for $\omega(t, a)$;
ensures correct and safe operation of the plant

Sample Actuator Functions

Actuator	Command Set	Actuator functions
P101	{ON, OFF}	$f[P101\|ON](\{LIT101, LIT301, MV201\})$ = (LIT101 > 250 AND LIT301 <= 800 AND MV201 == OPEN) $f[P101\|OFF](\{LIT101, LIT301, MV201\})$ = (LIT101 < 250 OR LIT301 > 800 OR MV201 == CLOSE)
MV101	{OPEN, CLOSE}	$f[MV101\|OPEN](\{LIT101\})$ = LIT101 < 500 $f[MV101\|CLOSE](\{LIT101\}))$ = LIT101 > 80

Source of invalid (malicious) commands

Faulty component or network communications

Faulty network communications

Incorrect code

Cyber attack

Origin of a Malicious Command

Direct:
Attacker sends a malicious command to an actuator.

Indirect:
Attacker deceives a PLC through manipulation of state variables.
In turn the deceived PLC sends a malicious command.

A Key Requirement for Validation

Given what we know about the origin of a command…

…a command validator must be able to obtain accurate estimate of the system state and predict continuous state variables.

Challenge 1

How to ensure that a command validator can obtain accurate state estimate?

Challenge 2

Where should a command validator be installed?

Challenge 3

When a command is found to be malicious, should it be sent to the target actuator?

Challenge 4

How to avoid the damaging impact of late detection?

Past work

Stone et al., 2012
Improved modeling and validation of command sequences using a checkable sequence language

Mashima et al., 2016
An active command mediation approach for securing remote control interface of substations

Lin et al., 2016
Runtime semantic security analysis to detect and mitigate control-related attacks in power grids

Maimone et al., 2018
RP-check: An architecture for spaceflight command sequence validation

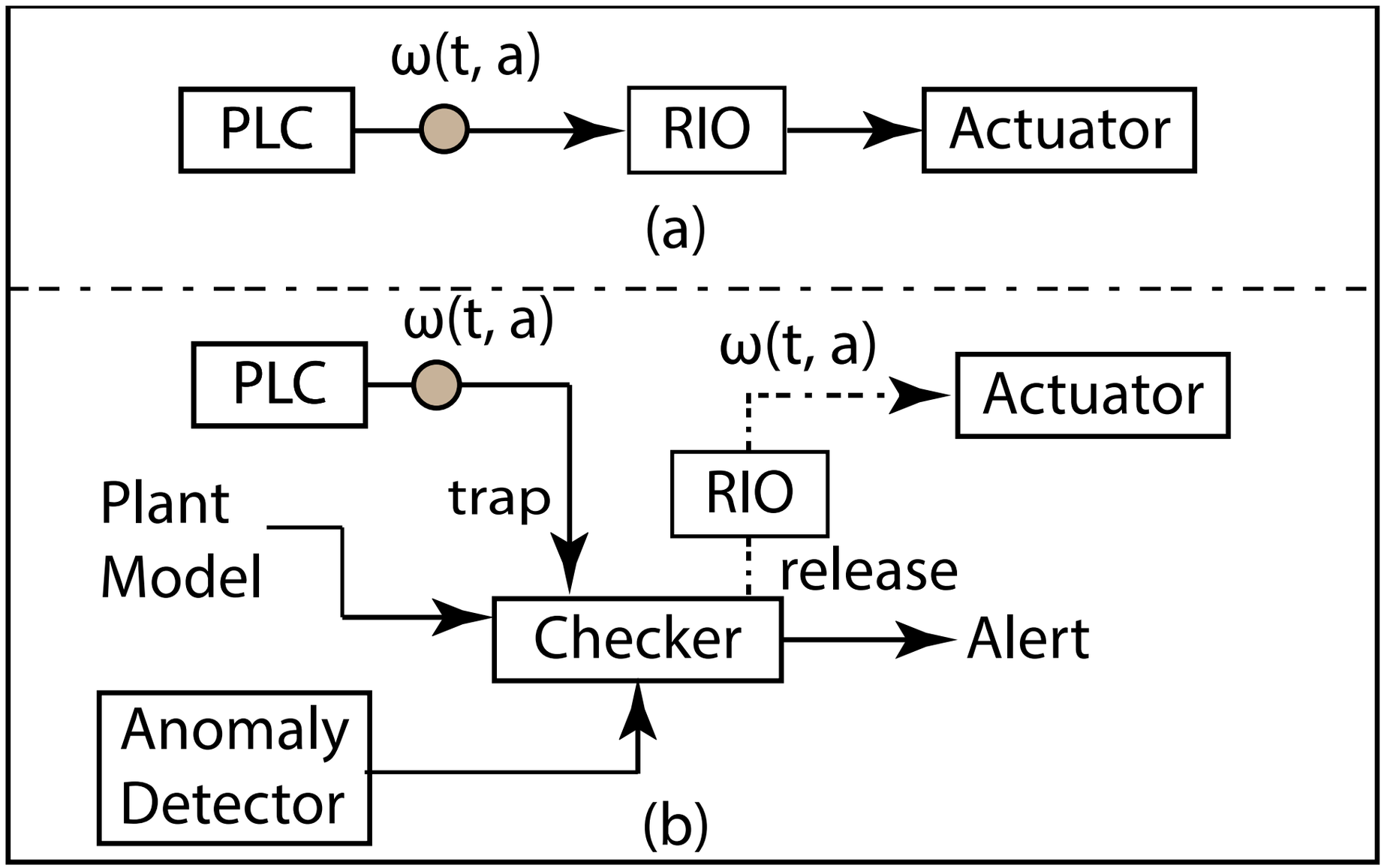
Our approach

Real-time (not simulation)

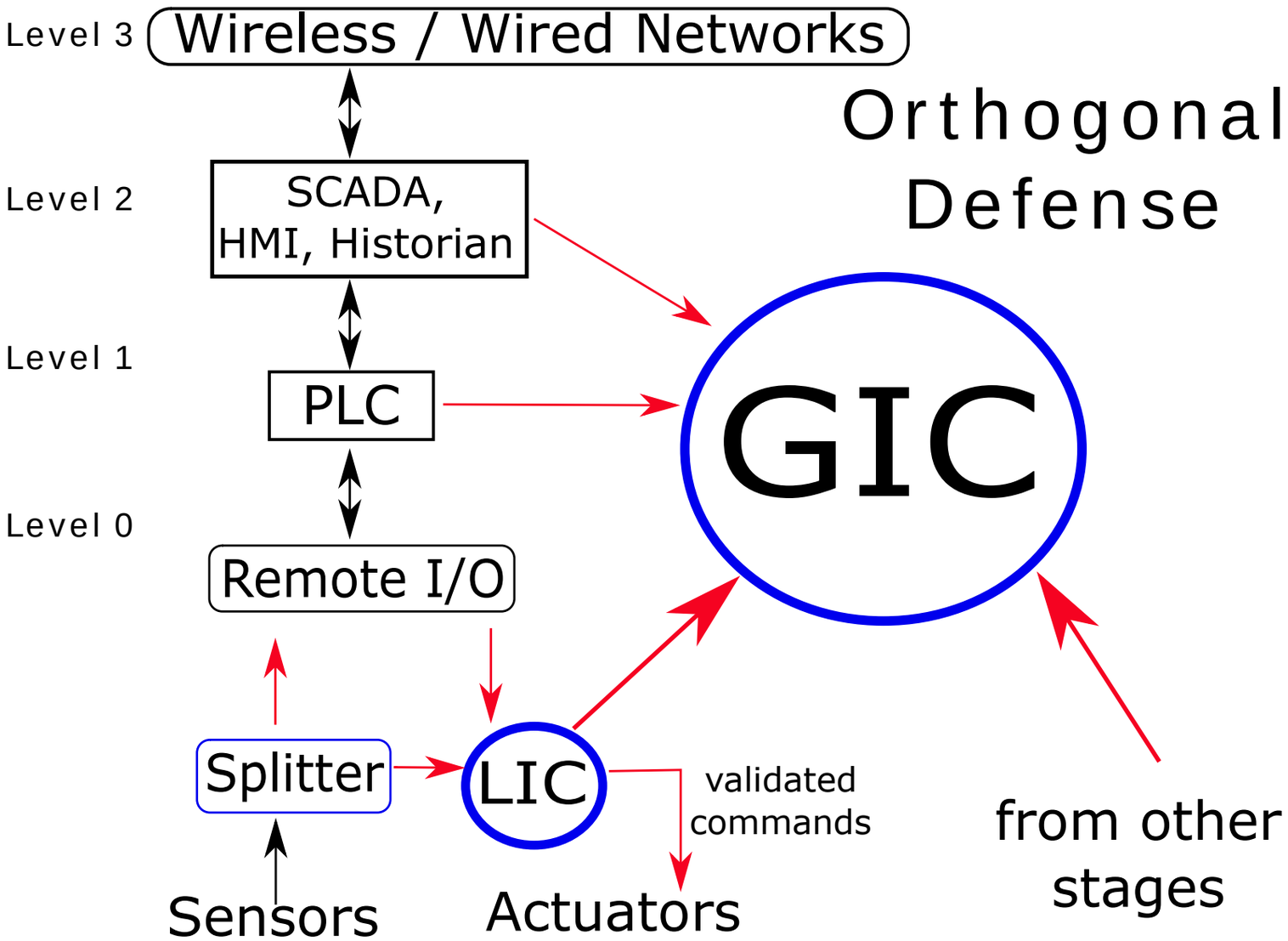
Design centric; partial state estimation

ALL commands are validated

The Approach



Architecture for Command Validation

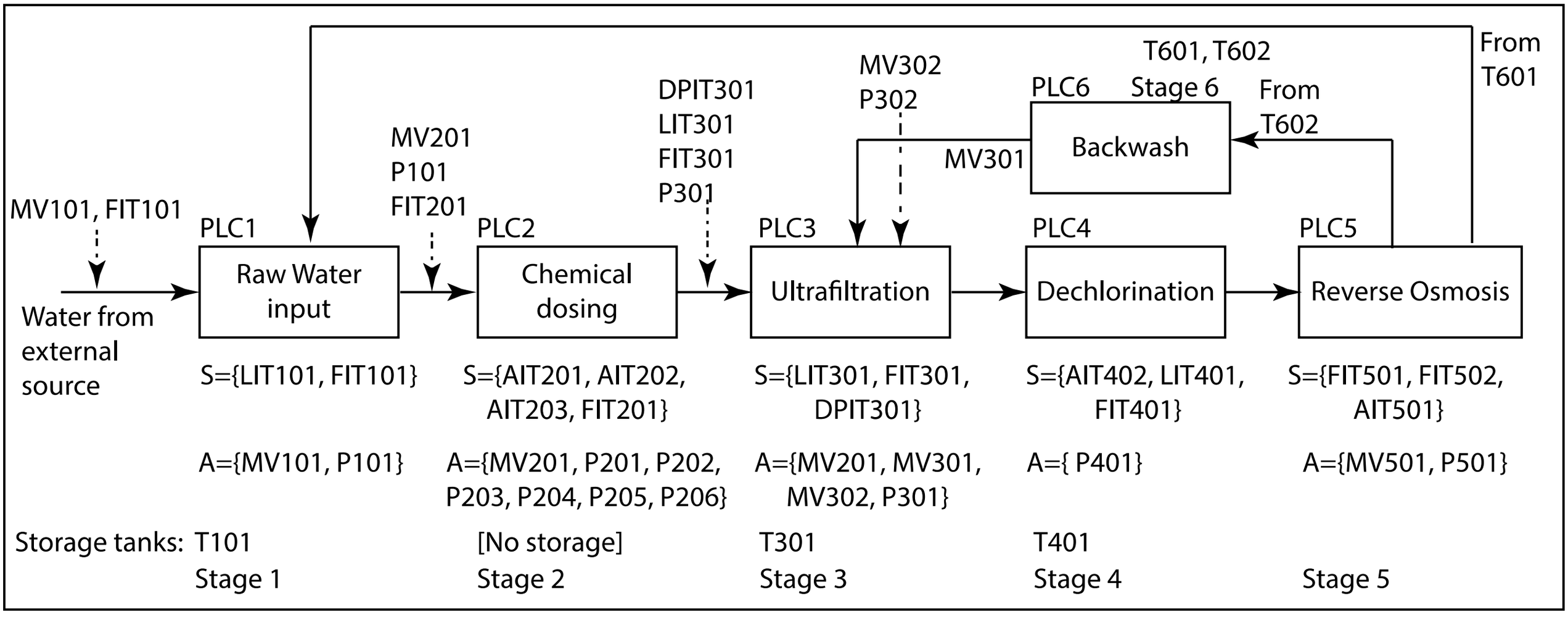


LIC: Local Intelligent Checker

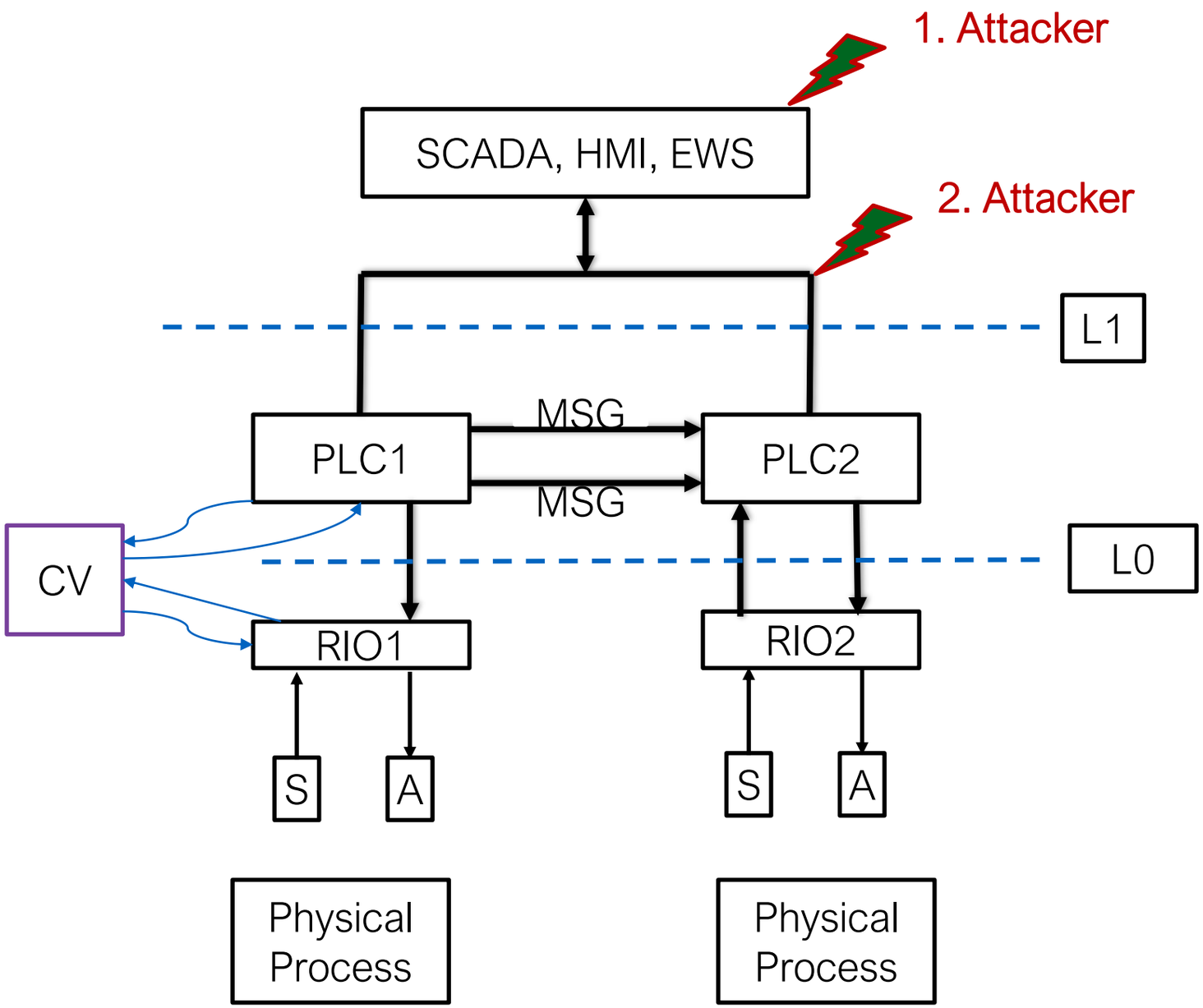
GIC: Global Intelligent Checker

E. Experimental Evaluation

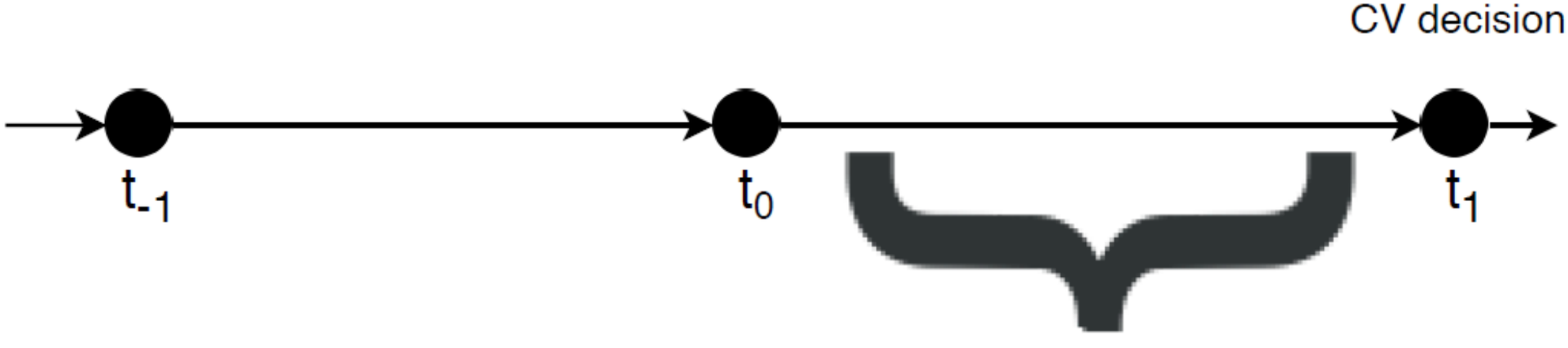
Critical Infrastructure: Water Treatment



Set-up


1. Attacker
SCADA, HMI, EWS
2. Attacker
L1
MSG
PLC1
PLC2
MSG
CV
L0
RIO1
RIO2
S
A
S
A
Physical Process
Physical Process

Time to make decision



Case 1: No attack before t0

Case 2: Attack before t0, detected before t0

Case 3: Attack before t0,

a. detected between t0 and t1,
b. detected after t1, and
c. Not detected.

Attacks: Stage 1

Target	Attack	Detected first by
MV101	Open and Close (chatter attack)	CV
LIT101	Spoof level to low	DAD; then after 6-seconds CV stopped the MV101 open command
P101	Stop the pump	CV
LIT101	Cut sensor wire in RIO	DAD

Attacks: Stage 2

Target	Attack	Detected first by
AIT202	Decrease the pH value	CV
MV201	Close	CV
P205 (NaOCl)	Stop the pump	CV
P201, P202	Turn ON	CV

Attacks: Stage 3

Target	Attack	Detected first by
P301	Stop outflow from UF	CV
DPIT301	Activate backwash	CV
LIT301	Spoof to HH	DAD

Summary 1: Detection and anomalies

CV detected 8 out of 11 attacks.

Remaining three attacks:

- on analog values,
- detected by DAD, i.e., caused anomalies, but
- did not lead to the desired impact.

Summary 2: Timing

No attack detected before t_0.

Attacks detected between t_0 and t_1:

Stage 1: Two out of four attacks detected before t_1

Stage 2: All four attacks detected before t_1

Stage 3: Two out of three detected before t1

Conclusions

In the experiments conducted, CV worked well in concert with the anomaly detector.

Anomalies arising out of continuous state variables are detected by DAD. These may lead to malicious commands (indirect). .

Direct malicious attacks possible only when intelligent checkers are compromised.

F. Next Steps

Full Implementation and Evaluation

Implement CV across the entire plant.

Design and launch single and multi-point masking attacks.

CV Inside PLCs?

Should CV, with state prediction, be placed inside PLCs?

Design of Command Validator for Power Grid

Will the approach work on a power grid?

Timing is critical

100% anomaly avoidance?

Is that a realizable dream?

Thanks…

…to all those who are making it happen!

PhD Students

Sridhar Adepu

Mujeeb Chuadhary

Gayathri Sugumar

Collaborators

Professor Sicco Verwer

Lin Qin, PhD Student

Research Staff

Jonathan Heng

Gauthama Iyer

Nandha Kandasamy

Robert Kooij

Vishrut Mishra

Venkat Reddy

Siddhant Shrivastava

Andrew Yoong

Je vous remercie

Thank You!