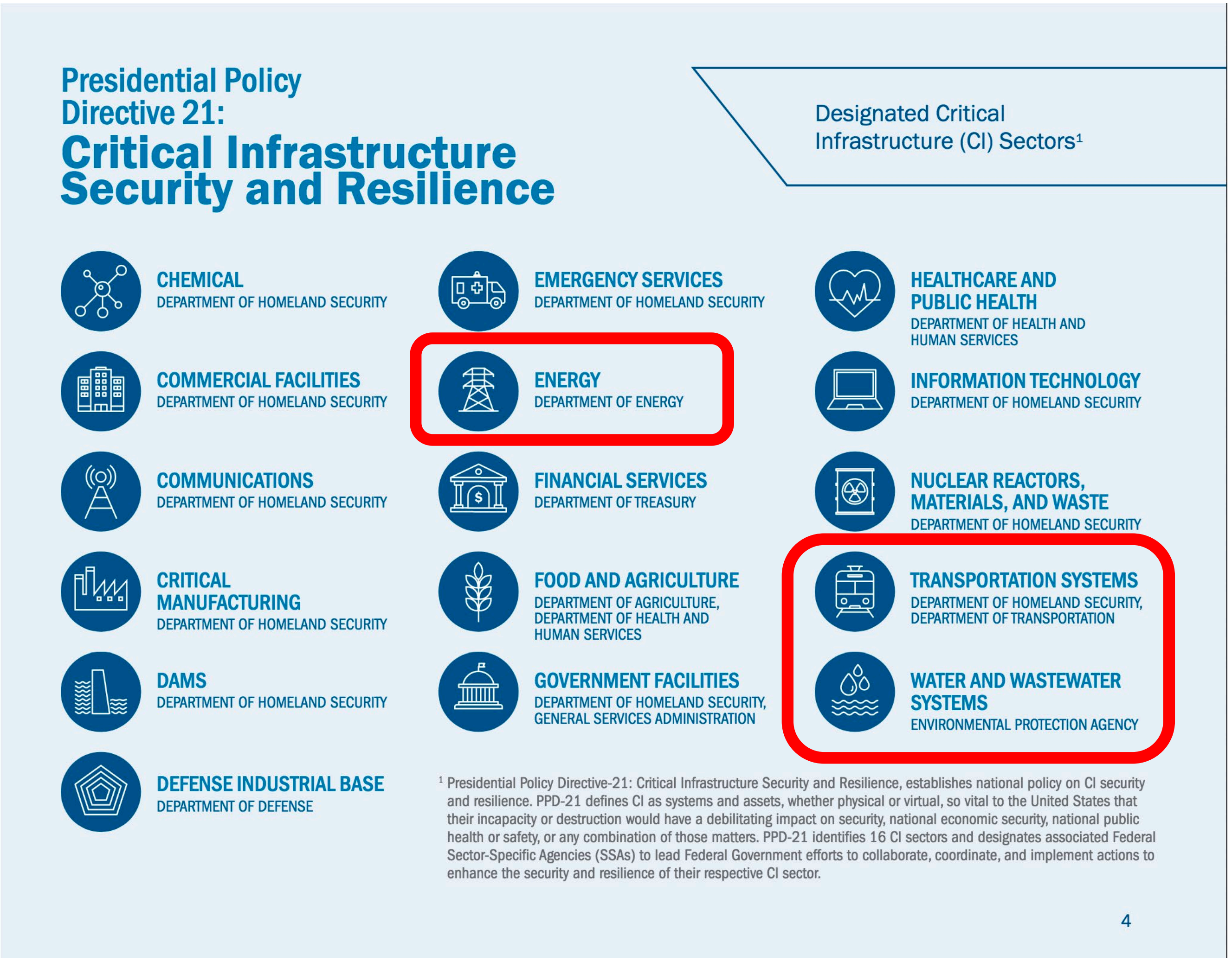
Securing Critical Infrastructure: Challenges and Solutions

Jianying Zhou

Singapore University of Technology and Design (SUTD)

26 May 2021

Critical Infrastructure



Presidential Policy Directive 21:

Critical Infrastructure Security and Resilience

Designated Critical Infrastructure (CI) Sectors[1]

CHEMICAL
DEPARTMENT OF HOMELAND SECURITY

COMMERCIAL FACILITIES
DEPARTMENT OF HOMELAND SECURITY

COMMUNICATIONS
DEPARTMENT OF HOMELAND SECURITY

CRITICAL MANUFACTURING
DEPARTMENT OF HOMELAND SECURITY

DAMS
DEPARTMENT OF HOMELAND SECURITY

DEFENSE INDUSTRIAL BASE
DEPARTMENT OF DEFENSE

EMERGENCY SERVICES
DEPARTMENT OF HOMELAND SECURITY

ENERGY
DEPARTMENT OF ENERGY

FINANCIAL SERVICES
DEPARTMENT OF TREASURY

FOOD AND AGRICULTURE
DEPARTMENT OF AGRICULTURE, DEPARTMENT OF HEALTH AND HUMAN SERVICES

GOVERNMENT FACILITIES
DEPARTMENT OF HOMELAND SECURITY, GENERAL SERVICES ADMINISTRATION

HEALTHCARE AND PUBLIC HEALTH
DEPARTMENT OF HEALTH AND HUMAN SERVICES

INFORMATION TECHNOLOGY
DEPARTMENT OF HOMELAND SECURITY

NUCLEAR REACTORS, MATERIALS, AND WASTE
DEPARTMENT OF HOMELAND SECURITY

TRANSPORTATION SYSTEMS
DEPARTMENT OF HOMELAND SECURITY, DEPARTMENT OF TRANSPORTATION

WATER AND WASTEWATER SYSTEMS
ENVIRONMENTAL PROTECTION AGENCY

[1] Presidential Policy Directive-21: Critical Infrastructure Security and Resilience, establishes national policy on CI security and resilience. PPD-21 defines CI as systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. PPD-21 identifies 16 CI sectors and designates associated Federal Sector-Specific Agencies (SSAs) to lead Federal Government efforts to collaborate, coordinate, and implement actions to enhance the security and resilience of their respective CI sector.

4

https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf

Cyber Attacks in Real World

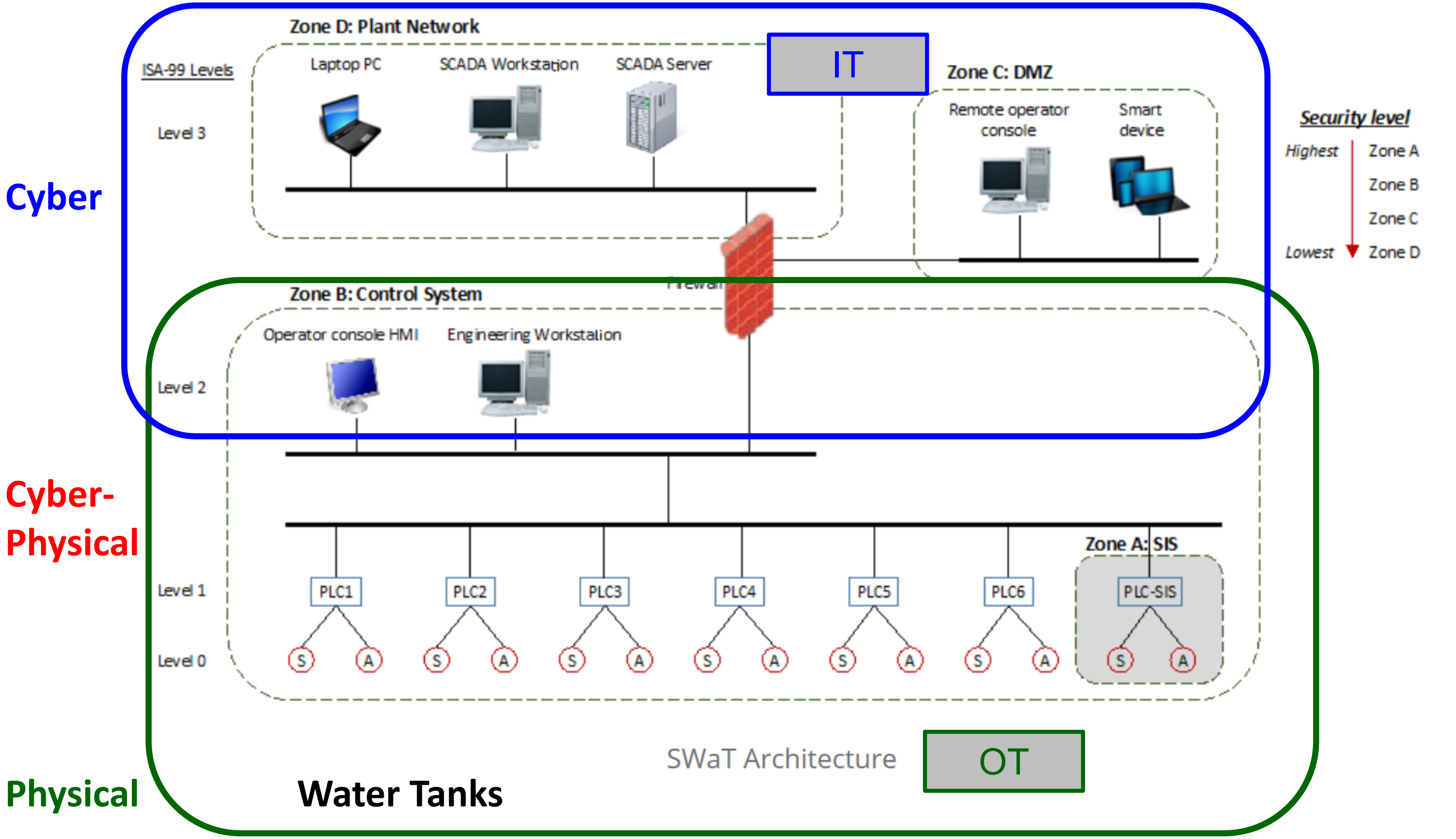
Iran nuclear plant (2010)

Florida water treatment plant (Feb 2021)

Ukraine power grid (2015, 2016)

Colonial Pipeline (May 2021)

Cyber-Physical System Architecture



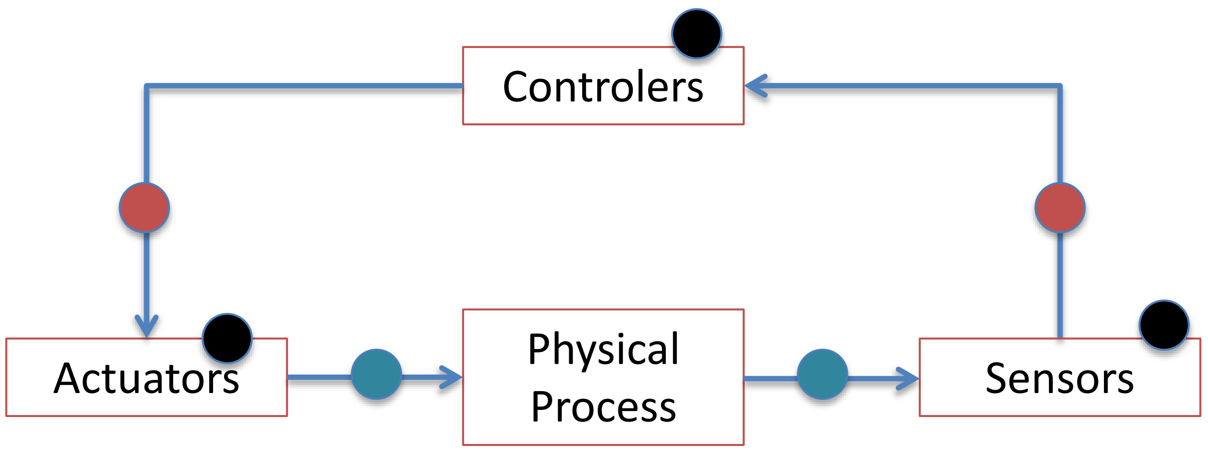
Key Features of CPS

- **Reactive**
  - Interact with its environment via inputs and outputs.
- **Real-Time**
  - Have time constrain to execute the necessary computations and communicate the results.
- **Concurrency**
  - Multiple processes execute concurrently, exchanging information with one another to achieve the desired goal of the computation.
- **Safety-Critical**
  - Safety of the system has a higher priority over other design objectives such as performance and development cost.

Causes of Vulnerability in CPS

- **Isolation assumption**
  - “Security by obscurity” has been dominant in most of CPS applications since their initial design.
  - Focus on designing reliable and safe systems.
  - The systems were supposed to be isolated from the outside world.
- **Increased connectivity**
  - CPS are more connected than ever before.
  - More connectivity increases the number of access points to CPS, thus more attack surfaces arise.
- **Heterogeneity**
  - CPS are almost always multi-vendor systems.
  - Each product has its own security problems.
  - Internal details of the integrated and heterogenous components are unknown. They may produce unexpected behavior when they are deployed.

Attack Points in CPS



- Physical damage to devices
- Tempering with electrical connections
- Attack via network intrusion

CPS Security Challenges

- **Difference with traditional IT systems**
  - Software patching and frequent updates, are not well suited for CPS.
  - Real-time availability provides a stricter operational environment than most traditional IT systems.
  - Many cyber-physical systems are legacy systems, almost no security by design.

  \+ Simpler network dynamics: fixed topology, stable user population, regular communication patterns, and limited number of protocols.

Cyber Defense of CPS

Operational Technology [OT] centric:

- Avoid process anomalies due to an attack
- Detect process anomalies due to an attack
- Recover from process anomalies due to an attack

Design Centric (Physics/Chemistry)	vs	Data Centric (AI + ML)
Authentication & Attestation (on-line)	vs	Modeling & Analysis/Verification (off-line)

CPS Testbeds @ iTrust


Secure Water Treatment (SWaT)


Water Distribution (WADI)


IoT Shielded Room


Transformer & inverters


Electric Power & Intelligent Control (EPIC)


Generators & programmable loads

Secure Water Treatment (SWaT)

- Consists of a modern six-stage water process.
- A layered communications network, PLCs, HMIs, SCADA workstation and historian.

- Virtual tour of SWaT – https://www.youtube.com/watch?v=2r1ctjULCnI

Water Distribution (WADI)

- A natural extension of SWaT.
- Consists of two elevated reservoir tanks, six consumer tanks, two raw water tanks and a returned tank.

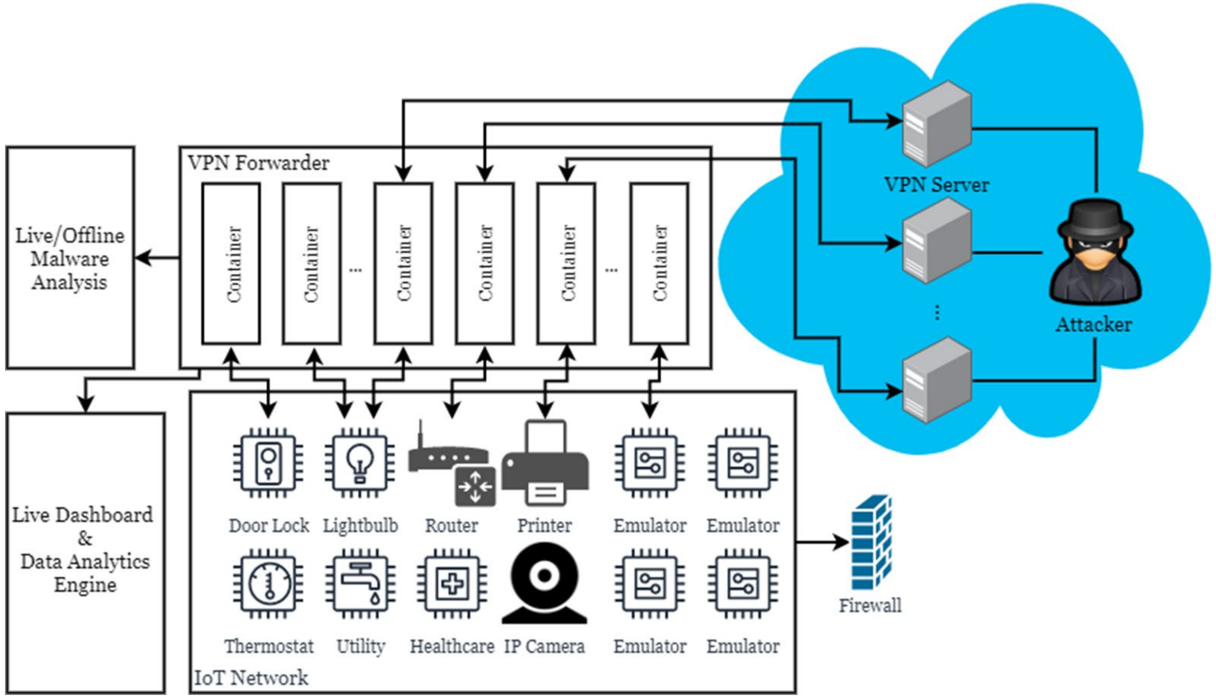
- Able to simulate the effects of physical attacks such as **water leakage** and **malicious chemical injections**.

Electric Power & Intelligent Control (EPIC)

- Consists of four stages, from power generation, transmission, to micro-grid (PV, battery), and smart home.

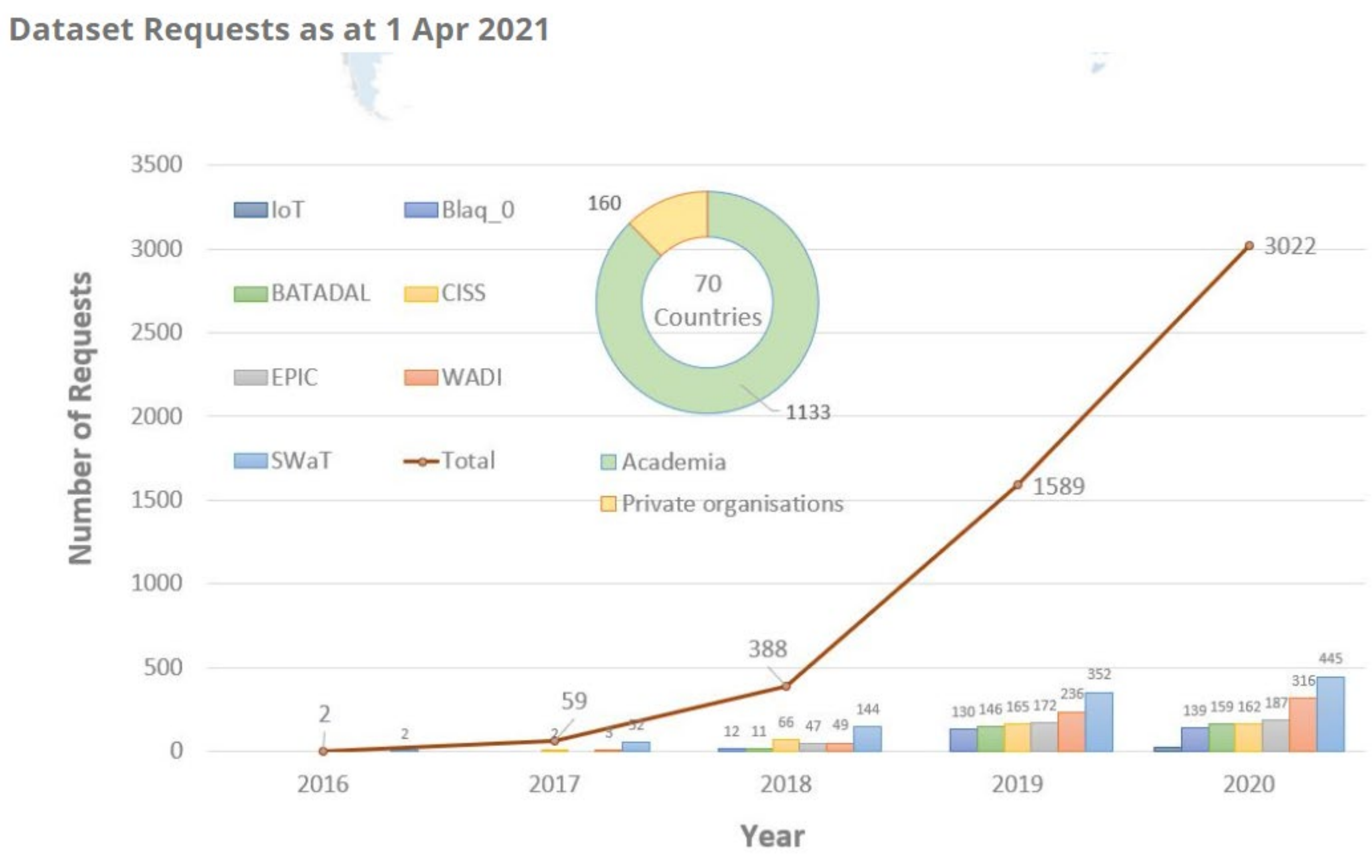
- Designed to enable cyber security researchers conduct experiments to assess the effectiveness of novel cyber defense mechanisms.

IoT Honeypot



- 17 real IoT devices & 5 ICS emulators
- 31 wormholes globally
- Live since Nov 2019
- Collected 71GB of network traffic data

CPS Datasets @ iTrust



Datasets downloaded by 3022 research groups from70 countries.

https://itrust.sutd.edu.sg/itrust-labs_datasets/

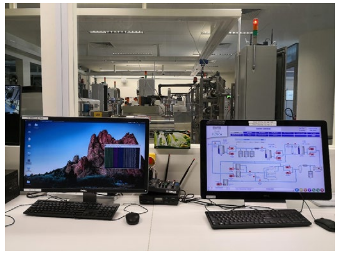
CPS Security Technologies @ iTrust

Layer 1 (PLC)

- *DAD* (AsiaCCS’17)*
- *PAtt (RAID’19)*
- *PoA* (ACSAC’19)*
- *ProcessSkew* (WiSec’20)*
- *ScanCycle* (AsiaCCS’21)*

Practical & Reliable Solutions:

- Novelty
- Generality
- Applicability
- Scalability

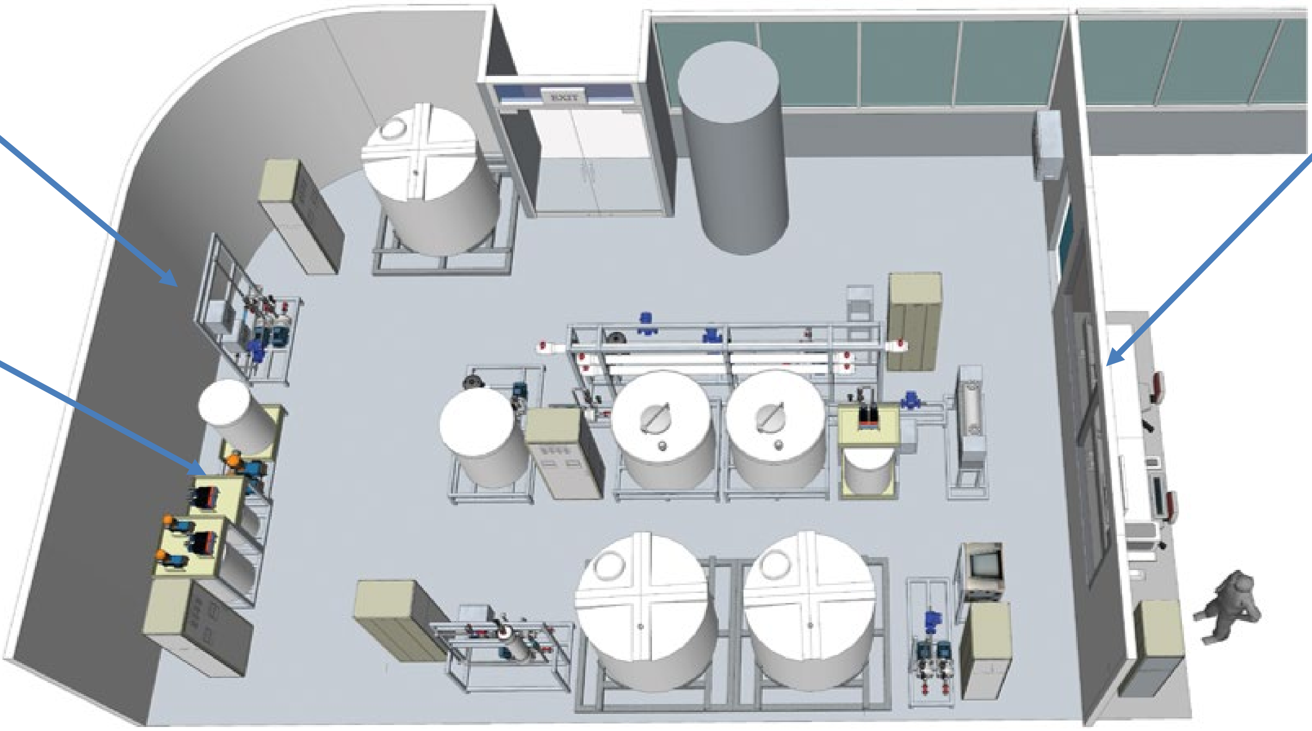


Layer 2 (Historian)

- *BlockOps**
- *VVateR*

Layer 0 (Sensor/Actuator)

- *HD2FA* (ESORICS’16)*
- *NoisePrint* (AsiaCCS’18)*
- *BbTest* (ACNS’19)*



* *Patent / patent pending*

NoisePrint

Motivation:

- Identify devices (sensors and actuators) and detect anomalies in CPS.

Solution:

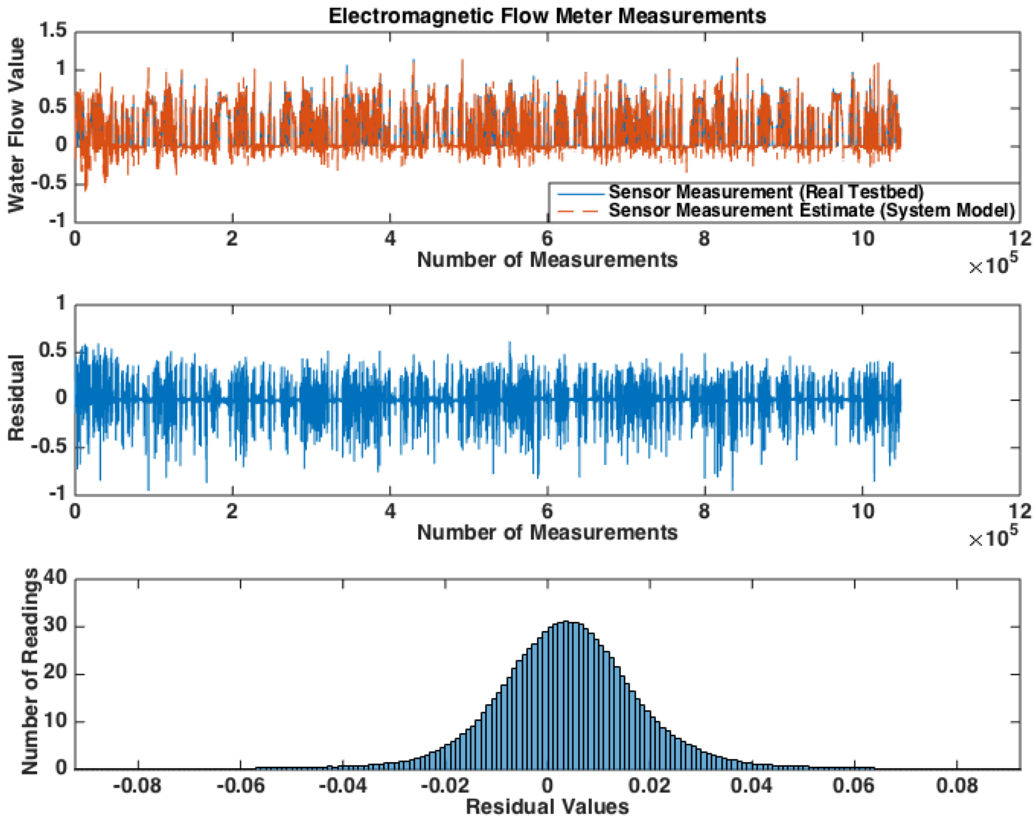
- Fingerprint two noise sources:
  - ✓ Device noise: comes from device manufacturing imperfections
  - ✓ Process noise: comes from the physical process of a system
- NoisePrint = device identification + attack detection

Features:

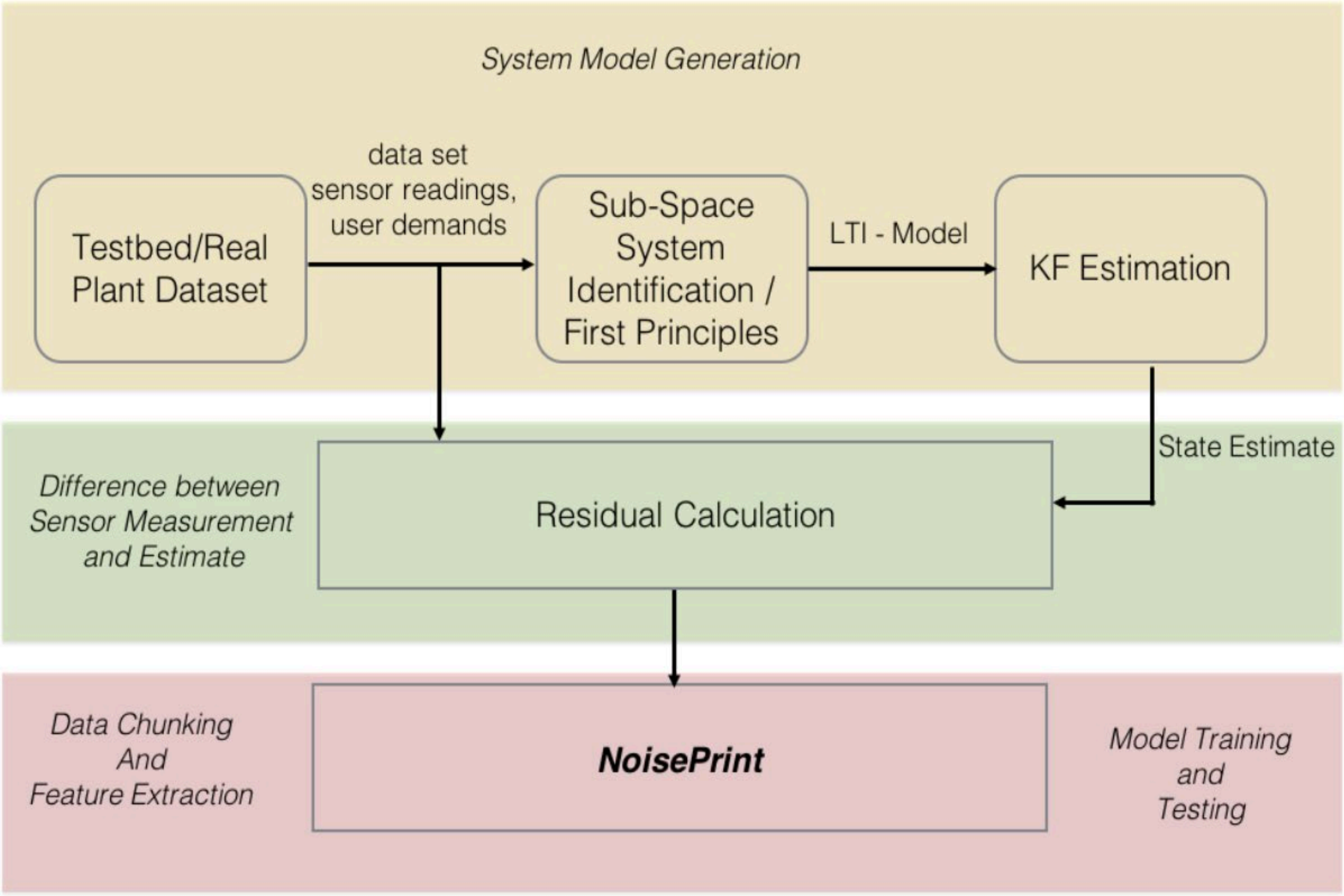
- High accuracy
- Non-intrusive detection

Reference:

- "NoisePrint: Attack Detection Using Sensor and Process Noise Fingerprint in CPS". **ACM AsiaCCS'18** (patent pending)



NoisePrint: Framework



NoisePrint: Flow Chart

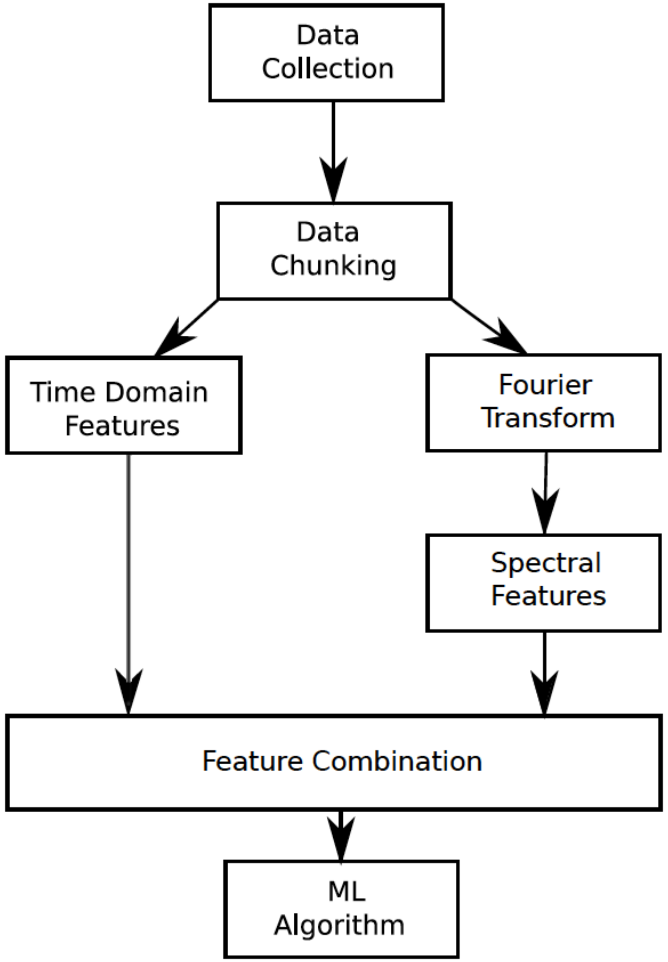


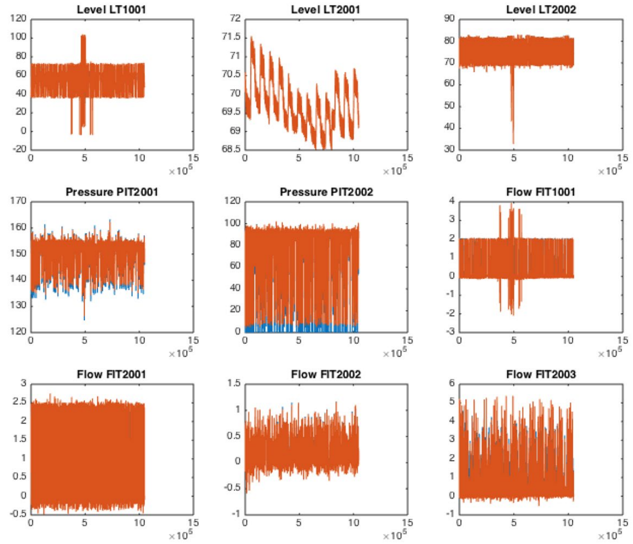
TABLE 1. LIST OF FEATURES USED.

Feature	Description
Mean	$\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i$
Std-Dev	$\sigma = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(x_i - \bar{x}_i)^2}$
Mean Avg. Dev	$D_{\bar{x}} = \frac{1}{N}\sum_{i=1}^{N} \lvert x_i - \bar{x}\rvert$
Skewness	$\gamma = \frac{1}{N}\sum_{i=1}^{N}(\frac{x_i - \bar{x}}{\sigma})^3$
Kurtosis	$\beta = \frac{1}{N}\sum_{i=1}^{N}(\frac{x_i - \bar{x}}{\sigma})^4 - 3$
Spec. Std-Dev	$\sigma_s = \sqrt{\frac{\sum_{i=1}^{N}(y_f(i)^2)*y_m(i)}{\sum_{i=1}^{N} y_m(i)}}$
Spec. Centroid	$C_s = \frac{\sum_{i=1}^{N}(y_f(i))*y_m(i)}{\sum_{i=1}^{N} y_m(i)}$
DC Component	$y_m(0)$

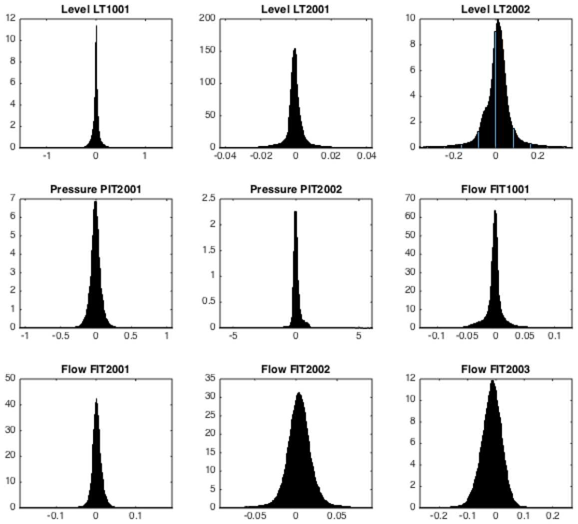
Vector x is time domain data from the sensor for N elements in the data chunk. Vector y is the frequency domain feature of sensor data. y_f is the vector of bin frequencies and y_m is the magnitude of the frequency coefficients.

NoisePrint: Sensor Identification in WADI

WADI for device identification



WADI: System Model



WADI: Residues

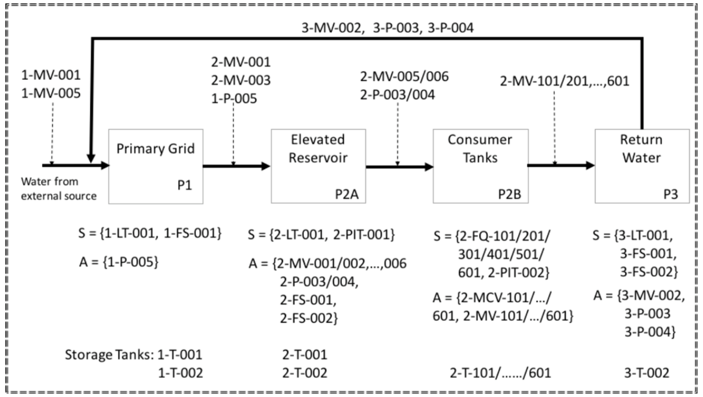


Figure 2: Three stages in WADI are shown. Solid arrows indicate flow of water and sequence of processes. S and A represent, respectively, sets of sensors and actuators. 1-LT-001: level sensor in stage 1 and tank 1; 1-FS-001: flow meter 1 in stage 1; 1-T-001: Tank 1 in stage 1; 2-MV-001: motorized valve 1 in stage 2; 2-MCV-101: motorized consumer valve 1 in stage 2; and 3-P-004: water pump 4 at stage 3.

Table 5: WADI Sensor Identification Accuracy Result

Sensor	Type and Model	Identification Accuracy
RADAR Level Sensor (Primary Grid)	iSOLV RD700	90.87%
RADAR Level Sensor (Secondary Grid)	iSOLV EFS803/CFT183	96.41%
RADAR Level Sensor (Secondary Grid)	iSOLV EFS803/CFT183	91.52%
Differential Pressure Transmitter (Secondary Grid)	iSOLV SPT 200	92.02%
Differential Pressure Transmitter (Secondary Grid)	iSOLV SPT 200	92.95%
Electromagnetic Flowmeter (Primary Grid)	iSOLV EFS803/CFT183	92.76%
Electromagnetic Flowmeter (Secondary Grid)	iSOLV EFS803/CFT183	90.76%
Electromagnetic Flowmeter (Secondary Grid)	iSOLV EFS803/CFT183	90.0%
Electromagnetic Flowmeter (Secondary Grid)	iSOLV EFS803/CFT183	92.04%

BbTest – Black-Box Security Testing

Motivation:

- Evaluating the security of CPS is challenging, as it brings risks not acceptable in mission-critical systems.
- Model-based approaches help to address such challenges by keeping the risk associated with testing low.

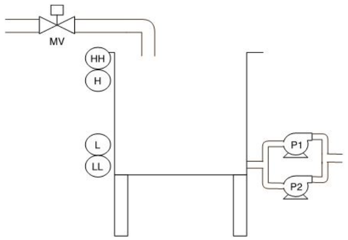
Solution:

- Provide a methodology to model a CPS as a hybrid system model.
- Develop a model-based attack detection mechanism for CPS.
- Introduce time-to-critical-state as metrics to evaluate attack impacts to CPS and resilience of the system.

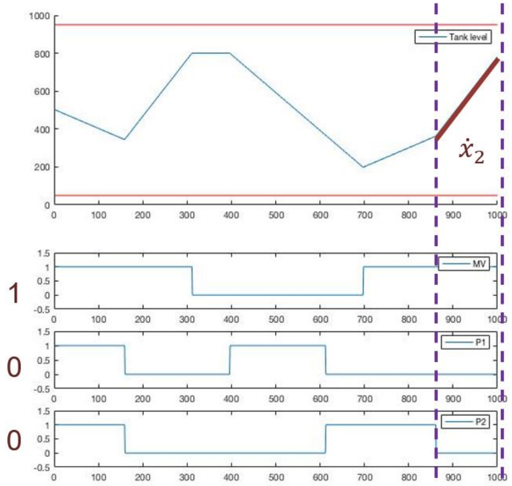
Features:

- Take a black-box approach to model CPS without the controllers' source code.
- Require minimal initial configuration to build model automatically.

Cyber-Physical System

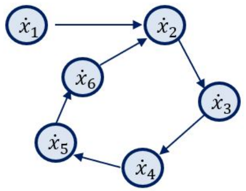


System Behaviour



Hybrid Model

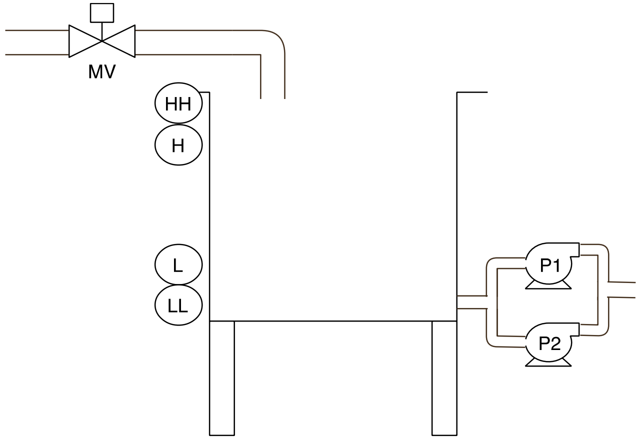
MV	P1	P2	loc
1	1	1	1
1	0	0	2
0	0	0	3
0	1	0	4
0	0	1	5
1	0	1	6



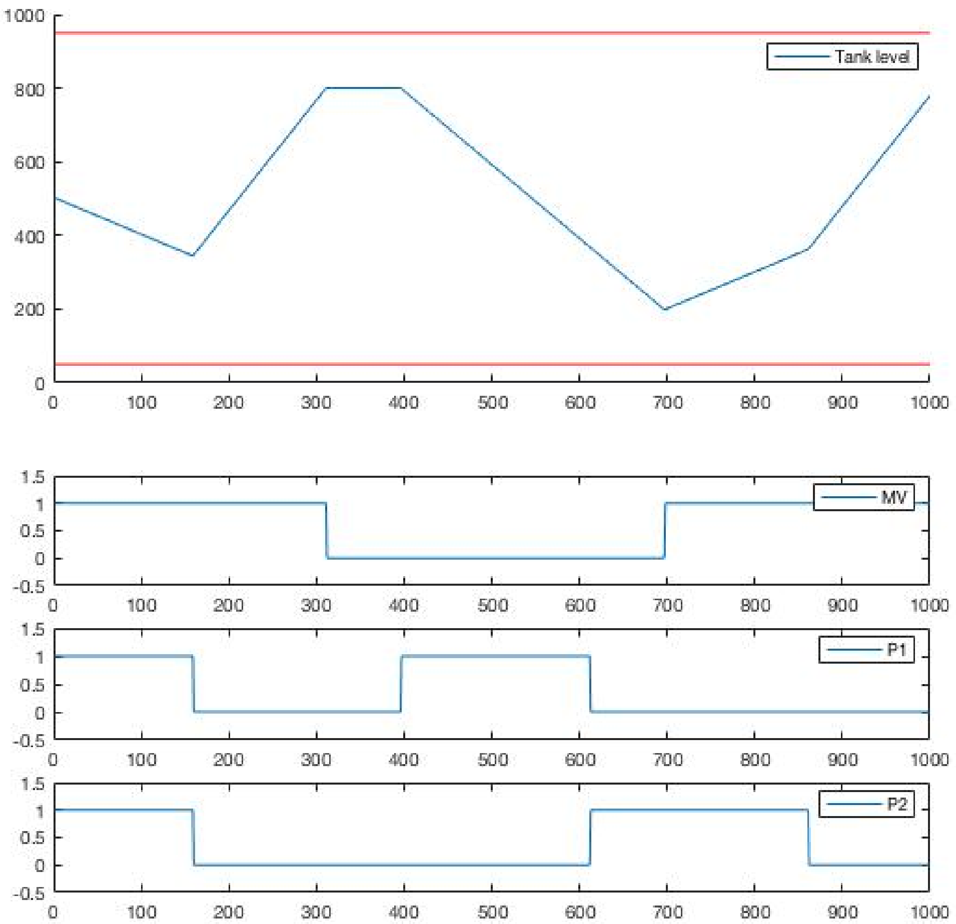
Reference:

- "A Modular Hybrid Learning Approach for Black-Box Security Testing of CPS". **ACNS'19** (PCT patenting)

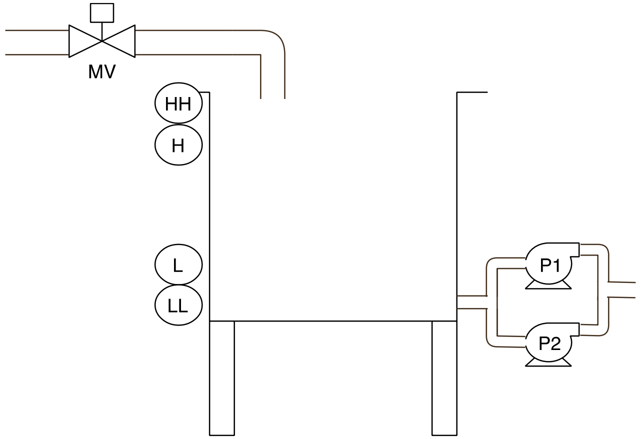
BbTest: Black-Box Modelling



Sensors(y) / Actuators(u)

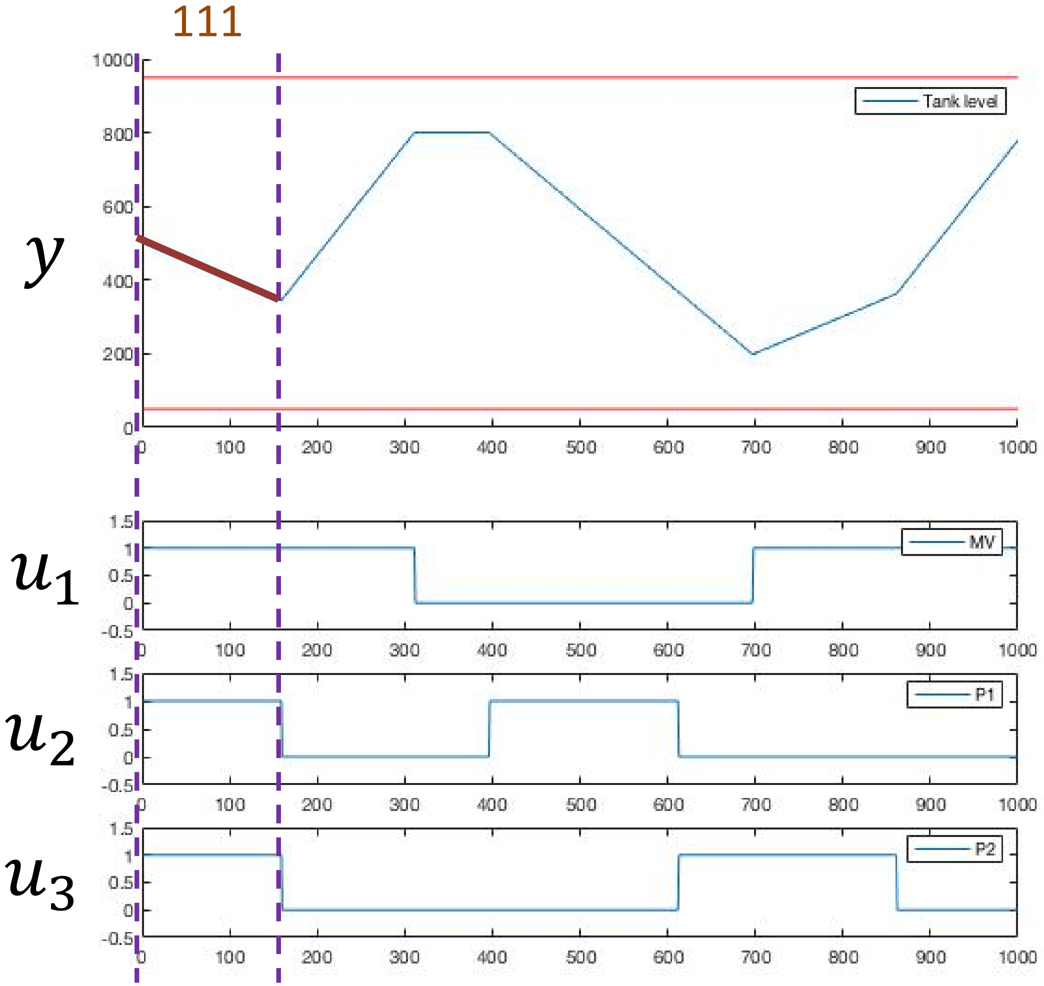


BbTest: Black-Box Modelling

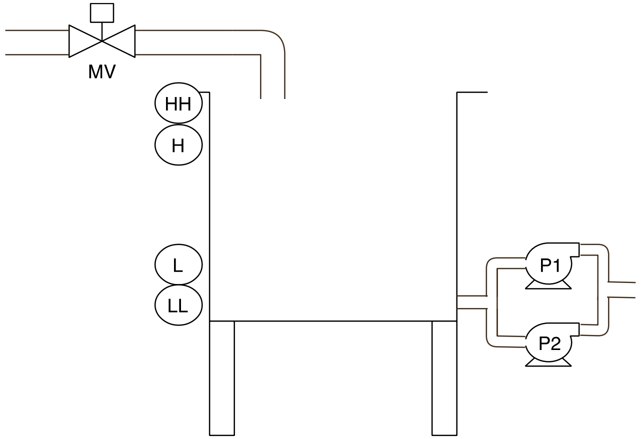


Finite State Machine

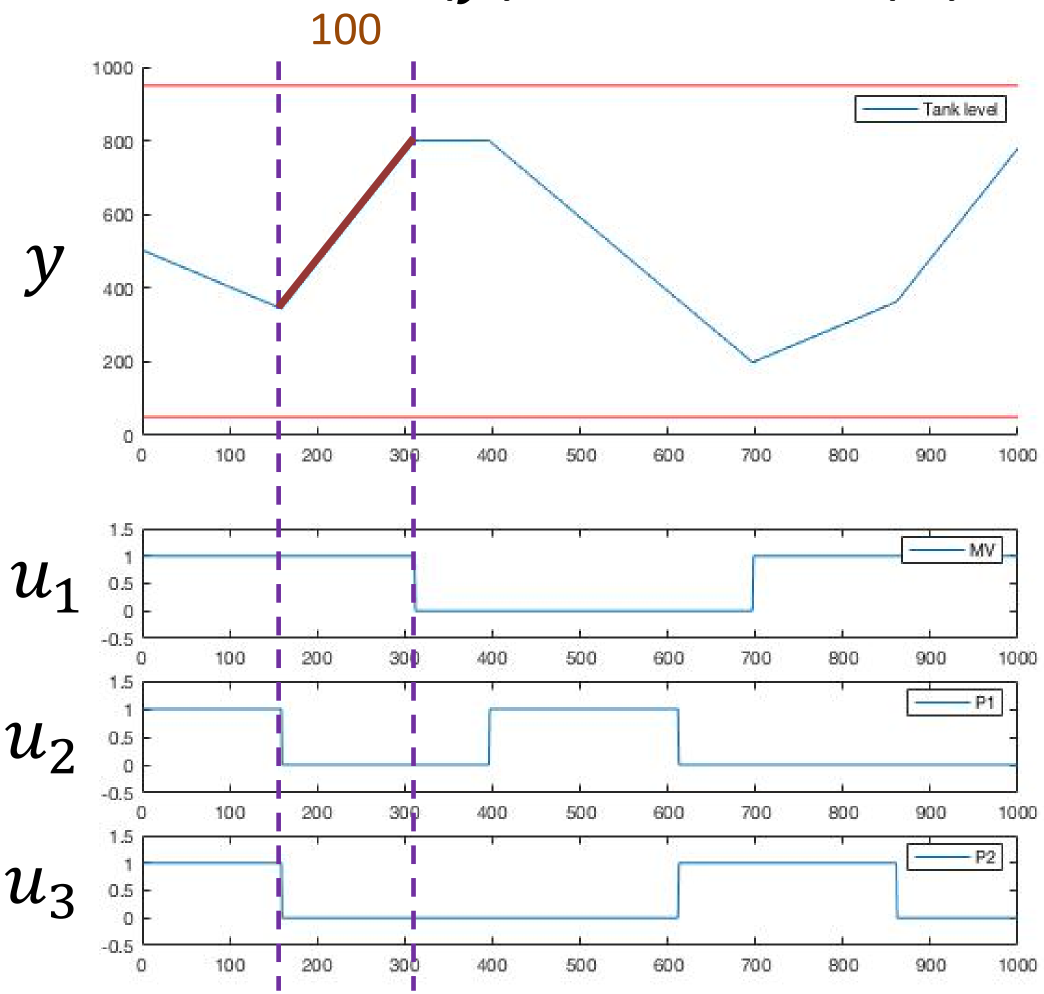
Sensors(y) / Actuators(u)

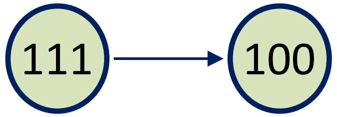


BbTest: Black-Box Modelling



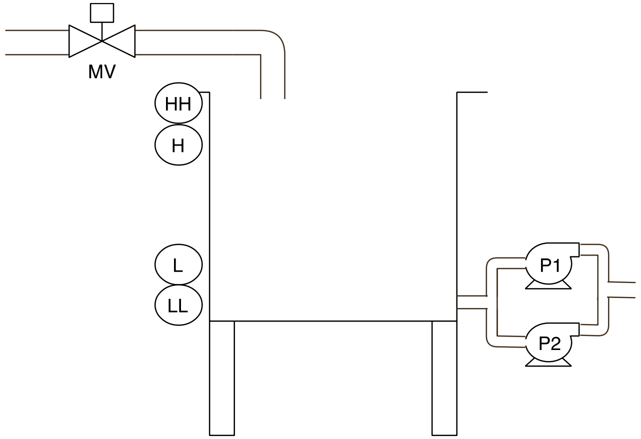
Sensors(y) / Actuators(u)



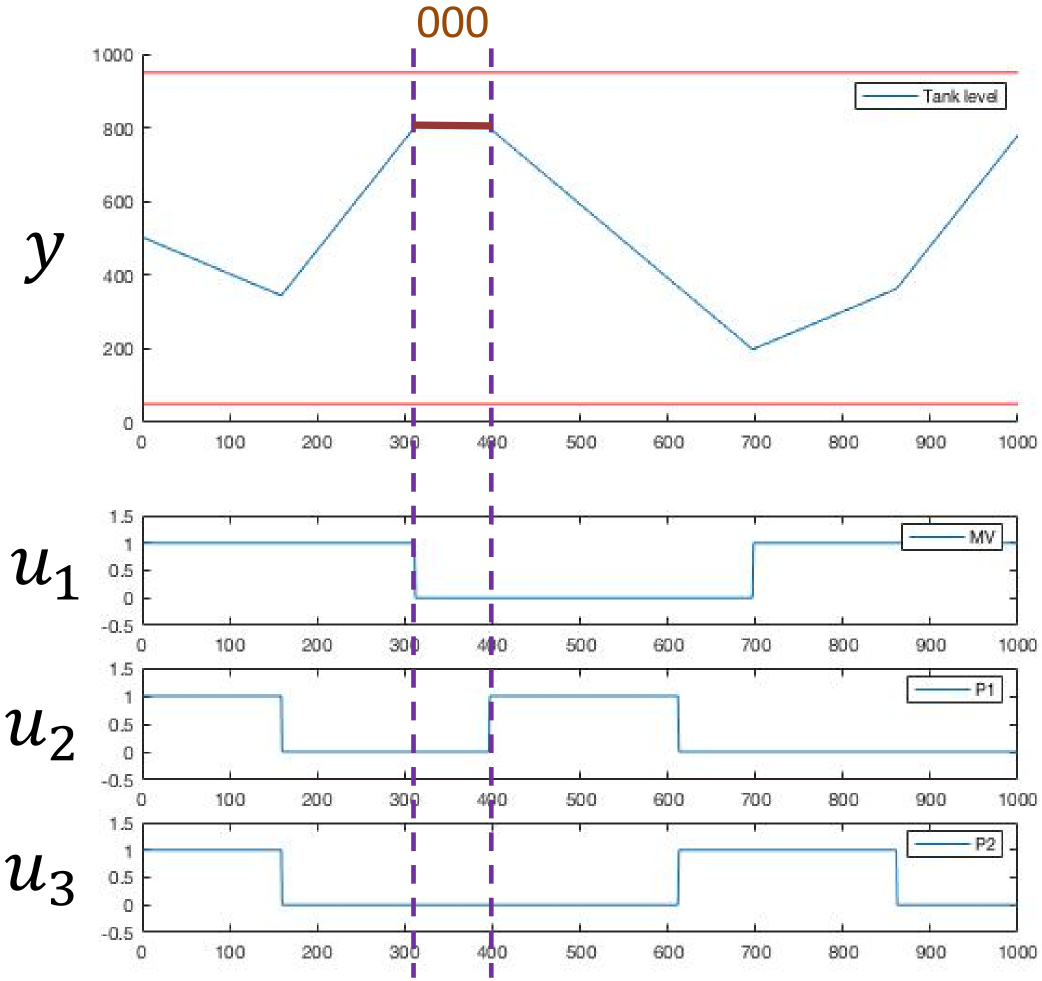


Finite State Machine

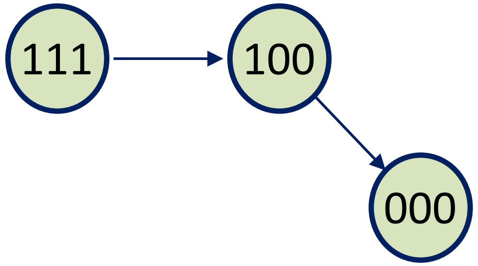
BbTest: Black-Box Modelling



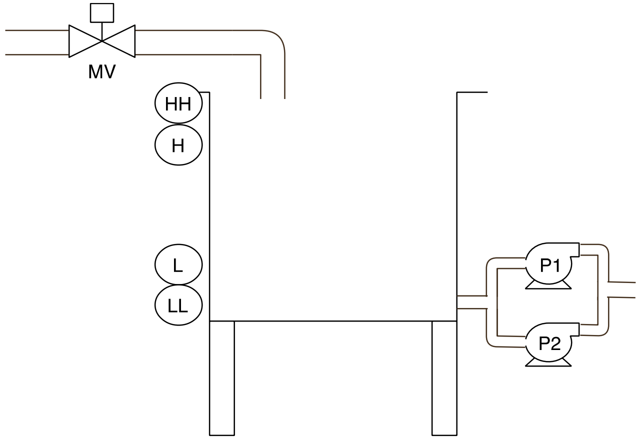
Sensors(y) / Actuators(u)



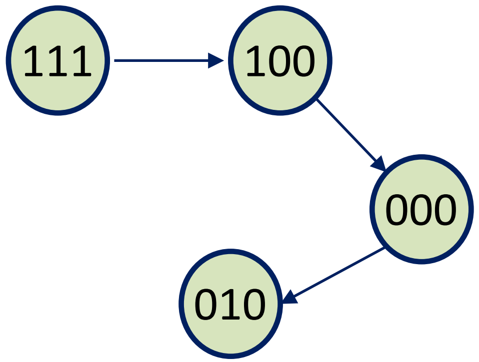
Finite State Machine



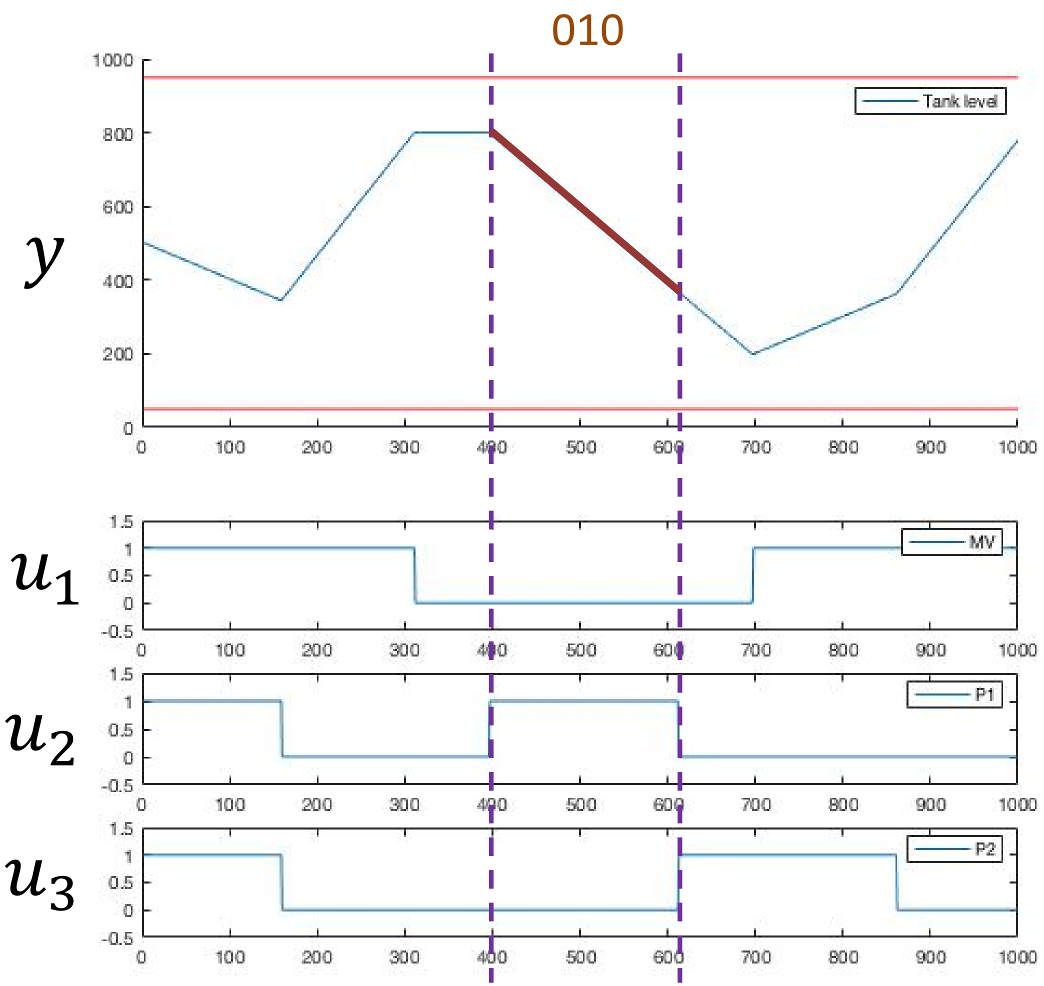
BbTest: Black-Box Modelling



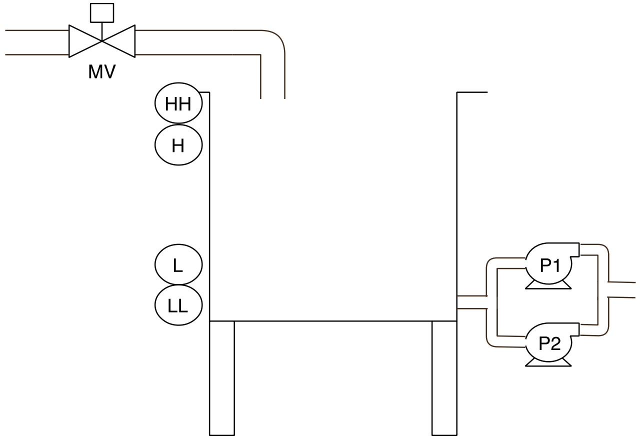
Finite State Machine



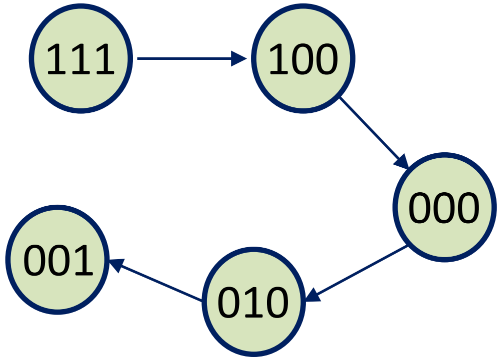
Sensors(y) / Actuators(u)



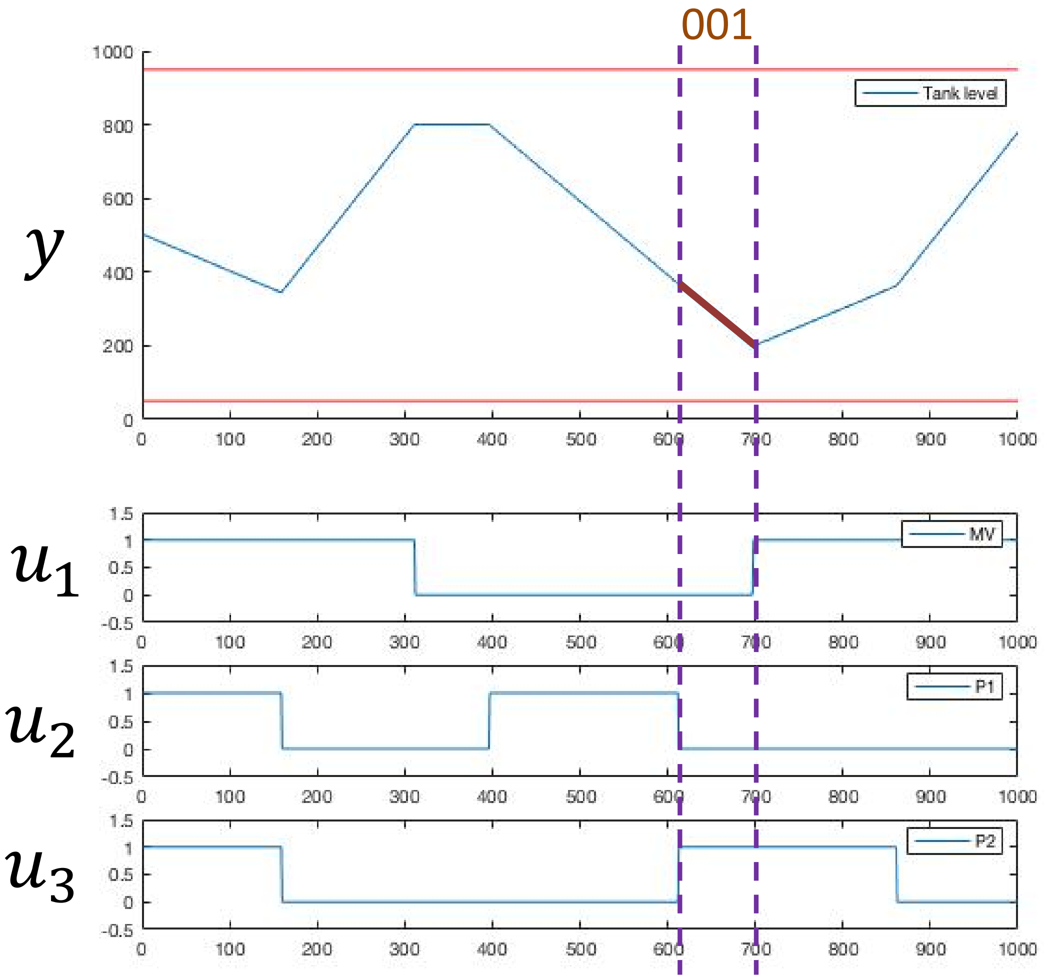
BbTest: Black-Box Modelling



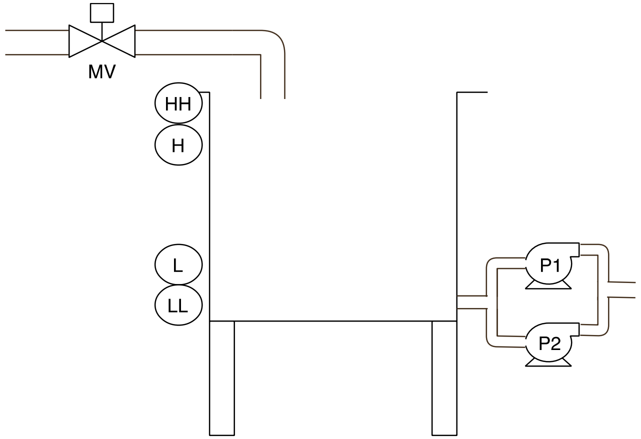
Finite State Machine



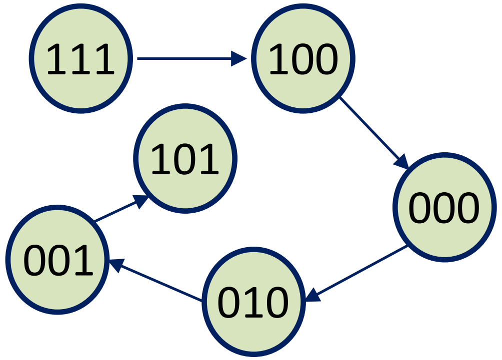
Sensors(y) / Actuators(u)



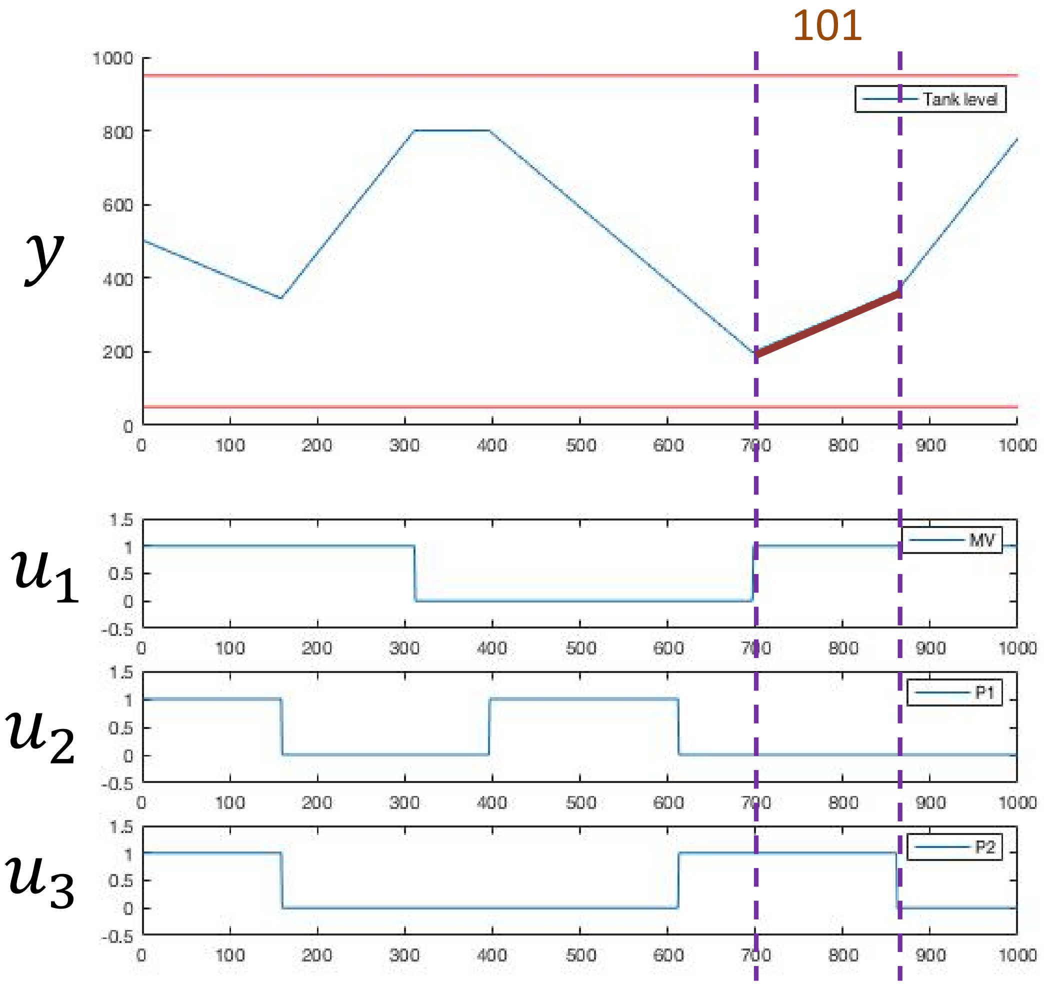
BbTest: Black-Box Modelling



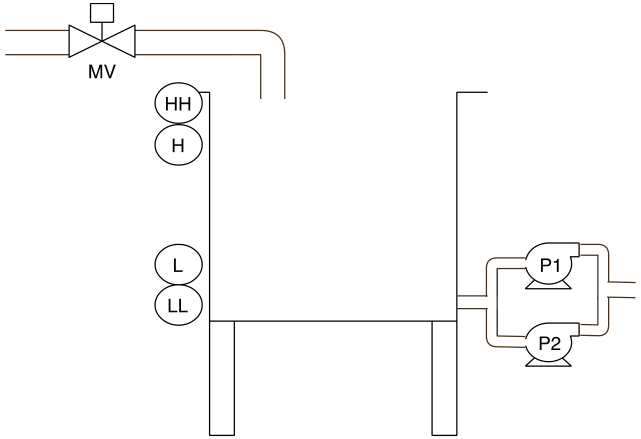
Finite State Machine



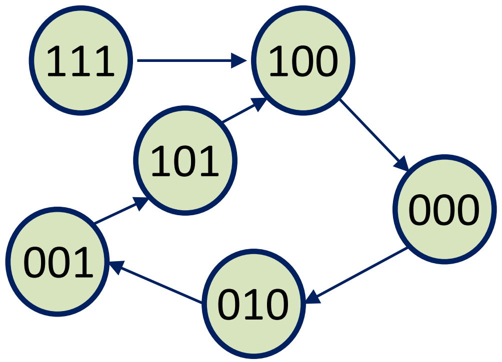
Sensors(y) / Actuators(u)



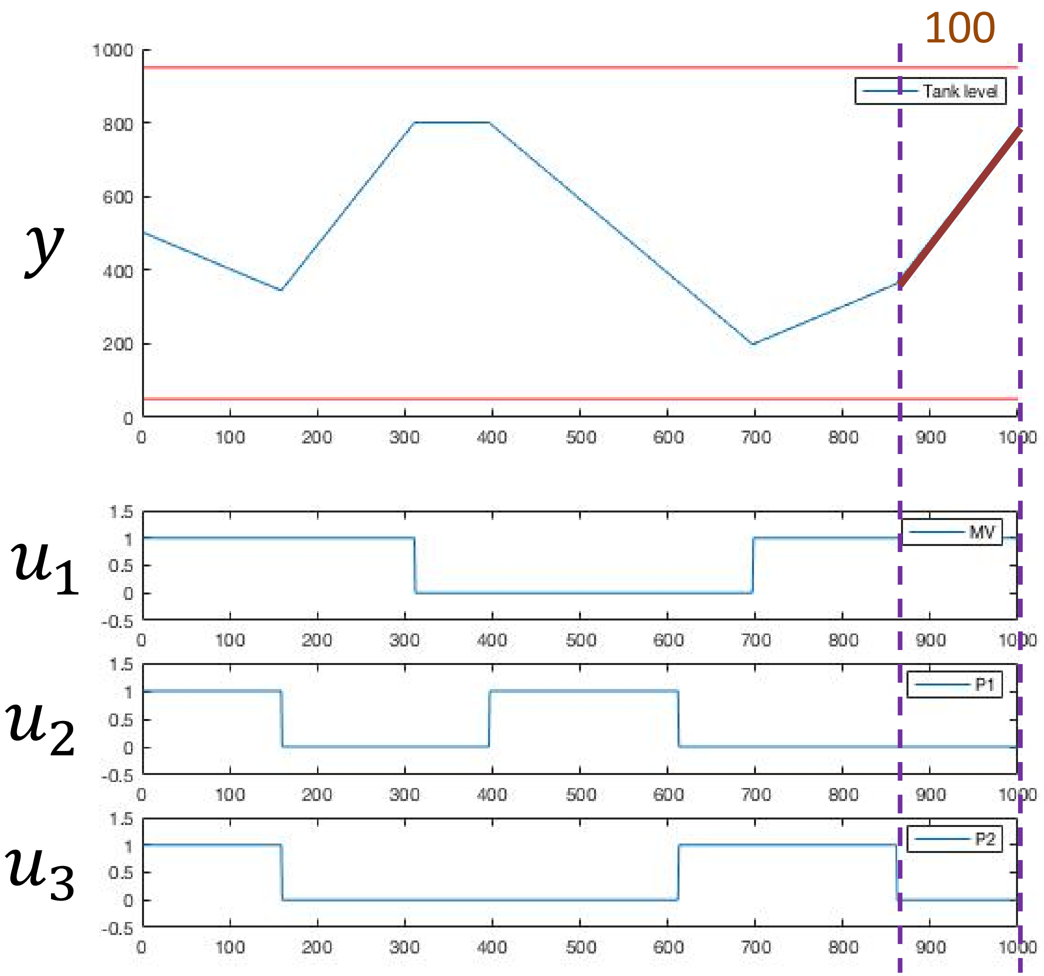
BbTest: Black-Box Modelling



Finite State Machine



Sensors(y) / Actuators(u)



BbTest: Security Metrics

Critical States (Q)

Critical states can be considered as a state where the system operation cannot satisfy minimal safety conditions and threatens product or service quality or human lives.

i.e. Tank overflow, pipe high pressure.

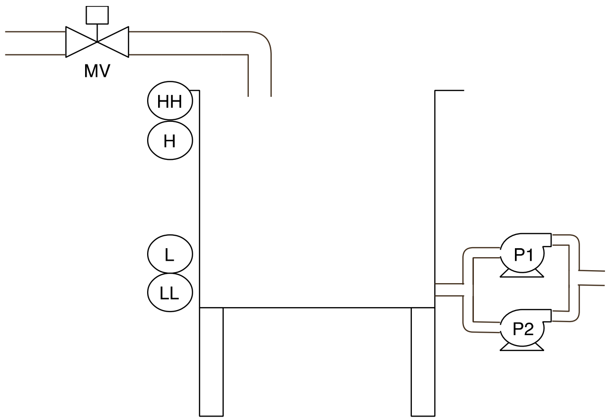
Time-to-critical-state (t_q)

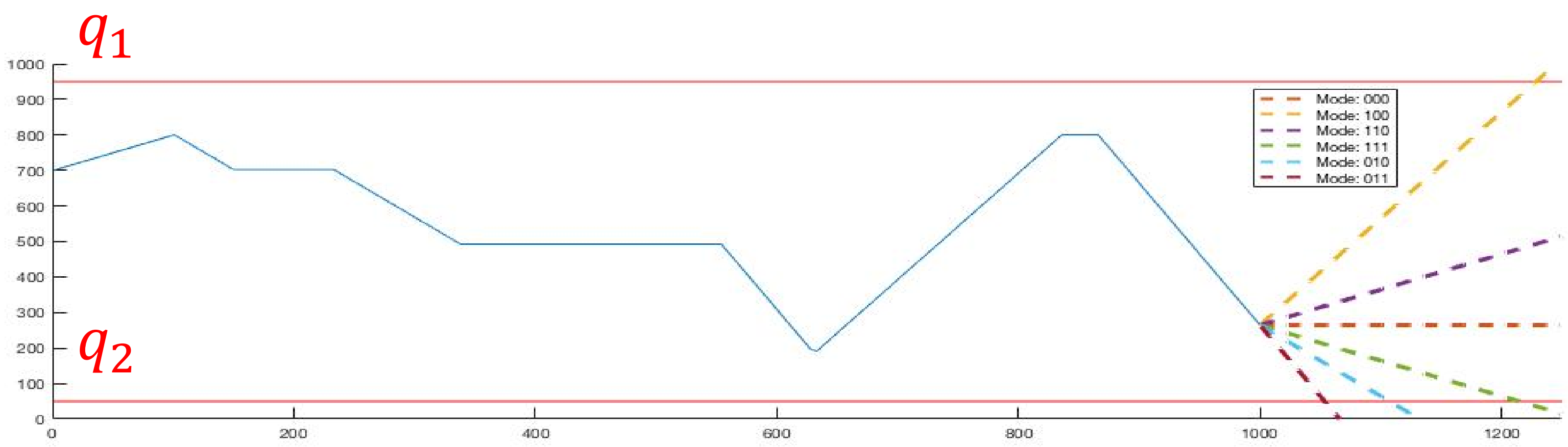
It is the shortest time a system might take to reach its closest critical state. Based on historical registries.

$$r_q = \max\{\dot{x}_l : l \in \bar{L}\}$$

$$t_q = \frac{q - x_q}{r_q}; \quad \forall q \in \bar{Q}$$

BbTest: Critical States & Time-to-Critical-State





Time-to-critical-state (t_q)

Critical states (Q)

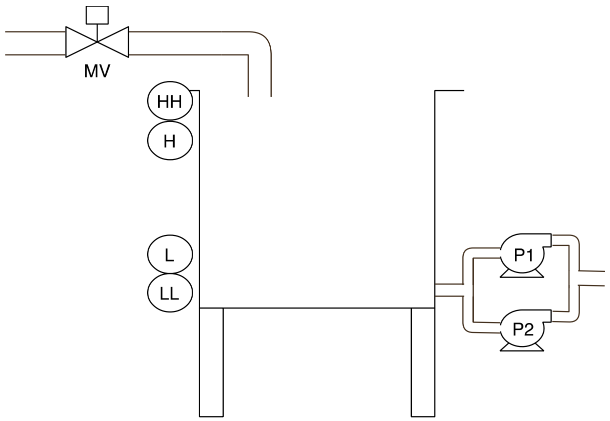
$q_1 : HH$

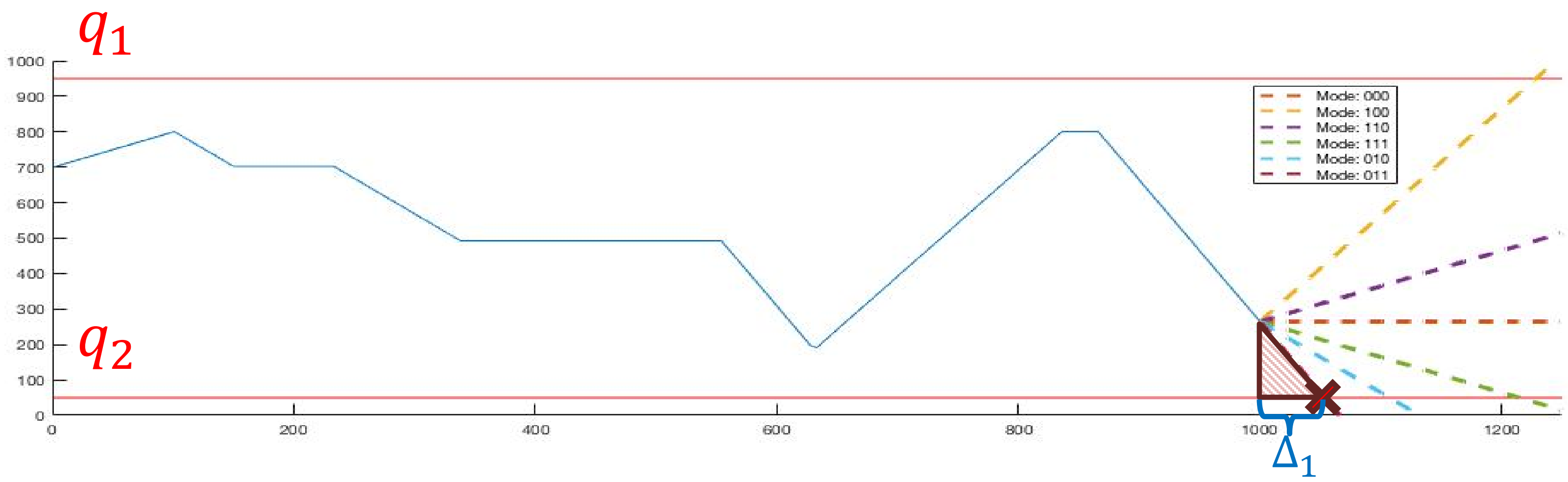
$q_2 : LL$

t_{q1}

t_{q2}

BbTest: Critical States & Time-to-Critical-State





Time-to-critical-state (t_q)

Critical states (Q)

$q_1 : HH$

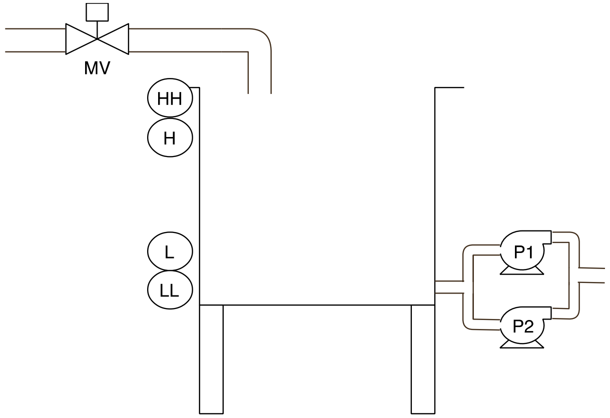
$q_2 : LL$

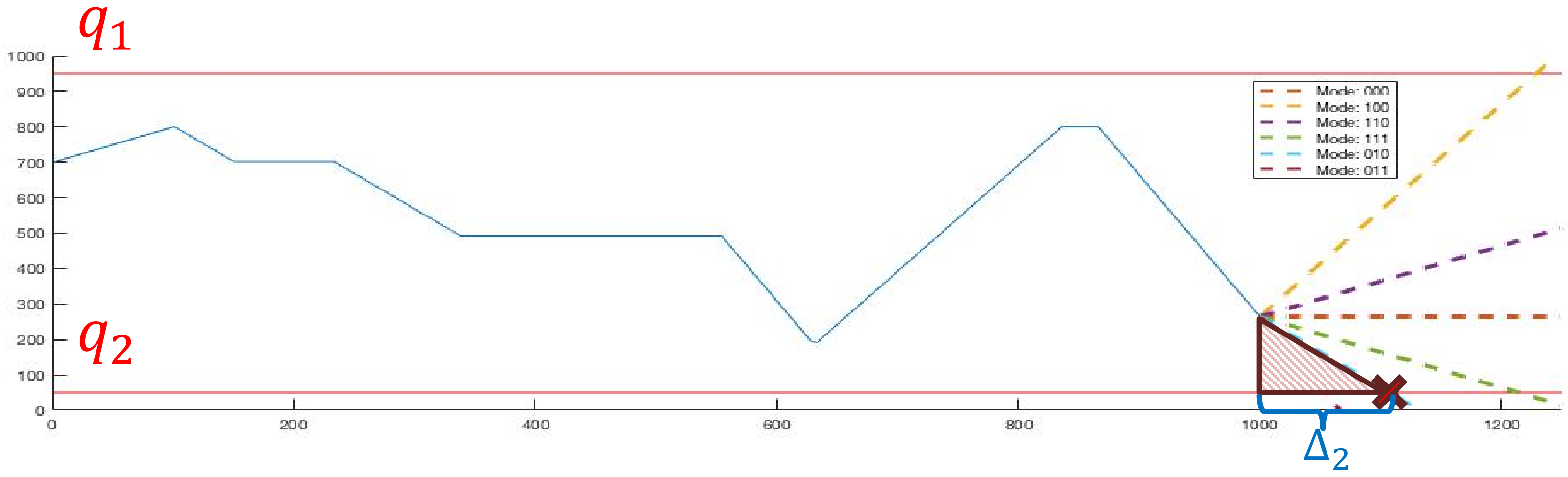
t_{q1}

t_{q2}

Δ_1

BbTest: Critical States & Time-to-Critical-State





Time-to-critical-state (t_q)

Critical states (Q)

$q_1 : HH$

$q_2 : LL$

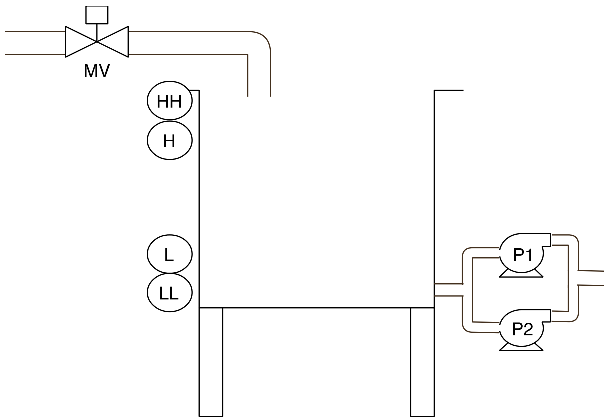
t_{q1}

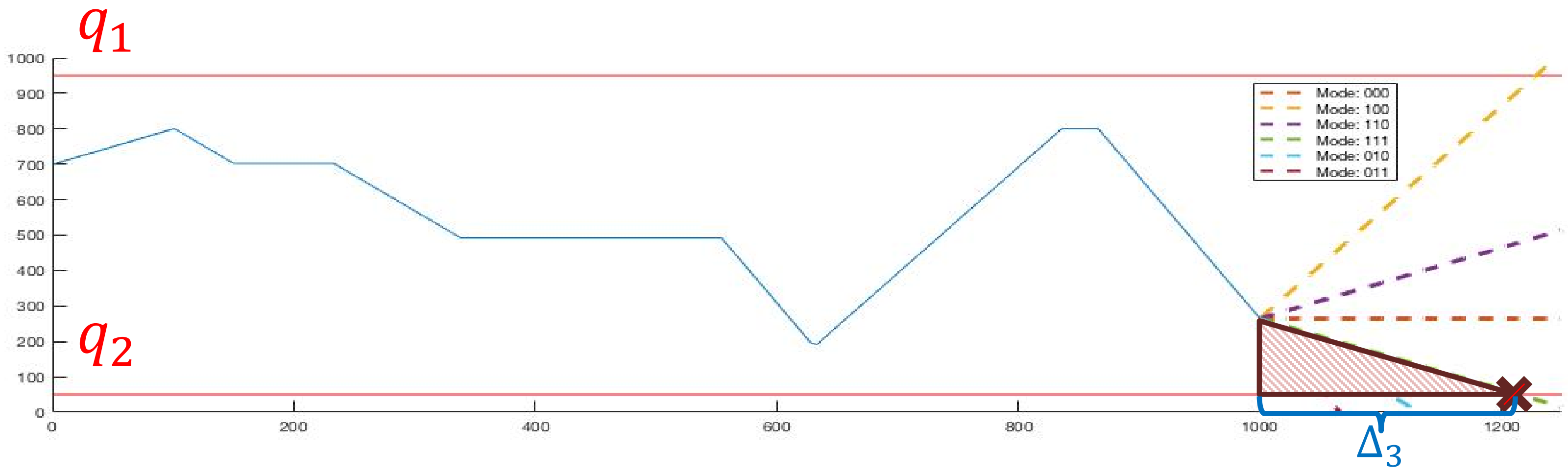
t_{q2}

Δ_1

Δ_2

BbTest: Critical States & Time-to-Critical-State





Time-to-critical-state (t_q)

Critical states (Q)

$q_1: HH$

$q_2: LL$

t_{q1}

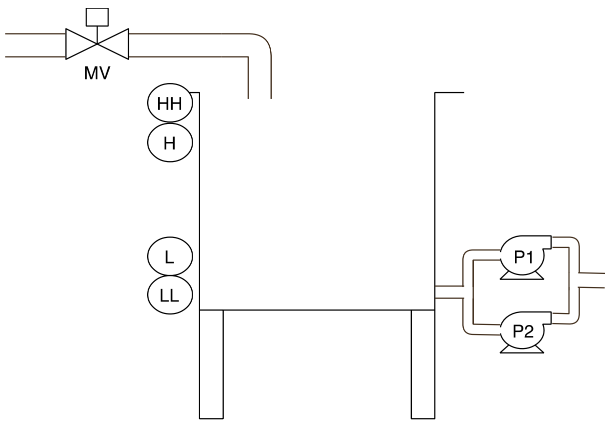
t_{q2}

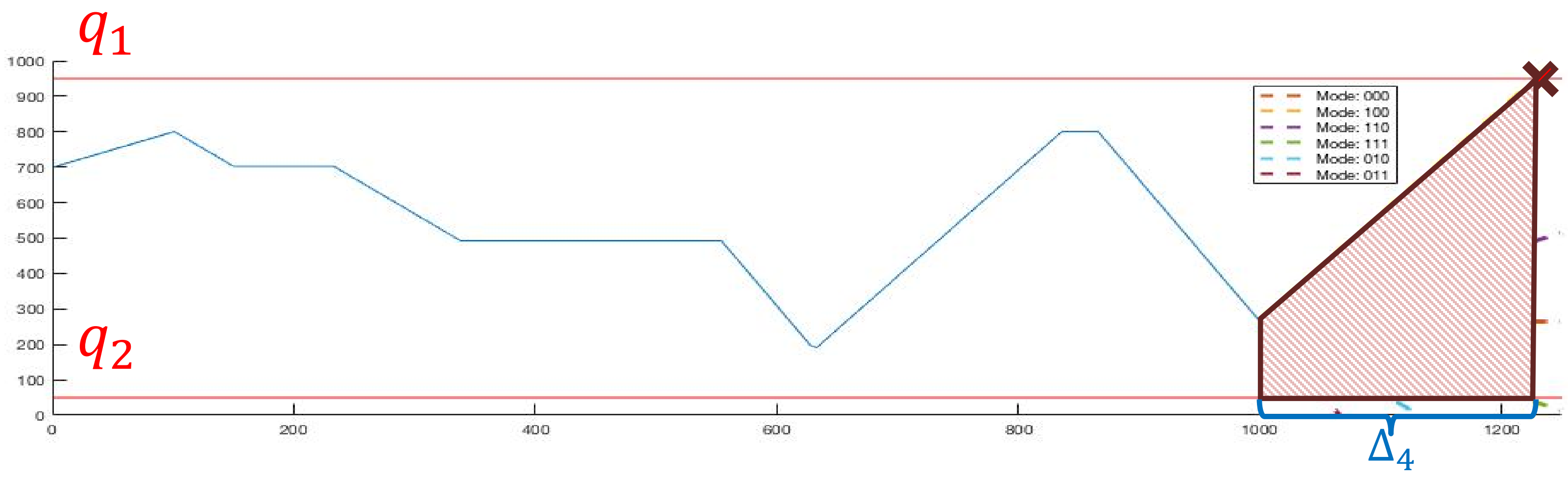
Δ_1

Δ_2

Δ_3

BbTest: Critical States & Time-to-Critical-State





Time-to-critical-state (t_q)

Critical states (Q)

$q_1: HH$

$q_2: LL$

t_{q1}

Δ_4

t_{q2}

Δ_1

Δ_2

Δ_3

NSoE DeST-SC @ iTrust

DeST-SCI National Satellite of Excellence
Design Science and Technology for Secure Critical Infrastructure

NATIONAL RESEARCH FOUNDATION
PRIME MINISTER'S OFFICE
SINGAPORE
Research . Innovation . Enterprise

Thrusts

- Incidence Response: Forensics and recovery
- Attestation and Assessment
- Digital Twinning: water and electric power
- Attack Prevention
- Novel approaches to design secure CI

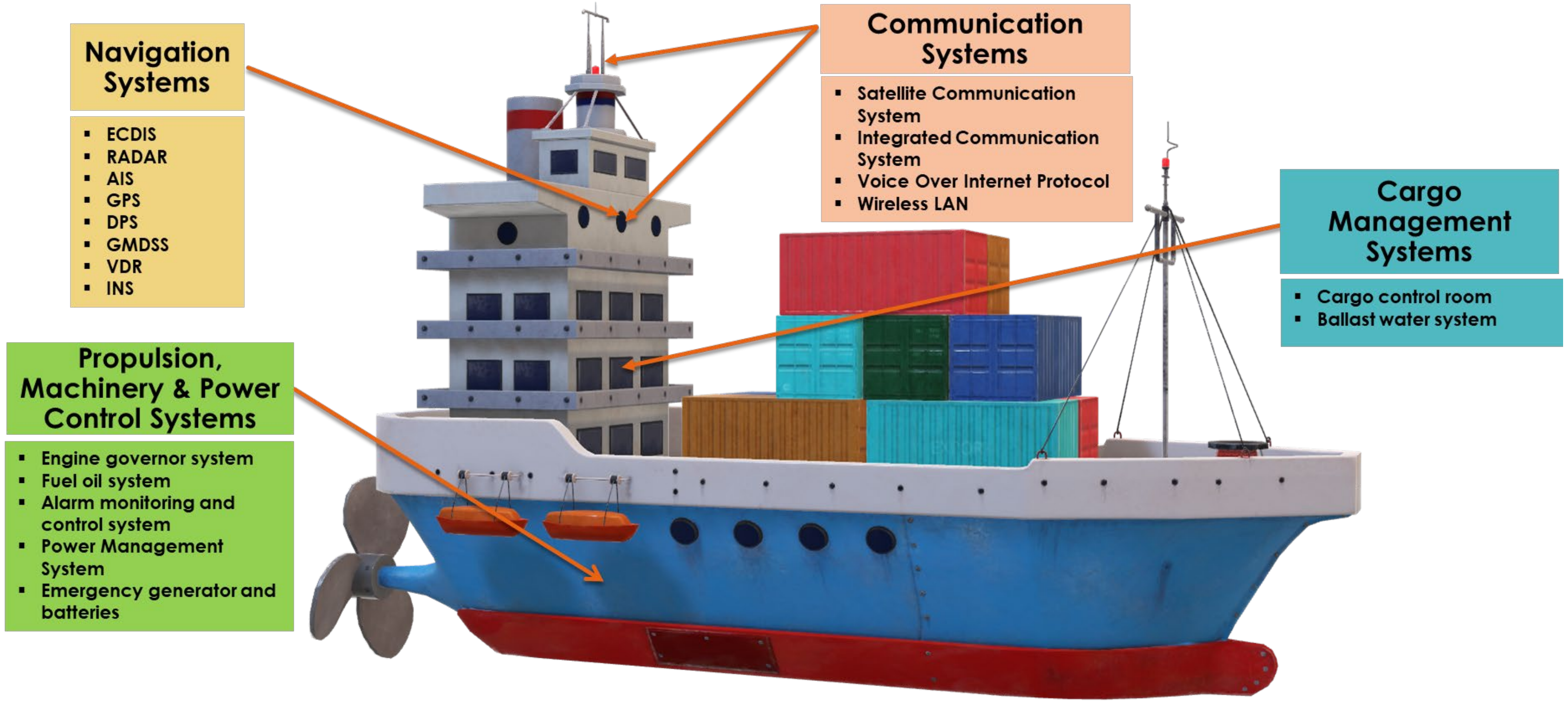
https://itrust.sutd.edu.sg/nsoe-destsci/

New CPS Security Initiative @ iTrust

- Cyber Risk Management in Shipboard OT Systems
- Produce a new guideline for Singapore's context
  - ✓ *Consider the balance of risk vs costs;*
  - ✓ *Take a tiered security approach for major shipboard systems;*
  - ✓ *Make it easy for adoption by ship owners and enforcement by maritime authorities.*

MPA SINGAPORE

SINGAPORE MARITIME INSTITUTE



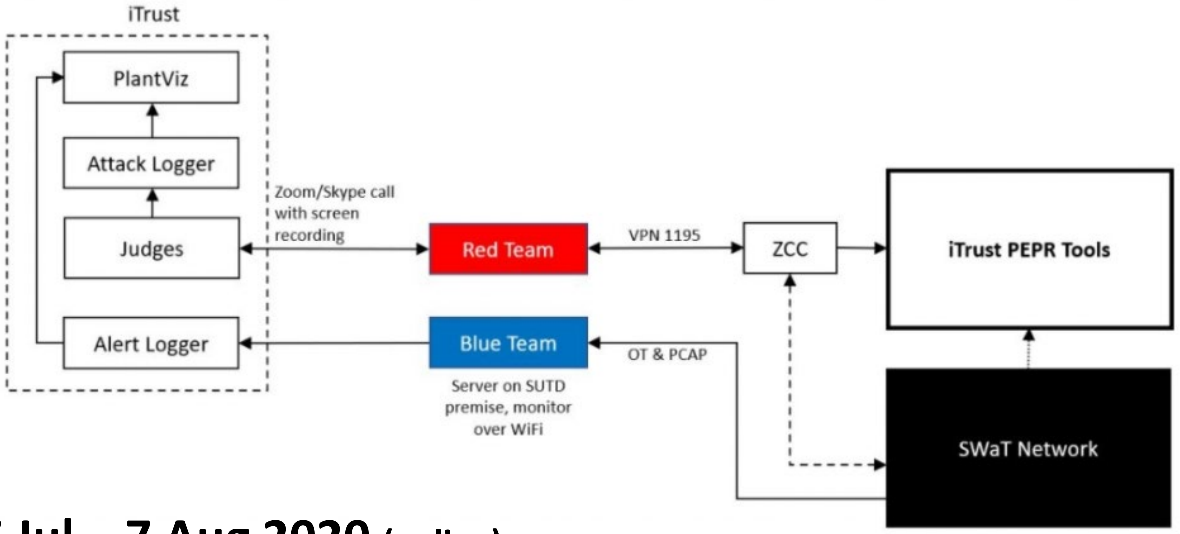
CISS @ iTrust

CISS

Critical Infrastructure Security Showdown

2019

Critical Infrastructure Security Showdown



26 – 30 Aug 2019

- 6 x Red Teams (Asia, Europe, America)
- 5 x Blue Teams (commercial vendors)
- iTrust: 1 x Red Team, 1 x Blue Team
- https://itrust.sutd.edu.sg/ciss-2019/

27 Jul – 7 Aug 2020 **(online)**

- 16 x Red Teams (Asia, Europe, America)
- 10 x Blue Teams (commercial vendors)
- iTrust: 1 x Red Team, 1 x Blue Team
- https://itrust.sutd.edu.sg/ciss-2020-ol/

Participating Red Teams in CISS2020-OL

CTF.SG EY JYVSECTEC KPMG

NSHC SECURITY RED TEAM Cyber Security Services

ST Engineering

Other teams:

- 6 private teams
- 3 student teams
- 1 iTrust team

iTrust @ Locked Shields 2021

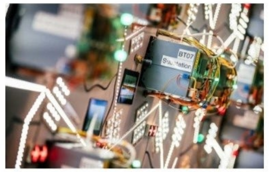
iTrust
Centre for Research in Cyber Security

CCDCOE

About us Research Library Training Exercises CyCon Careers News

International Live-Fire Cyber Defence Exercise Introduces New Highlights

Events



Locked Shields 2021

13th April, 2021

iTrust is proud to cooperate with CCDCOE for Locked Shields 2021: https://ccdcoe.org/news/2021/worlds-largest-international-live-fire-cyber-exercise-to-be-launched-next-week-2/

LOCKED SHIELDS 2021

Locked Shields 2021 **Key Facts:**

- → Live-fire = real-time Red Team vs. Blue Team exercise
- → 22 BTs participating with an average 40 experts in each team.
- → About 5000 virtualised systems subject to more than 4000 attacks
- → Involves regular business IT, cyber physical, and military systems
- → Integrates technical and strategic decision-making elements within a complex information environment
- → Hosted on an innovative Cyber Range managed by foundation CR14, the Estonian hub for cyber defence research and development
- → A truly international exercise with the total of more than 2000 participants from 30 nations taking part from their home countries
- → For the first time, the exercise controllers will also be distributed globally with only a small number of core personnel based in Tallinn

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) is a NATO-accredited cyber defence hub focusing on research, training, and exercises. The CCDCOE has representatives from most NATO nations and many partners across the globe based in Tallinn, Estonia. The Centre provides a comprehensive cyber defence capability, with expertise in the areas of technology, strategy, operations, and law. However, the CCDCOE is not an operational unit nor part of NATO´s command structure.

Locked Shields 2021 is organised by the CCDCOE in cooperation with NATO Communications and Information Agency, the Estonian Ministry of Defence, the Estonian Defence Forces, Siemens, Ericsson, TalTech, CR14, Bittium, Clarified Security, Arctic Security, Cisco, Stamus Networks, SpaceIT, Sentinel, the Financial Service Information Sharing and Analysis Center (FS-ISAC), US Defense Innovation Unit, Microsoft, Atech, Avibras, SUTD iTrust Singapore, The European Centre of Excellence for Countering Hybrid Threats, NATO Strategic Communications Centre of Excellence, European Defence Agency, Space ISAC, the US Federal Bureau of Investigation (FBI), STM, VTT Technical Research Centre of Finland Ltd, NATO M&S COE and PaloAlto networks.

CCDCOE
NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE

7th ACM Cyber-Physical System Security Workshop (CPSS 2021)

held in conjunction with ACM AsiaCCS'21
Hong Kong, China, 7 June 2021

Steering Committee

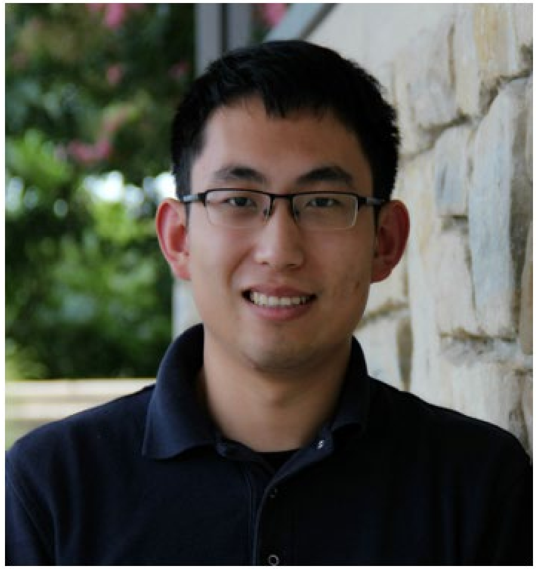
Dieter Gollmann (Hamburg University of Technology, Germany)
Ravishankar Iyer (UIUC, USA)
Douglas Jones (UIUC, USA)
Javier Lopez (University of Malaga, Spain)
Jianying Zhou (SUTD, Singapore) – Chair

Program Chairs

Mauro Conti (University of Padua, Italy)
Nils Ole Tippenhauer (CISPA, Germany)

https://spritz.math.unipd.it/events/2021/CPSS/

Keynotes



Qi Alfred Chen (University of California, Irvine, USA)

Towards Secure and Robust Autonomy Software in Autonomous Driving and Smart Transportation

Christina Pöpper (New York University Abu Dhabi, UAE)

High we Fly: Wireless Witnessing and Crowdsourcing for Air-Traffic Communication Security

Workshop Chairs:

Chenglu Jin, CWI Amsterdam, The Netherlands
Michail Maniatakos, New York University Abu Dhabi, UAE

Publicity Chairs:

Zheng Yang, Singapore University of Technology and Design, Singapore

Contact: chenglu.jin@cwi.nl

Springer

Lecture Notes in Computer Science
LNCS LNAI LNBI

https://cimssworkshop.github.io/

Recruitment of RF @ SUTD

iTrust
Centre for Research in Cyber Security

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

Thank You !

jianying_zhou@sutd.edu.sg

Welcome to visit iTrust.