11TH INTERNATIONAL CONFERENCE
ON CRITICAL INFORMATION
INFRASTRUCTURES
SECURITY

10-12 October 2016
UIC HQ Paris

CRITIS
2016

A Dataset to Support Research in the Design of Secure Water Treatment Systems

Jonathan Goh, **Sridhar Adepu**, Khurum Nazir Junejo and Aditya Mathur

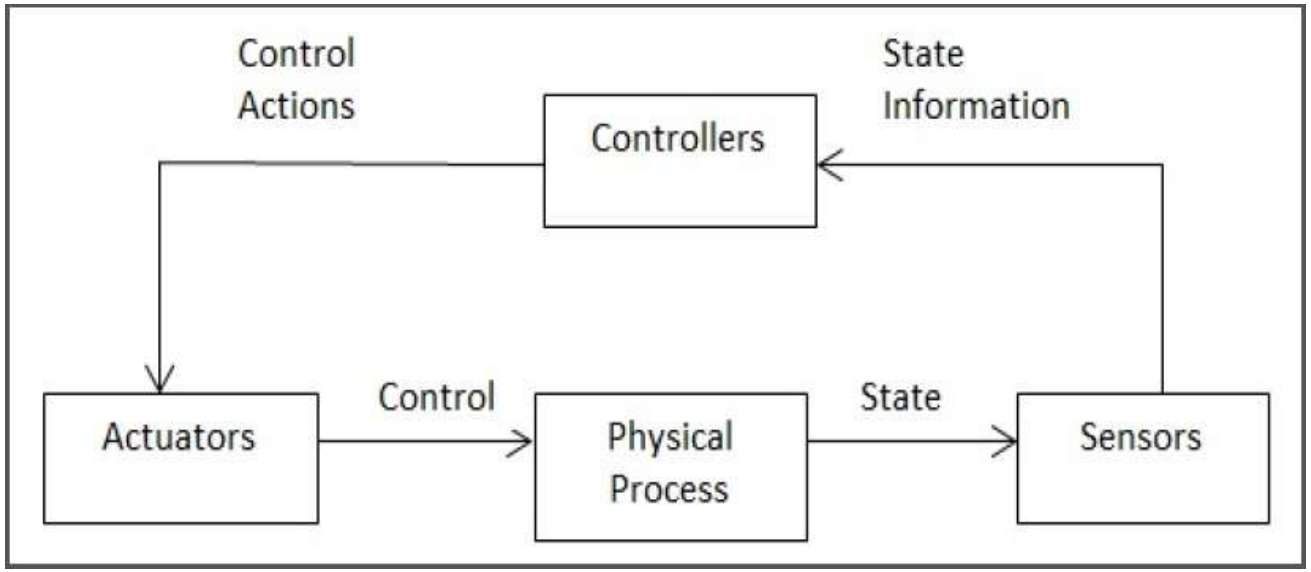
Singapore University of Technology and Design

iTrust
Centre for Research
in Cyber Security

SUTD
SINGAPORE UNIVERSITY OF
TECHNOLOGY AND DESIGN
Established in collaboration with MIT

Cyber Physical Systems

- CPS is a combination of physical process, computation and communication.
- CPS are across different sectors: energy, water, transportation, healthcare, manufacturing, etc.



Water treatment Systems

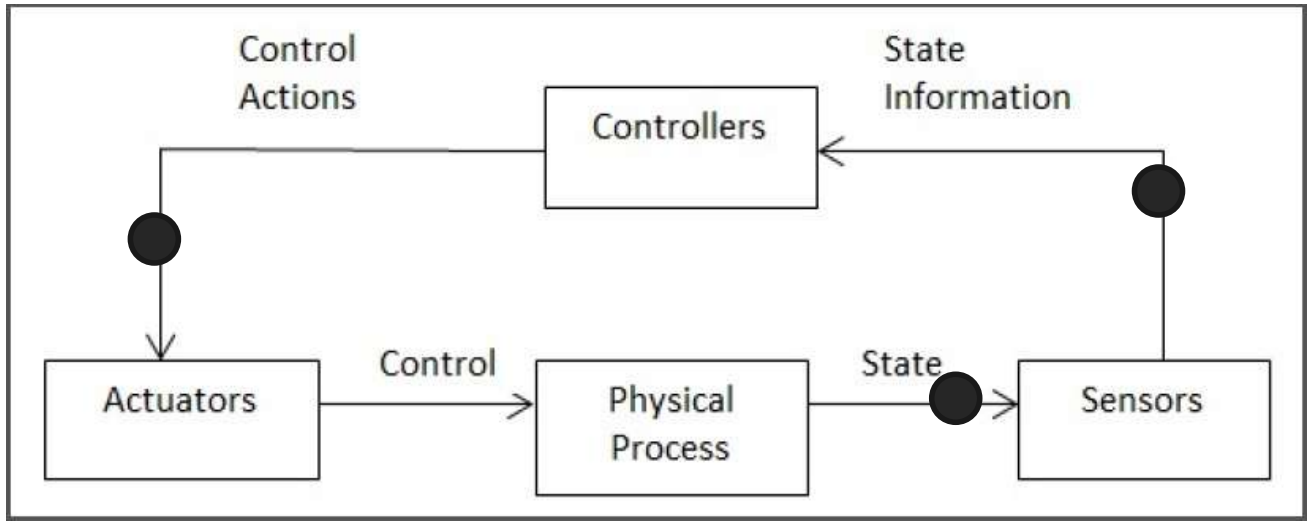
Hyflux Ltd.'s SingSpring Desalination Plant in Singapore. PHOTO: BLOOMBERG

The Secure Water Treatment (SWaT) testbed at the Singapore University of Technology and Design

Attacks on Cyber Physical Systems

- “Cyber attack" refers to an attempt at disturbing the state of CPS through its communication network and affect system behaviour with an intent to cause some economic harm.

  - Moaroochy shire: 2000
  - Stuxnet: 2010
  - Ukraine black out: 2015



Problem

- Machine learning researchers are learning physical behaviour of the Cyber Physical Systems (CPS), in order to asses the safety and security of CPS.
- Verification researchers are modelling CPS using formal models to verify safety, security of CPS.
- These researchers have a limited datasets available to advance this field of study.

Datasets in CPS systems

- Limited availability of operational data sets in this research community to advance the field of securing CPS
  - DARPA Intrusion Detection Evaluation Dataset
  - NSL-KDD99 Dataset
- These are simulations in a network environment.

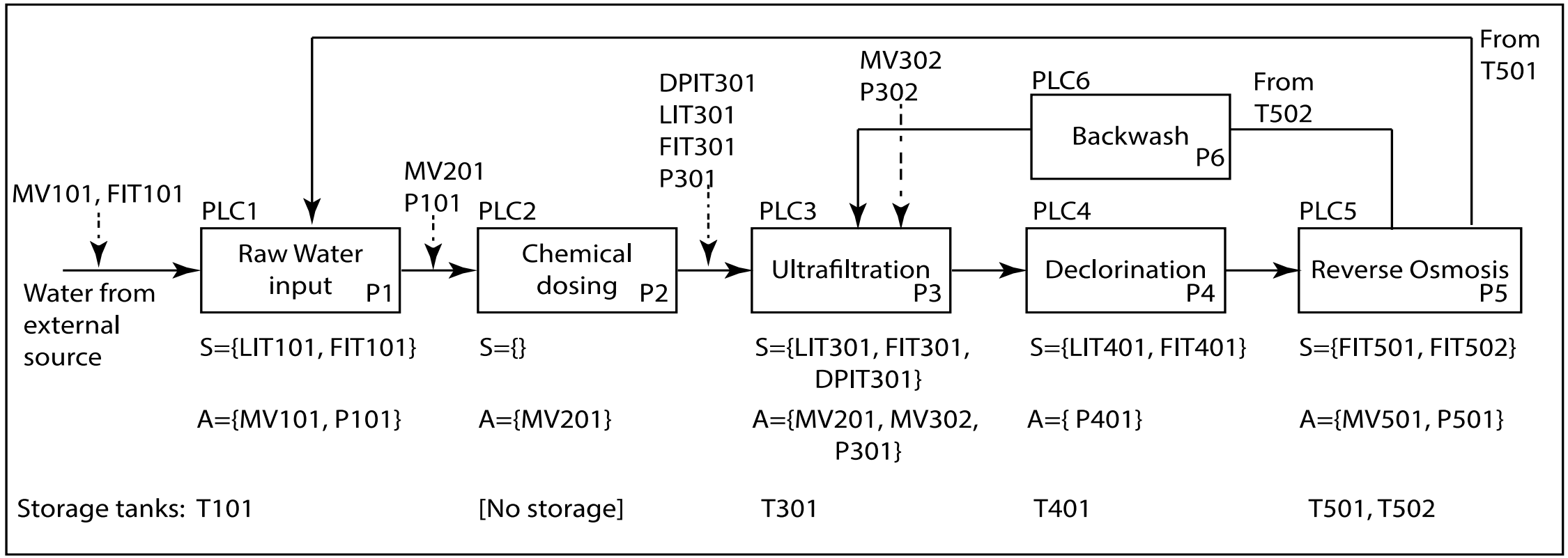
- Mississippi State University: Power, Gas, Water testbeds.
  - However, power dataset is simulated data and water, gas datasets were obtained from a very small scale laboratory testbed.

Contributions include

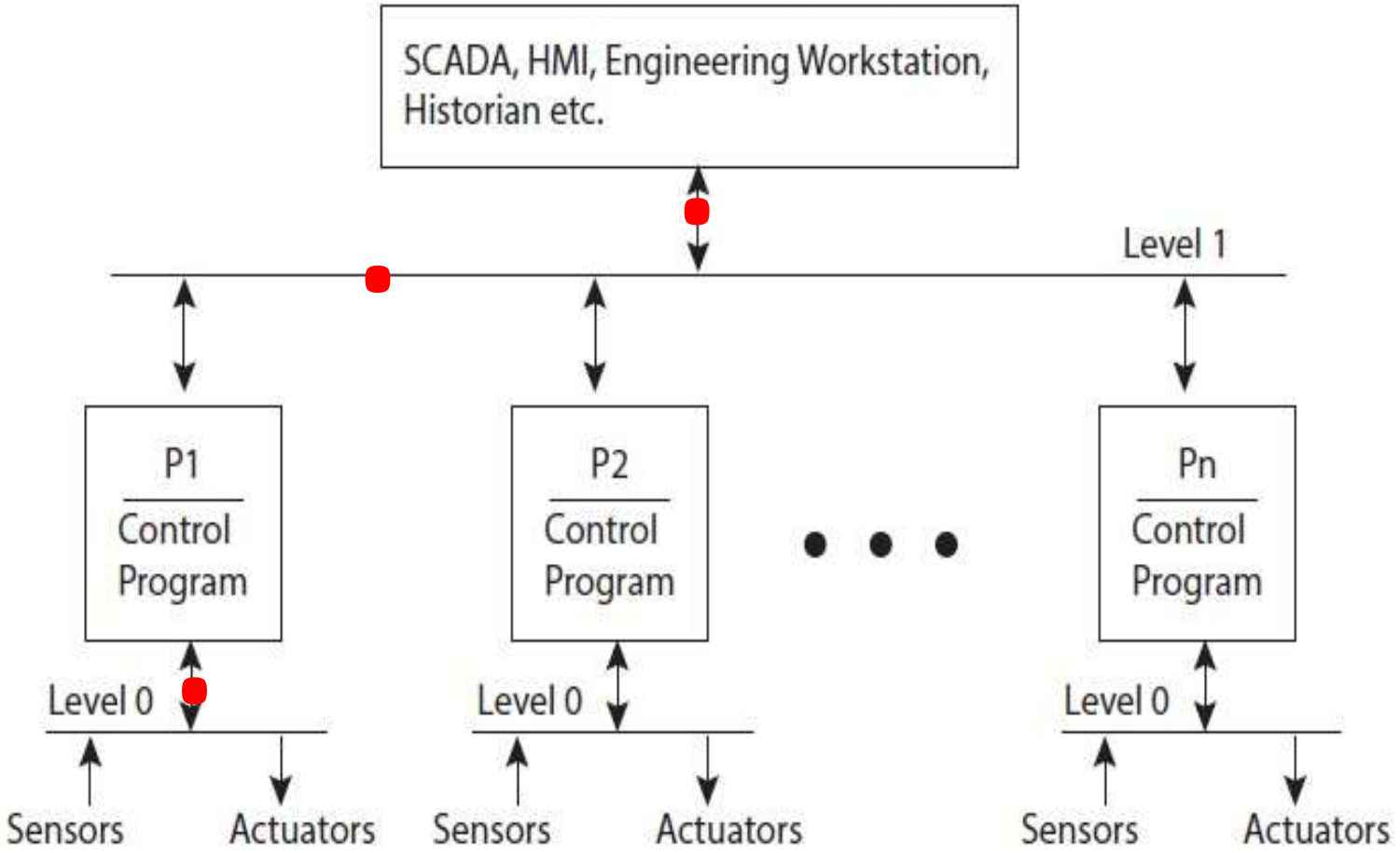
- Provide a realistic dataset
  - To design and evaluate CPS defence mechanisms.
  - Test mathematical models and formal models of CPS.

- A large scale labelled-normal and attack-dataset collected from a realistic testbed for sufficient complexity.
  - Includes both network traffic and physical properties of data.

Secure Water Treatment (SWaT)



Architecture of SWaT: Communication



Number of Attacks

- A total of 36 attacks were launched during the data collection process.

- Which include:
  - Bias attacks
  - Replay attacks
  - Single point attacks
  - Multiple point attacks

Data collection process

- Data collected continuously for 11 days.
- All tanks in SWaT were emptied prior to starting data collection; i.e. the data collection process starts from an empty state of SWaT.
- During first seven days SWaT was operating normally.
- During the remaining four days SWaT was under attack
- SWaT was either allowed to reach its normal operating state before another attack was launched or the attacks were launched consecutively.

Physical Properties of SWaT

- In total, 946,722 samples comprising of 51 attributes were collected over 11 days.

- Attributes include:
  - Sensor readings: water tank level, flow meter's, water properties, pressure.
  - Actuator readings: water pump, motorized valves, Ultraviolet De-chlorinator

Network Traffic

Category
Date
Time
Origin
Source IP
Destination IP
Protocol . . .

Labelling data

- Start time ----Time when attack starts
- End time ----Time when attack ends
- Attack Points ----Sensors or actuator which will be compromised
- Start State ----Current status of the point
- Attack ----Description of attack
- Attack Value---- Substituted value of sensor (based on the attack)
- Attacker's Intent ----The intended affect of the attack

Conclusion

- This paper presents a dataset to support research in the design of secure Cyber Physical Systems.
- Real industrial CPS facilities may not be able to provide datasets, where datasets include the process was under attack, as faults or attacks can only be assumed at best.
- Our goal is to make the collection of CPSs datasets an on-going process to benefit researchers.
- The data collected will be continuously updated to include datasets from our new testbeds as well as new attacks derived from our research team.

Thank You!

CRITIS 2016

Author contact information:

- Jonathan_goh@sutd.edu.sg
- adepu_sridhar@mymail.sutd.edu.sg
- aditya_mathur@sutd.edu.sg

iTrust
Centre for Research in Cyber Security

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN
Established in collaboration with MIT