SWaT: A Water Treatment Testbed for Research and Training on ICS Security

Nils Tippenhauer

Aditya P Mathur

iTrust

Center for Research in Cyber Security

Singapore University of Technology and Design

Singapore

CySWater 2016
Vienna

April 11, 2016

Projects CYPRO and ASPIRE: Long Term Goal

Design robust mechanisms for defending Cyber Physical Systems.

Focus Areas

Robots and robot swarms

Water treatment and distribution systems

Electric power generation, transmission and distribution systems

Testbeds

Testbeds

Testbeds for Research Support

- Water treatment [Operational]
- Water distribution [Operational by April 15, 2016]
- Electric power generation, transmission and distribution [Operational by end of 2016]
- IoT [Operational by June 2016]

Research focus

- Creation of attacker and attack models for CPS
- Understanding the impact of attacks
- Design of robust detection mechanisms
- Design of ultimate defense mechanisms

Collaboration with MIT and Imperial

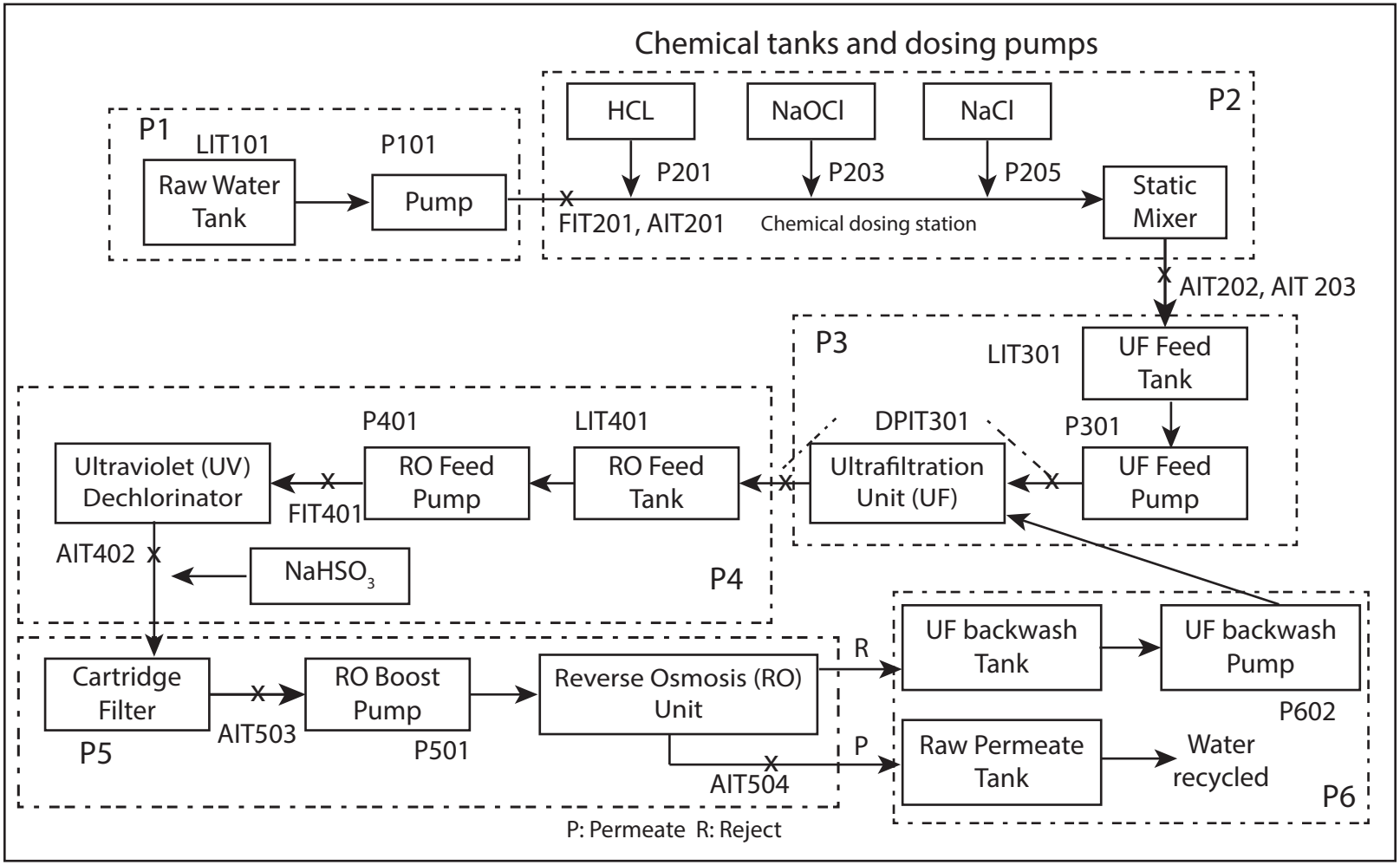
SWaT

iTrust
Centre for Research
in Cyber Security

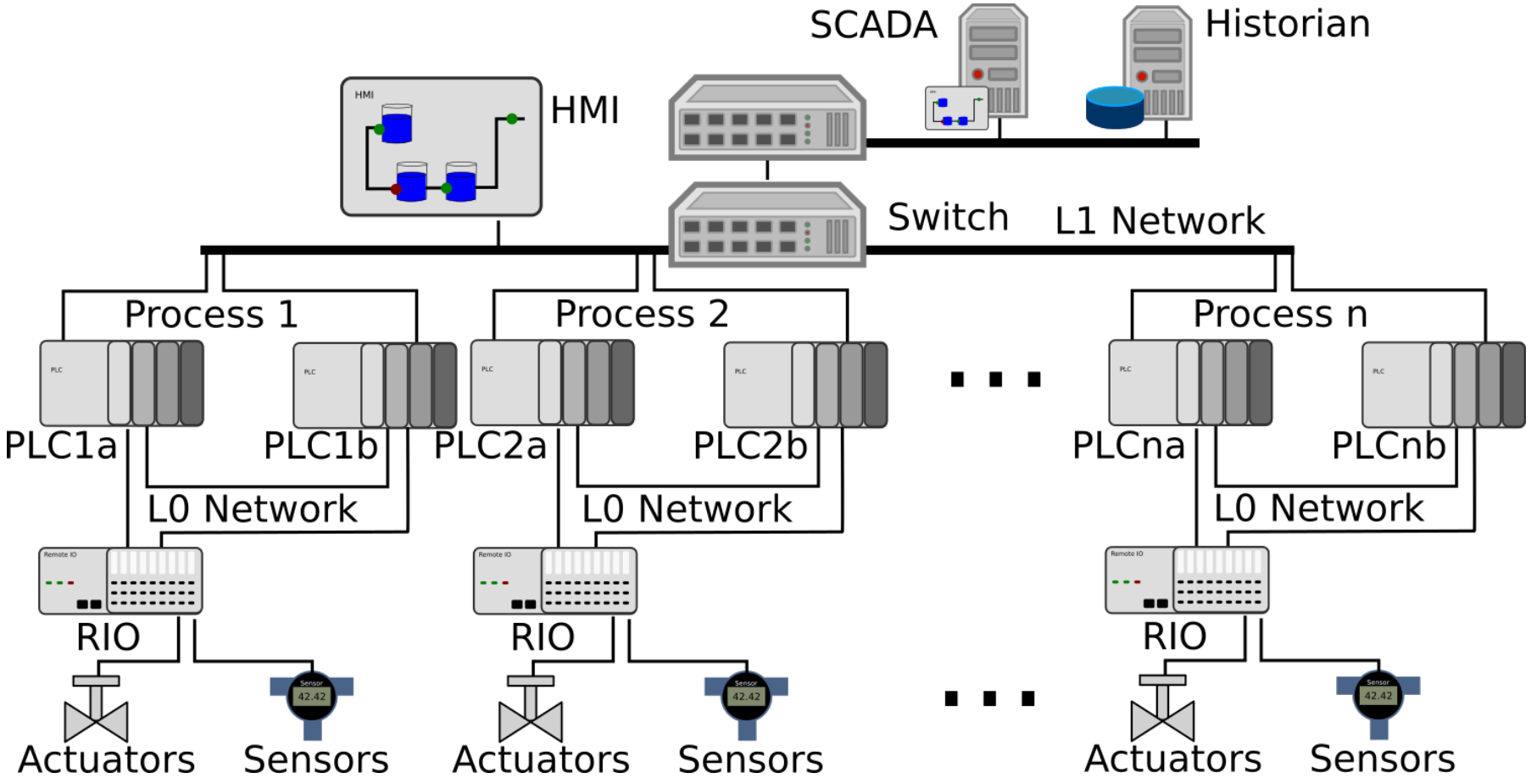
SINGAPORE UNIVERSITY OF
TECHNOLOGY AND DESIGN
Established in collaboration with MIT

https://www.youtube.com/watch?v=2r1ctjULCnI&feature=youtu.be

SWaT: Secure Water Treatment Testbed



SWaT: Communications



Attacks

Attack: Reconnaissance

- Access to local plant communication network
- Wireshark and Zenmap used
- Mapped local networking setup; determined available services.
- Anonymous FTP login enabled the discovery of hidden
- files that appear to contain the complete HMI configuration
- Sensor and actuator commands captured

Attack: Compromise through wireless network

- Attacker in physical proximity (within WiFi range)
- Access point: MOXA AWK-5222-EU; WPA2 security scheme with pre-shared keys.
- Perform brute-force attack or evil twin attack.
- Web interface for PLC configuration had a default password using which WiFi password can be obtained quickly.
- Sensor and actuator commands captured

Attack: Compromise through Direct Physical Access

- Attacker has direct physical access
- Re-wiring the network possible
- SD card slots can be used to update control logic
- Sensor and actuator commands captured

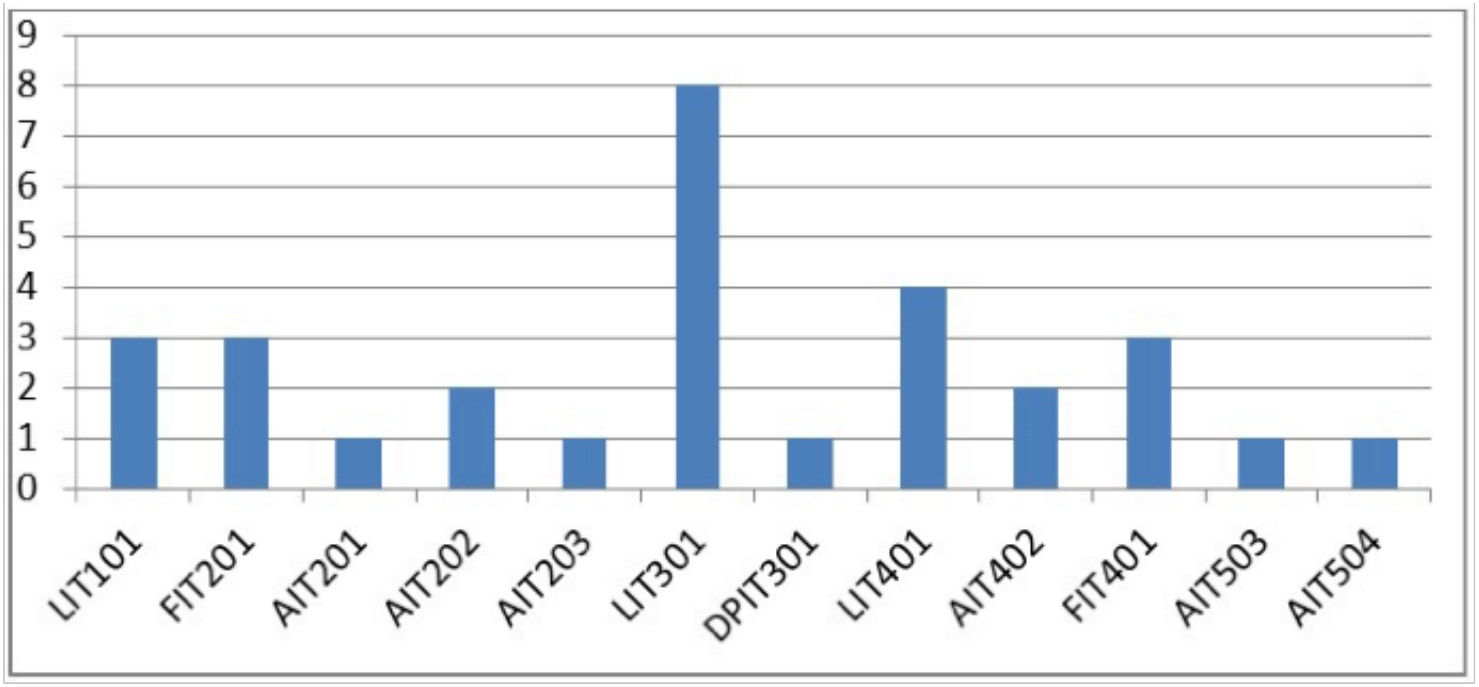
Impact analysis

Single Point Attacks

Attack point	Description	Start state (s_0)	Attack	Actuators(s) effected	Impact
P1: Control raw water intake					
LIT101	Raw water tank level	800mm	200mm	P101	Tank overflow
		400mm	1000mm	MV101, P601	Stops flow of water into the raw water tank
P2: Chemical dosing control					
FIT201	Flow transmitter	2.5cm/hr	0.7cm/hr	P201, P203, P205	Disturb chemical dosing
AIT201	Conductivity analyzer	$> 250\mu s/cm$	$< 250\mu s/cm$	P201	Conductivity altered
AIT202	pH Analyzer	>7.05	< 6.95	P203, P601	pH level altered
AIT203	ORP analyzer	420mV	450mV	P205	ORP altered

Impact: Components affected

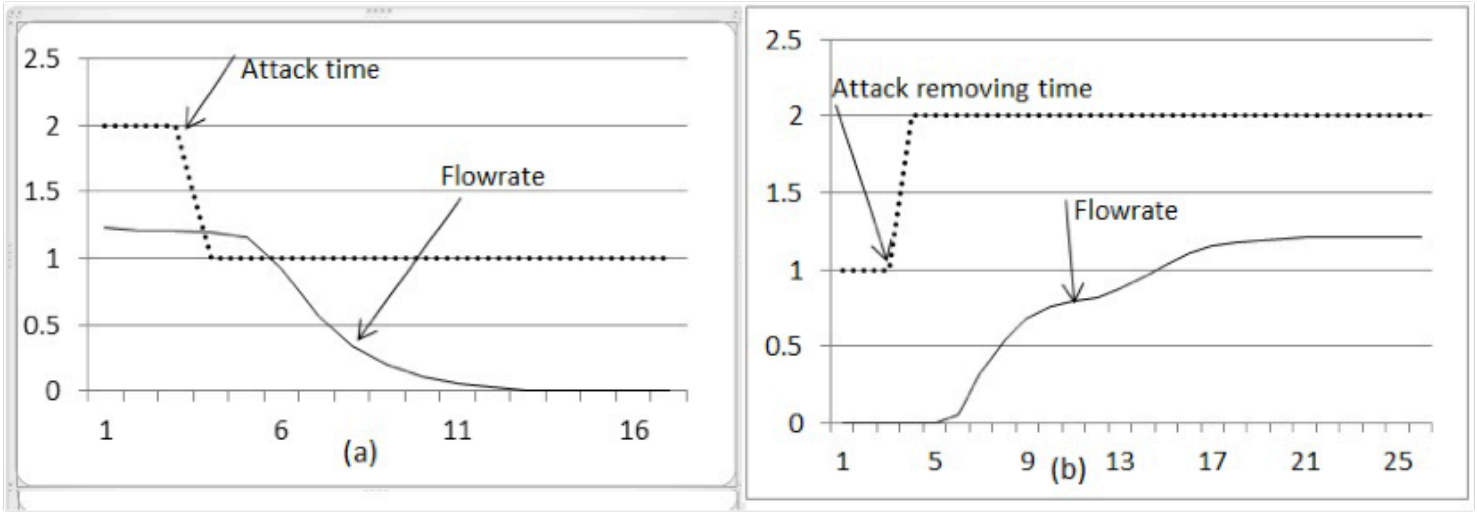
Q: How does an attack on a single component affect the remaining components?



Prioritize security efforts.

Flow rate reduction

Q: How does the flow rate change when LIT401 is attacked?



Overflow if attack not detected

Detection and defense

- Detection mechanisms for SSSP and SSMP attacks have been developed and tested to be found effective.

- Detection mechanisms for MSSP and MSMP attacks is under design.

- Reconfiguration control for defense upon attack detection is under design.

Summary

- Attacker model enables a clear specification of the space of cyber and physical attacks feasible on a CPS.
- Attack space is potentially infinite, an attacker model allows limiting the attack space, by constraining to a finite number of points.
- Limiting the attack space allows a designer of defense mechanisms to focus on finite domains for attack design.
- Realistic testbeds allow extensive experimentation with realistic attacks and the design of effective detection and defense mechanisms.

Questions?