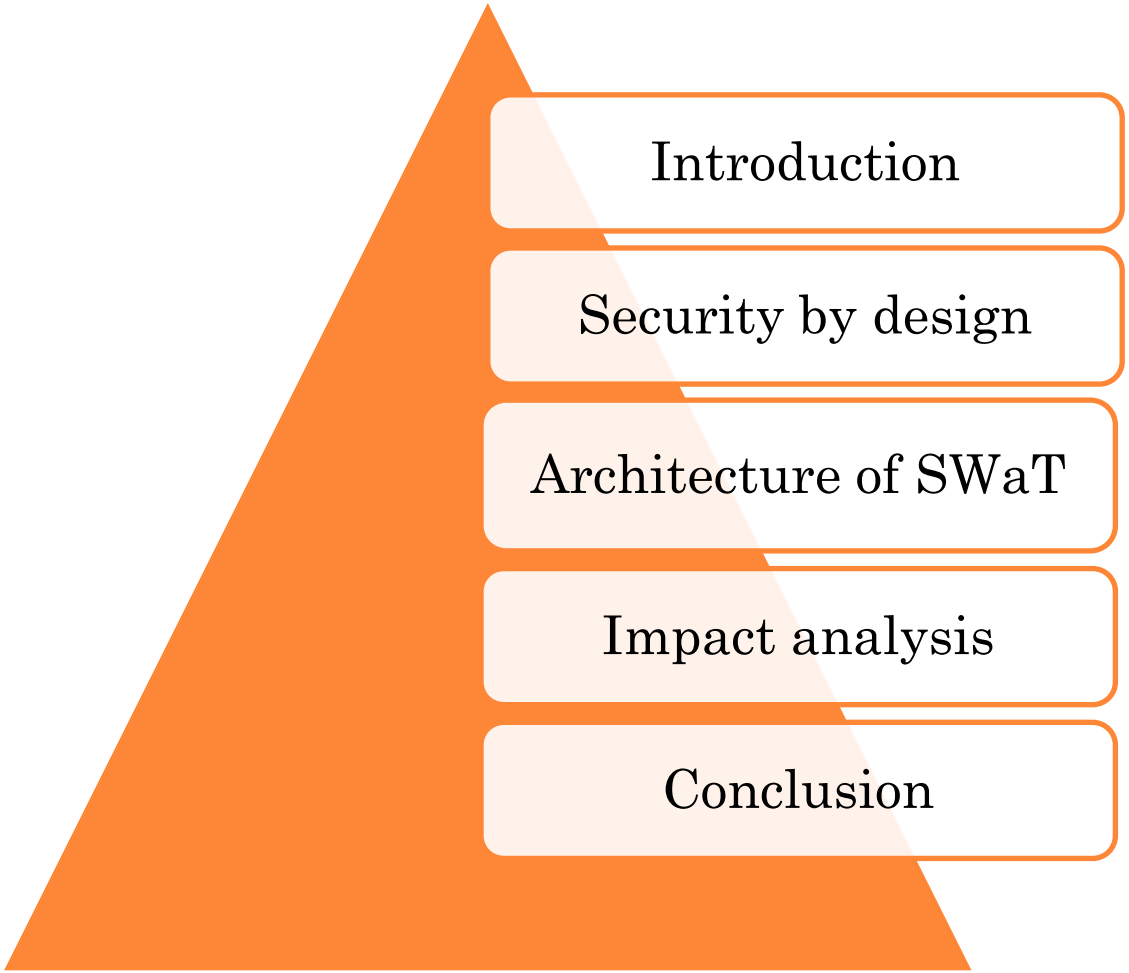
Introducing Cyber Security at the Design Stage of Public Infrastructures: A Procedure and Case Study

Sridhar Adepu and Aditya Mathur
iTrust Centre for Research in Cyber Security
Singapore University of Technology and Design

CSDM Asia, February 24-26, 2016

Outline

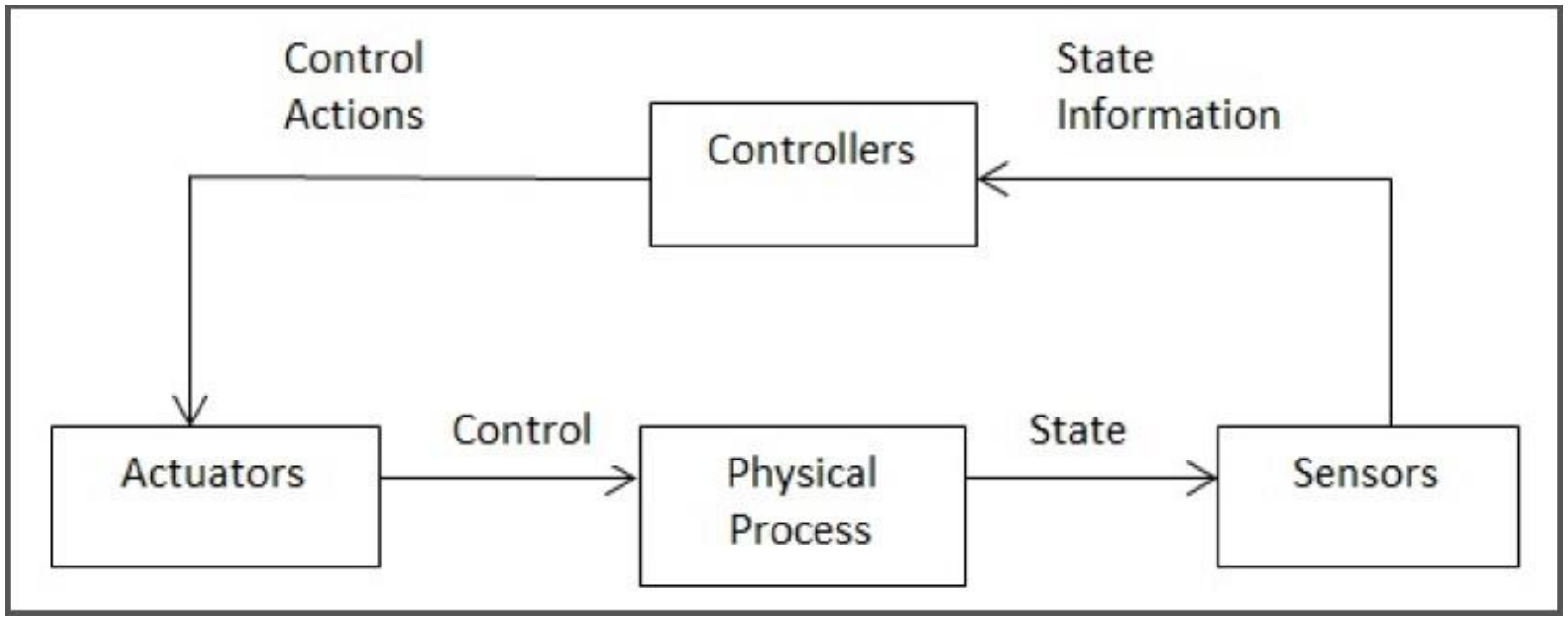

Introduction
Security by design
Architecture of SWaT
Impact analysis
Conclusion

Contributions

- A scalable and automatable security-by-design procedure to understand the response of a Cyber Physical System to attacks on its communications infrastructure.

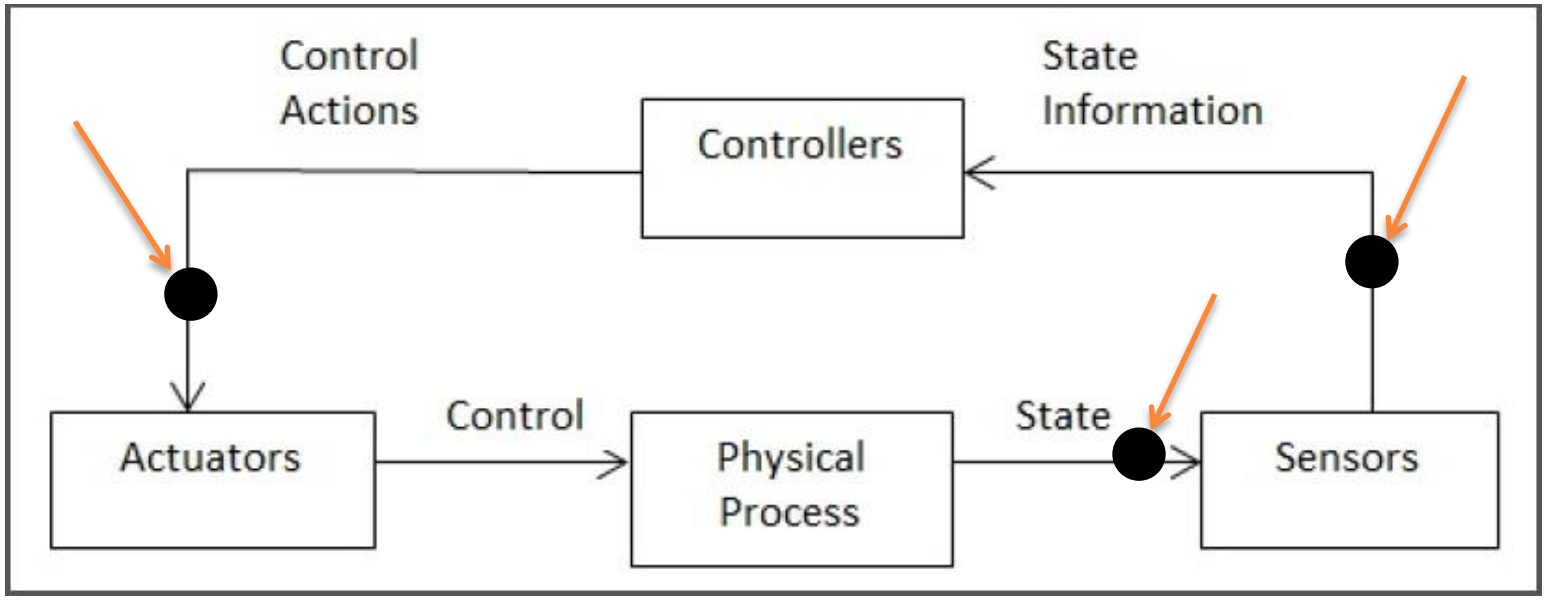
- Dynamic State Condition Graph (D-SCG) as a formal modeling device for sensor-actuator constraints in a CPS.

What is CPS?


Control
Actions
State
Information
Controllers
Actuators
Control
Physical
Process
State
Sensors

Cyber-attacks against CPS

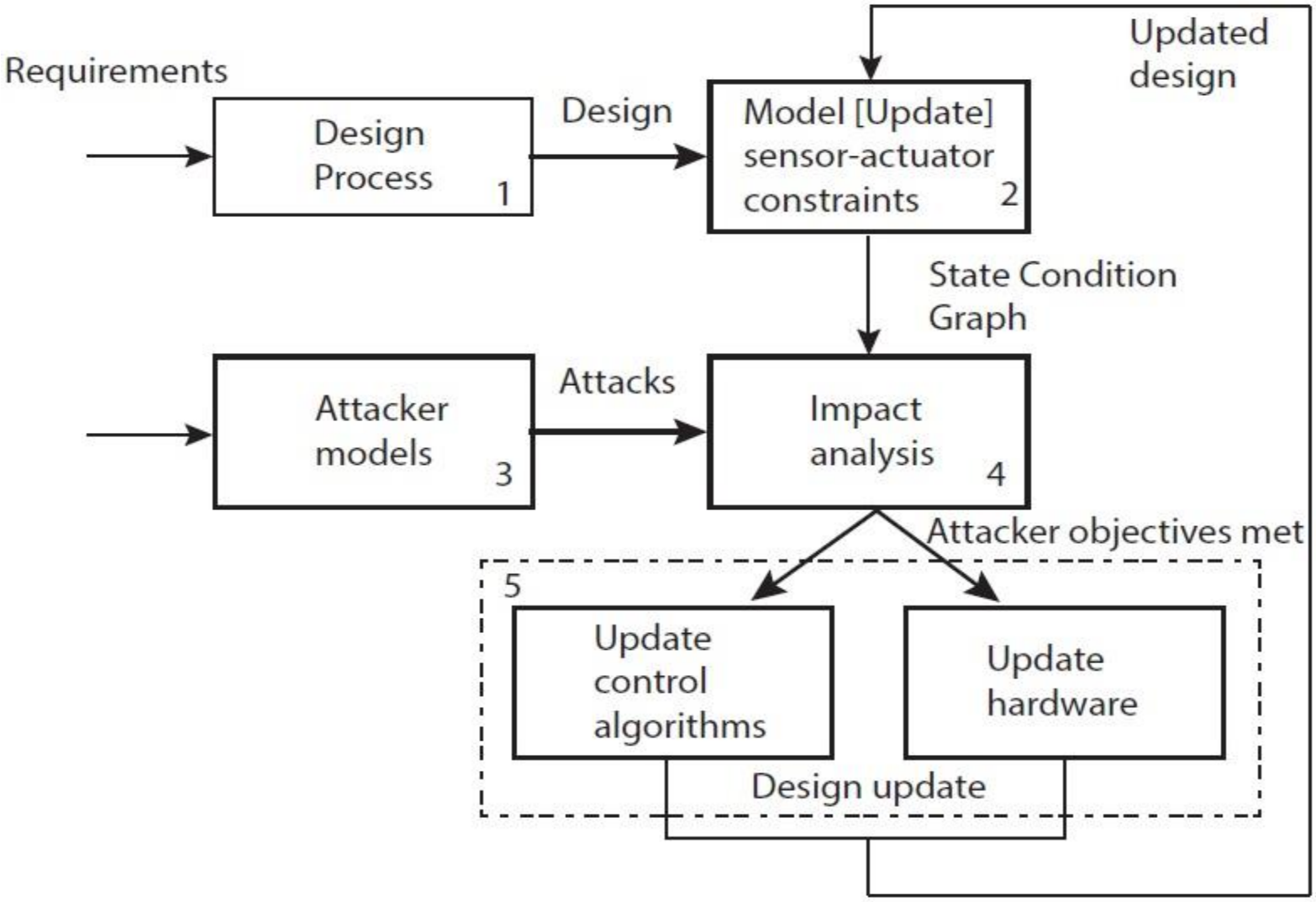
- "Cyber attack" refers to an attempt at disturbing the state of an Industrial Control Systems (ICS) through its communication network.



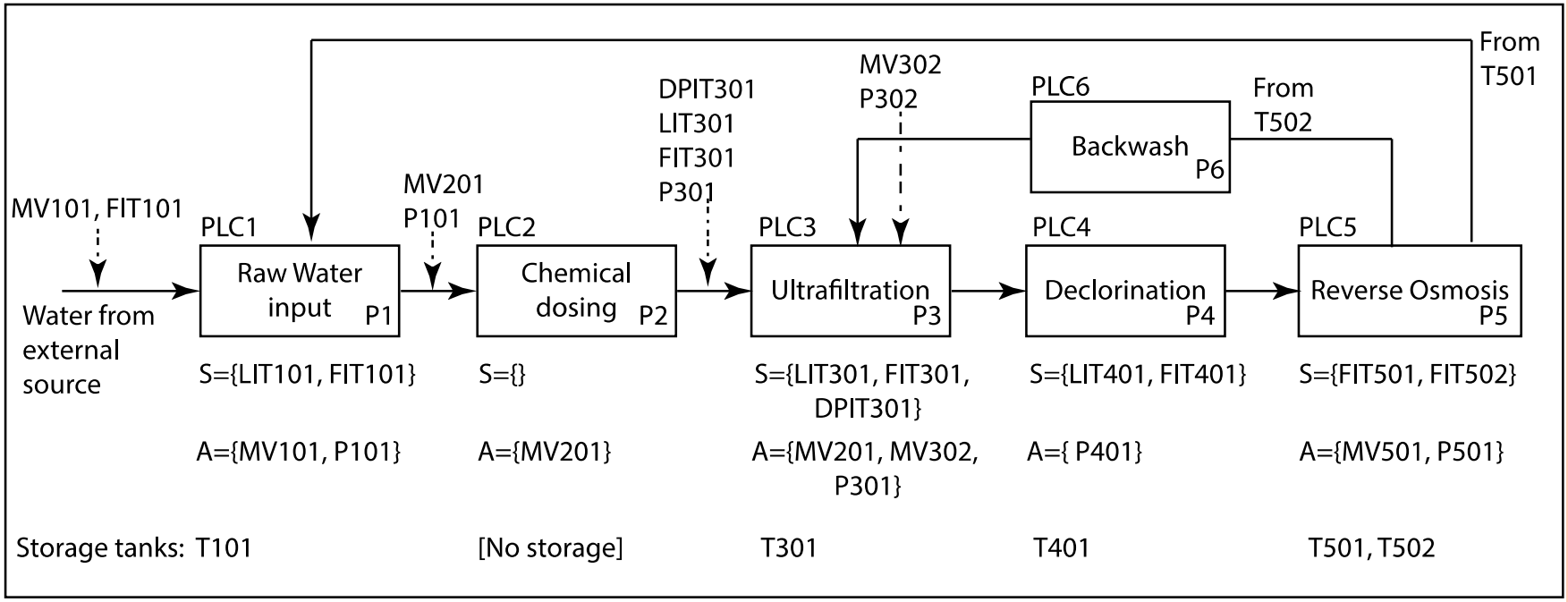
Popular breaches

- Maroochy shire sewage system 2000.
- Stuxnet Attack in 2010.
- Ukraine power plant black out 2016.
- Ukraine railway system black out 2016.

Security by design



SWaT Testbed: Simplified View



Level 0

PLC ⟷ Sensors/actuators

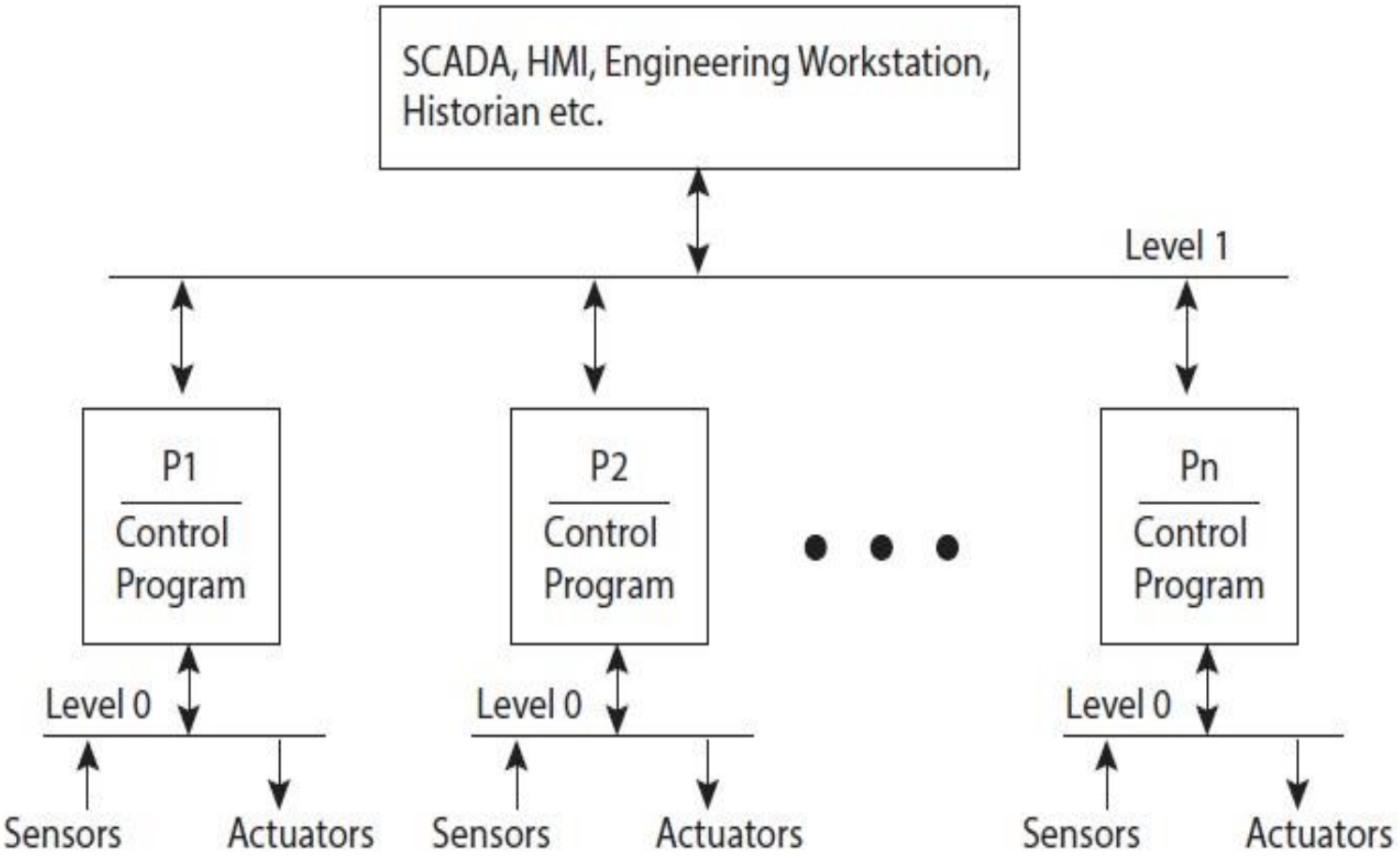
Level 1

PLC ⟷ PLC

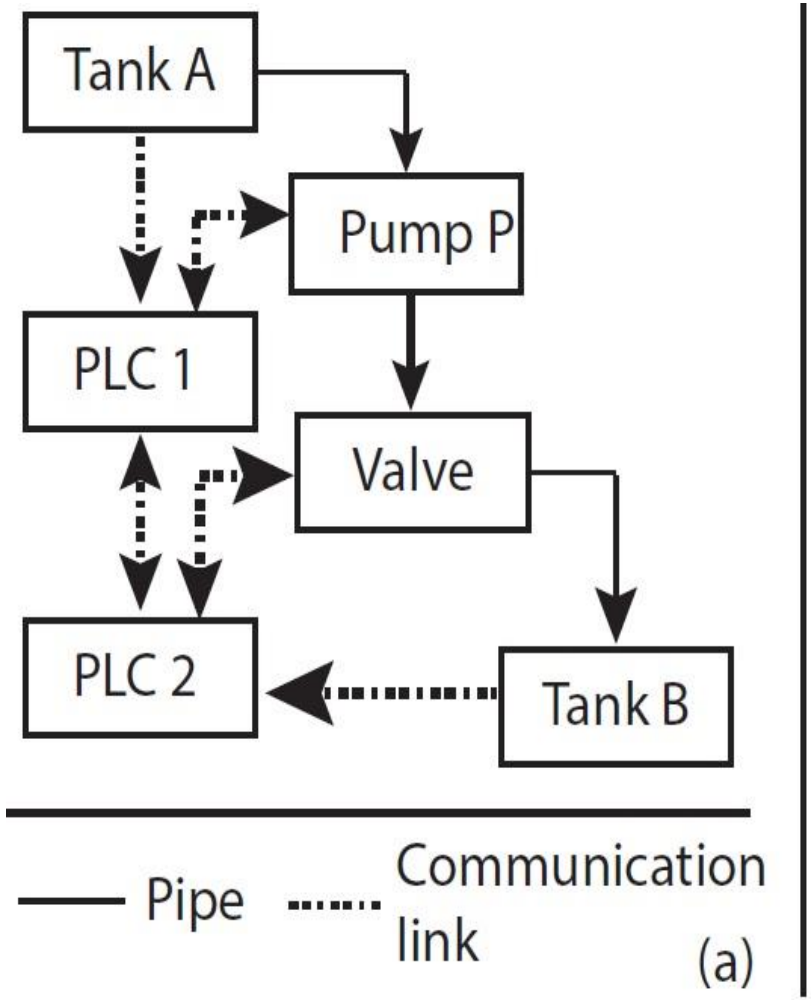
Level 2

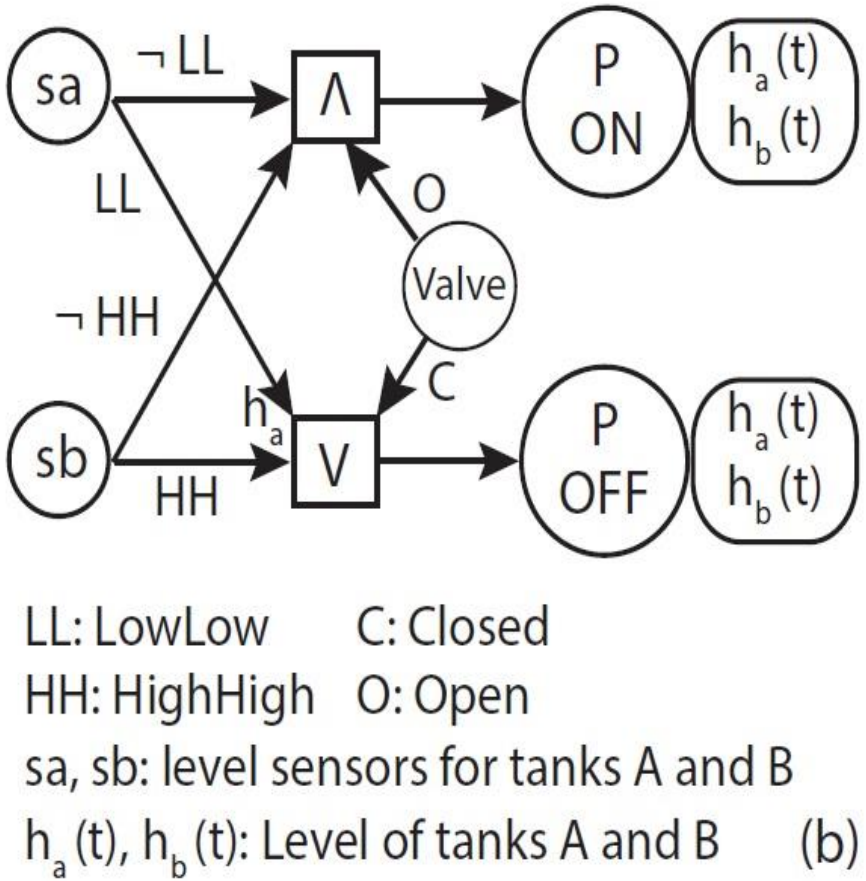
PLC ⟷ SCADA Workstation/HMI

Architecture of SWaT: Communication



Dynamic State Condition Graphs





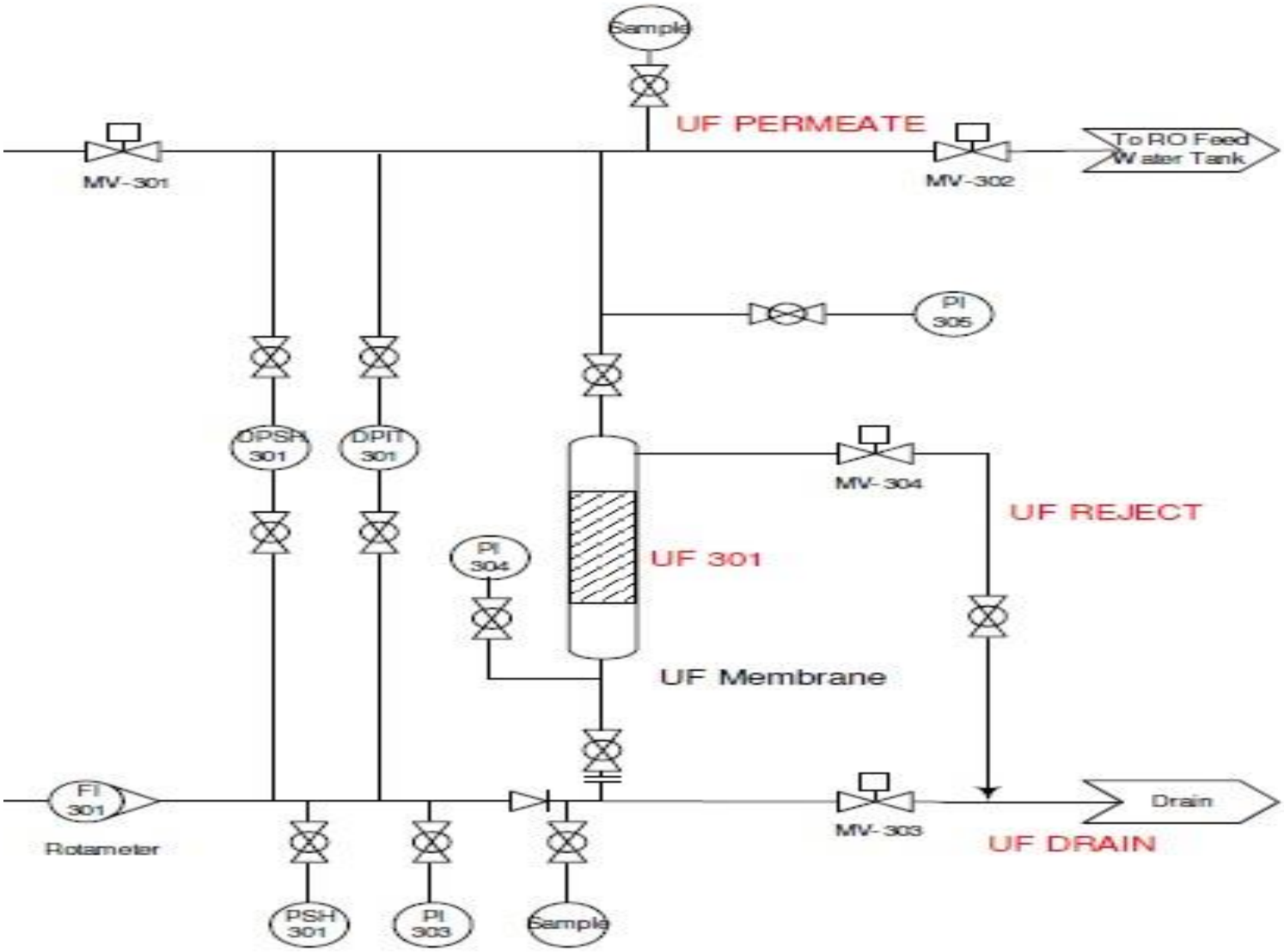
Attacker Model

- Attacker model is a pair (T;O),
  where T is an attack type to realise objective O.

- Example, “Damage generator A in a power grid,” or “Damage pump P302 in a water treatment network.”

- A cyber attack is a sequence of actions, a procedure, initiated by the attacker where each action is initiated via a cyber component, such as a wireless link or a SCADA computer.

Ultra Filtration process



Impact analysis: Damage the ultrafiltration

Attack	Actions	Consequence
1	Spoof messages going to PLC 3 by compromising the wireless link from the sensors	Attacker can send false data to PLC 3.
2	Set the high pressure sensor PSH-301 to 2.0 Bar	System state: PSH301>2.5 Bar In PLC: PSH301<2.5 Bar Hence, in the absence of the attack, P301 should be turned OFF, but as the PLC has the incorrect state information, it does not turn P301 OFF.
3	Set the differential pressure switch DPSH-301 to 0.3 Bar	System state: DPSH301> 0.5 Bar In PLC: DPSH301< 0.5 Bar Hence, in the absence of the attack, P301 should be turned OFF, but as the PLC has the incorrect state information, it does not turn P301 OFF.
4	Set the differential pressure indicator DPIT-301 to 0.3 Bar	System state: DPIT301>0.4 Bar In PLC: DPIT301<0.4 Bar
Impact on SWaT: UF does not enter immediate backwash cycle; UF deterioration accelerated; UF is likely to be damaged if the attack persists for sufficient time.The time to damage the UF will depend on the incoming water quality and the properties of the membranes in the UF unit.		

SUMMARY OF IMPACT ANALYSIS ON SWAT

Attack type	DSCG used	Outcome	Damage
Bias	p2_off	Dosing does not get activated to change the water properties	Water produced does not maintain desired chemical properties
Covert	p4_on	Water dechlorination does not take place for 10 minutes	Increased chances of damage to the RO unit
Replay	p5_on	Impure water gets into the RO unit permeate tank	No hardware damage
Surge	p3_off	Ultrafiltration unit damage accelerated due to delay in backwash	Increased chances of UF damage

Design update

- Based on the impact analysis, a detailed design of the defense mechanisms ought to be considered.
- Installation of additional water quality sensors will require the PLC code to be updated, and update the corresponding DSCG for further impact analysis.
- Independent network of sensors is one of the possible detection method.

Conclusions and future work

- The case study presented in this paper offers a glimpse into how the notion of "Security by Design" can be realised in practice.

- The analysis procedure needs some automation for it to be applicable in the design of realistic systems.

- However, doing so requires a clear understanding of component semantics such as when does a component fail.
- DSCGs could become an even more powerful tool once they are enhanced with physical operational constraints of each device included in the model.

Thank You