



**Industrial
Cybersecurity 2018:**
Opportunities and challenges
in Digital Transformation

Industrial Cybersecurity: Opportunities and challenges in Digital Transformation

KASPERSKY



Industrial Cybersecurity

Opportunities and challenges
in Digital Transformation



RICCARDO TAORMINA
SUTD
Singapore

- Postdoc at the iTrust, SUTD
- Contributed in epanetCPA, a cyber-physical attack simulator on water distribution networks
- Organized the BATADAL, an international data-science competition for attack detection algorithms

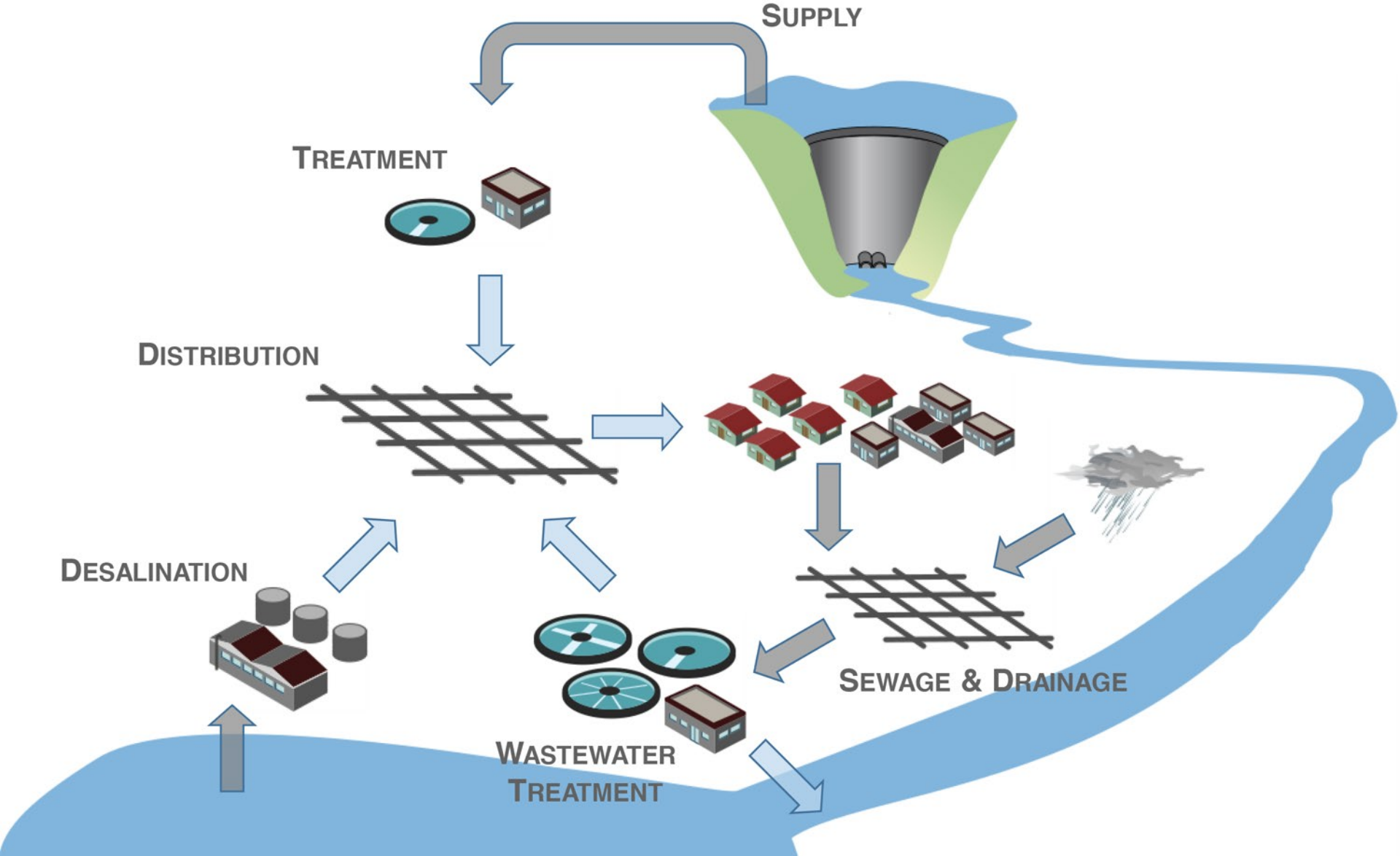
[linkedin.com/in/rictao](https://www.linkedin.com/in/rictao)

Contents

- Part I: Urban Water Infrastructures
- Part II: Cyber-Physical Security of Water Distribution Systems
- Part III: Testbeds @ iTrust
- Part IV: Conclusions

Part I: Urban Water Infrastructures

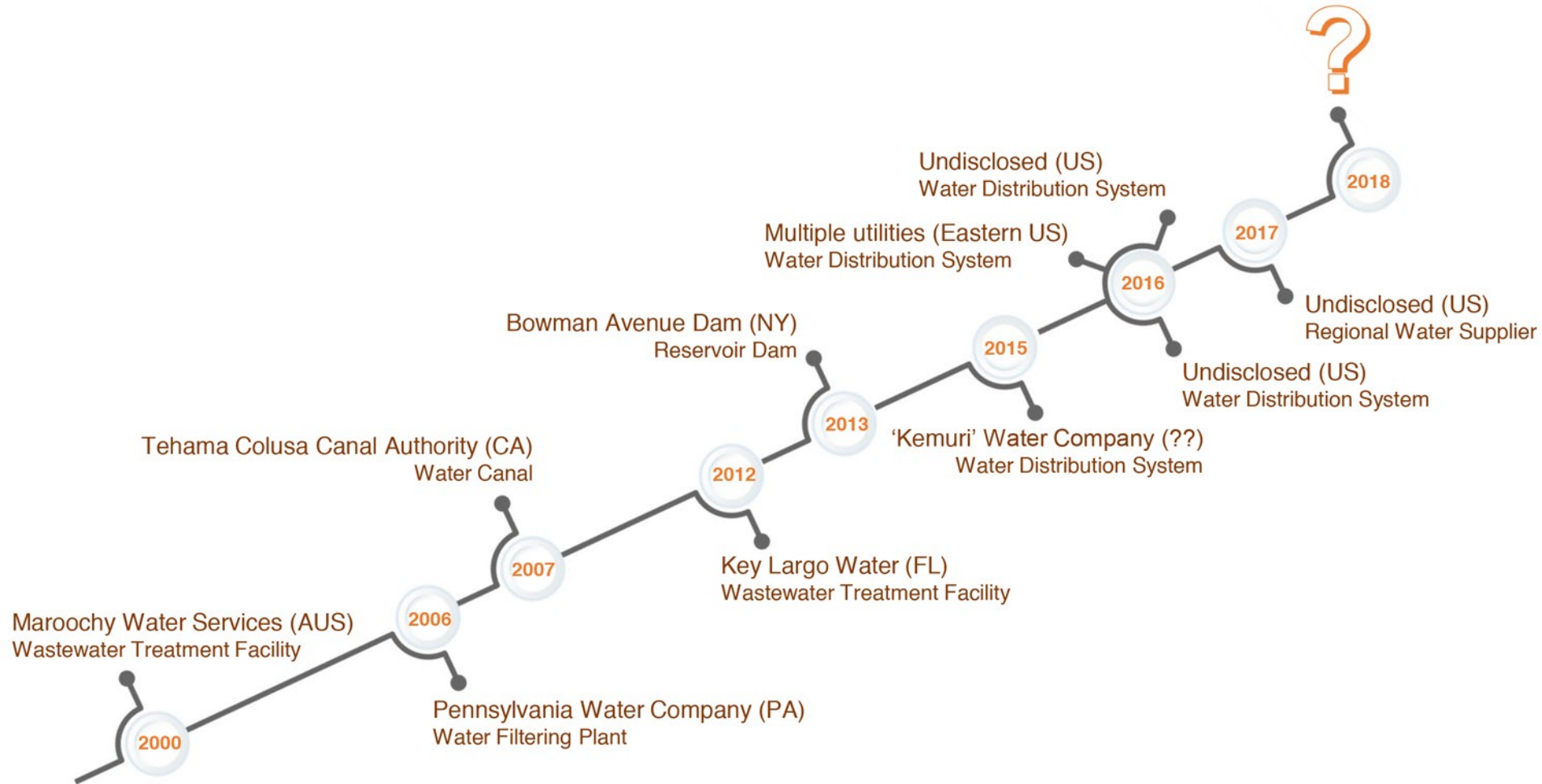
Urban Water Infrastructures



Urban Water Infrastructures

- Modern water infrastructures are cyber-physical systems.
- Cyber-layer depends on the type of underlying processes.
- Digital, interconnected ICS/SCADA replacing analog systems, air-gapped from corporate networks and internet.
- Higher efficiency, better service, cost-savings, real-time capabilities, ...
- Vast attack surface: 3rd most targeted sector after manufacturing and energy[#].

Review of attacks on Water Utilities



Review of attacks on Water Utilities

- At least 10 reported and confirmed attacks since 2000
- Targeted and untargeted attacks on very different infrastructures.
- Adversaries: outsiders, hacktivists, insiders, or third-party's insiders.
- Other suspicious incidents reported:
 - 2005, Taum Sauk Dam, St. Louis, MO
 - 2011, Pump Station, IL
 - 2011, Water Treatment Plant, Houston, TX
- Many unreported attacks: over 90% of attacks reported in the US, lack of data elsewhere.

Review of attacks on Water Utilities

Goals

- Cause damage
- Seize resources for other purposes
- Terrorism
- Ransom
- Revenge
- Steal money
- Data breach
- Practice
- Others, unknown

Means

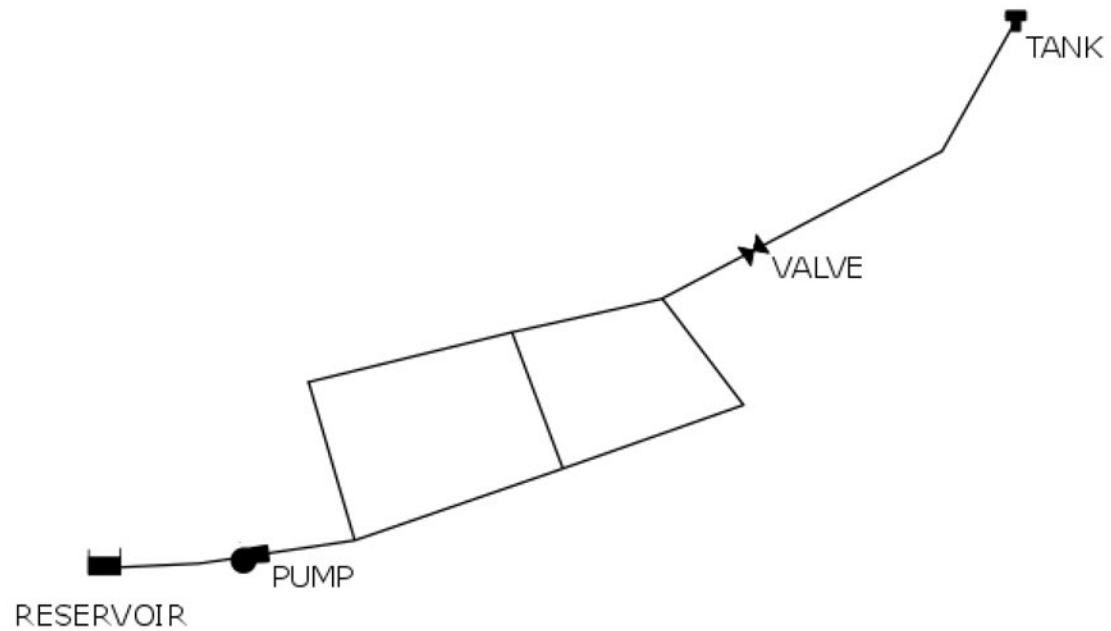
- Unauthorized access
- Exploitation of software vulnerabilities
- Malware, Viruses, Trojans, Worms, ...
- Ransomware
- Social engineering
- Insider information

Vulnerabilities

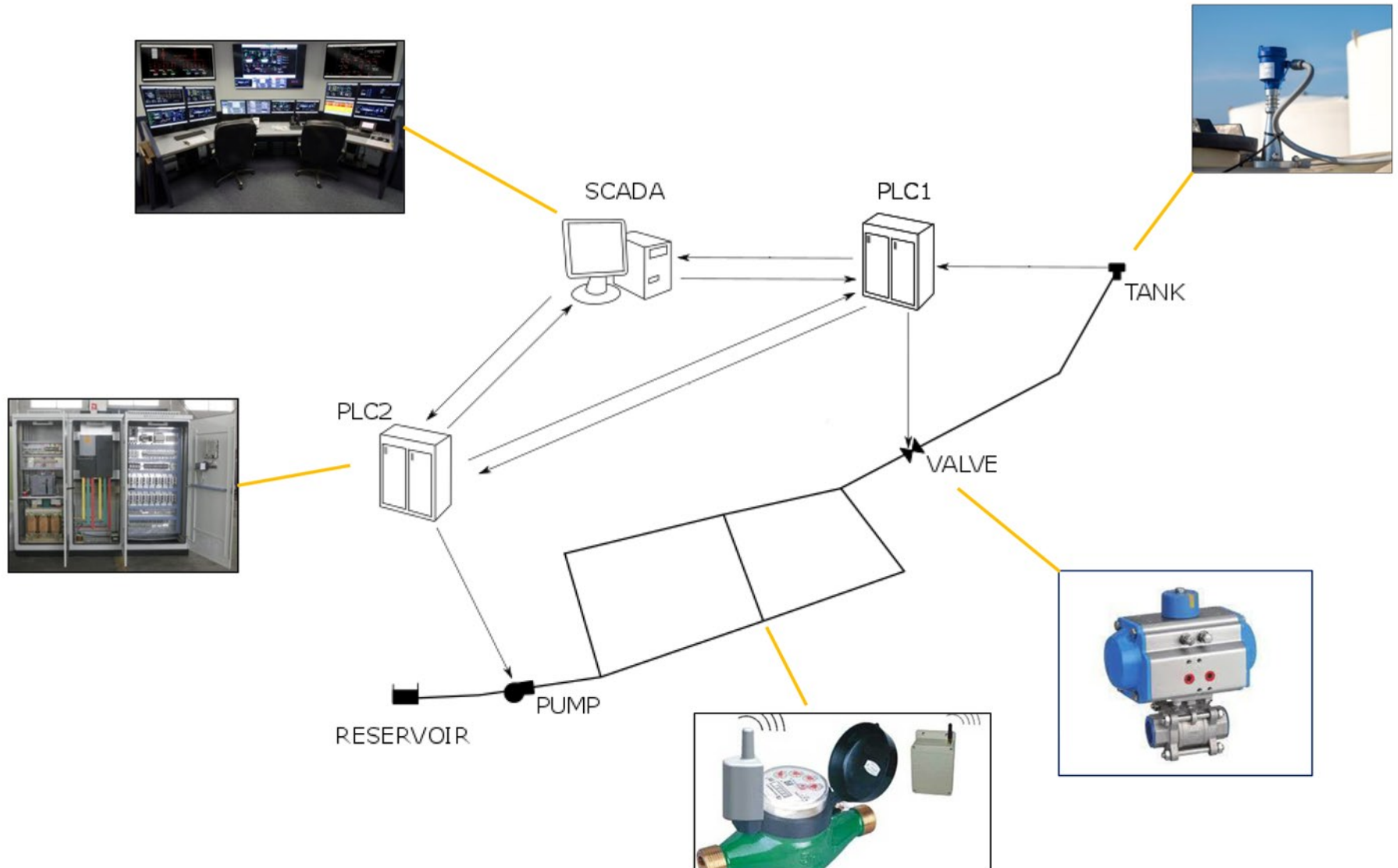
- Poor separation of ICS/SCADA and corporate networks
- Lack of awareness
- Lack of IT/OT security teams
- Outdated software, hardware, firmware
- Poor attention to security guidelines

Part II: CPS of Water Distribution Systems

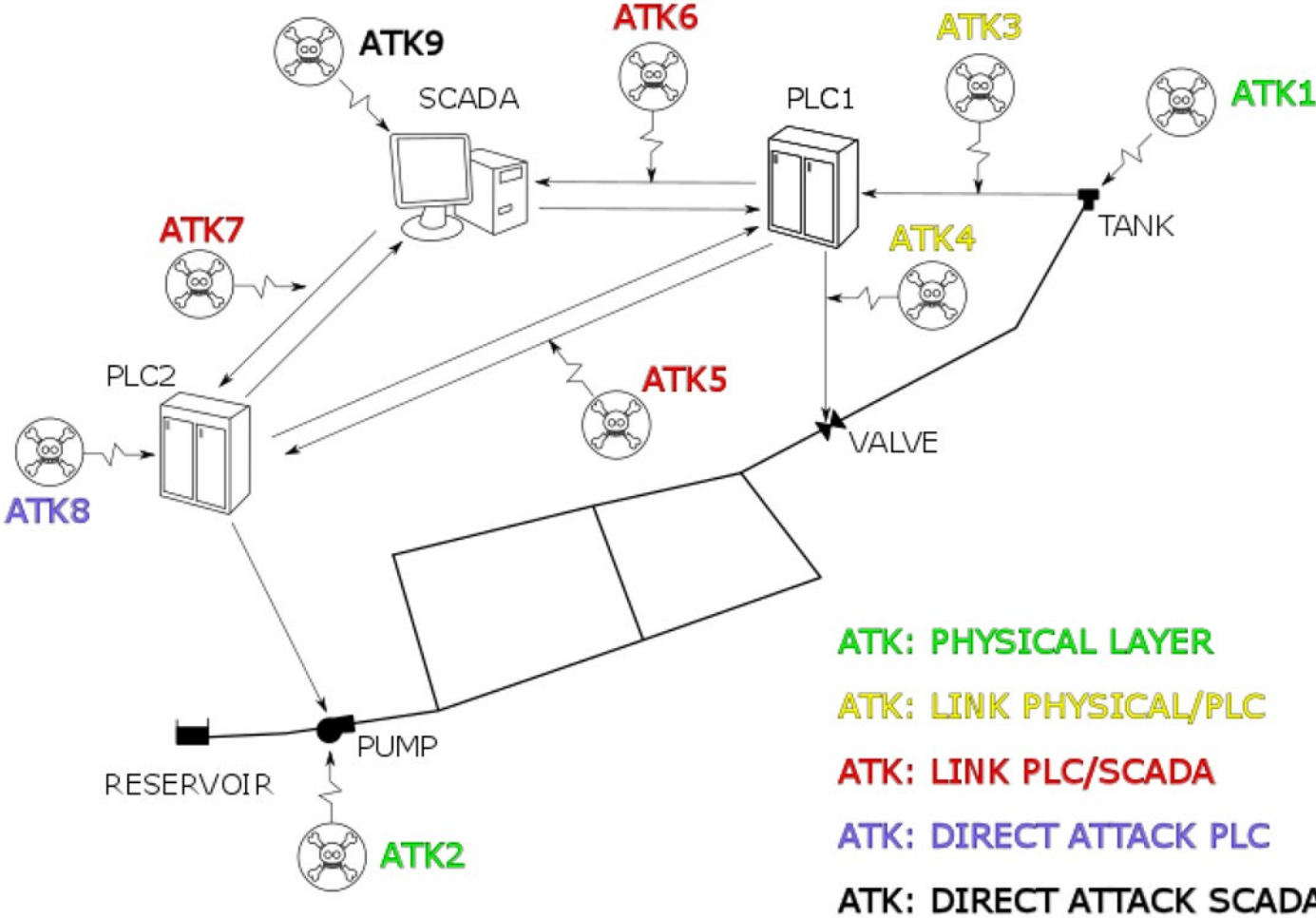
Water Distribution Systems (WDS)



WDS are cyber-physical systems

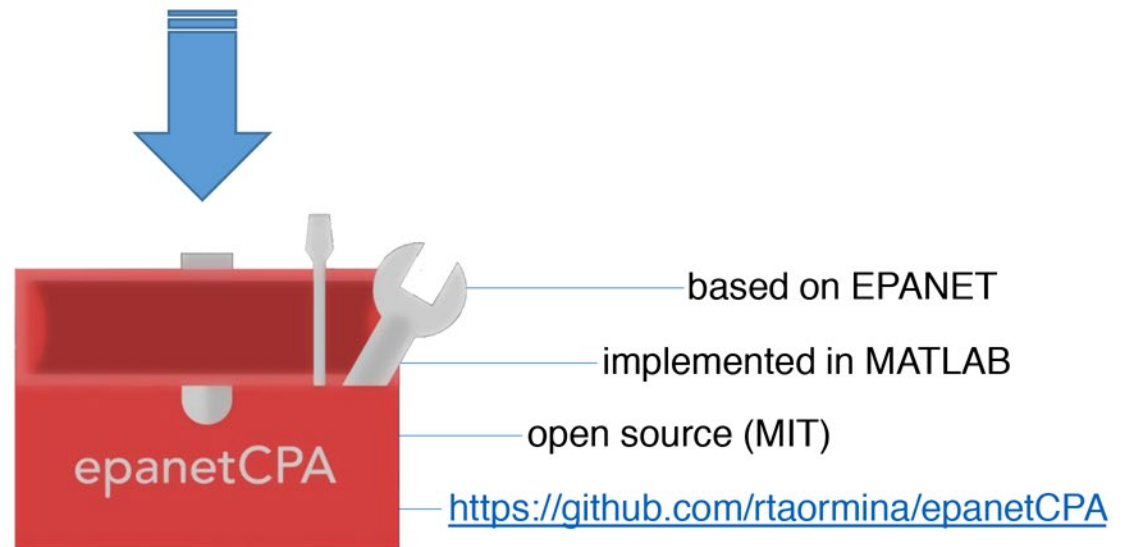


Attacker model for WDS



Estimating the impacts of attacks on WDS

- Utilities are not keen to share data on attacks.
- It is hard to estimate the risk associated to attacks on WDS.
- Computer simulations can help estimate the impacts.



epanetCPA: results

- Used to study attacks causing:
 - tank overflows,
 - low pressure conditions,
 - unmet demands,
 - total cutoffs of supply.
- Entity of impact depends on initial conditions.
- The tool can be used to assess district vulnerability.
- Existence of “windows of opportunity” for attack response.
- Usefulness of synthetic data generation.

Douglas, H.C., Taormina, R. and Galelli, S., 2018. Pressure-Driven Modeling of Cyber-Physical Attacks on Water Distribution Systems. *Journal of Water Resources Planning and Management* (in press).

Taormina, R., Galelli, S., Tippenhauer, N.O., Salomons, E. and Ostfeld, A., 2017. Characterizing Cyber-Physical Attacks on Water Distribution Systems. *Journal of Water Resources Planning and Management*. 143 (5), 04017009

(BATADAL) BATTLE OF THE ATTACK DETECTION ALGORITHMS

ABOUT BATADAL

© 9 September 2016

The BATtle of the Attack Detection ALgorithms (BATADAL) will objectively compare the performance of algorithms for the detection of cyber attacks in water distribution systems. Participants will contribute an attack detection algorithm for a given water network following a set of rules that determine the exact goal of the algorithms.

MOTIVATION

Modern Water Distribution Systems rely on computers, sensors and actuators for both monitoring and operational purposes. This combination of physical processes and embedded systems (cyber-physical systems, in short) improves the level of service of water distribution networks but exposes them to the potential threats of cyber attacks. During the past decade, several water supply and distribution systems have been attacked, with the consequent creation of cyber-security agencies and international partnerships to defend water networks. Yet, little is known about the potential effect of these attacks as well as the design and implementation of attack detection algorithms which identify anomalous behaviors of sensors, pumps and other components of water networks.

[MORE DETAILS ON DESIGN CHALLENGE](#)



**ENVIRONMENTAL &
WATER RESOURCES
INSTITUTE**

NEWS

RESULTS ANNOUNCED

© 26 May 2017

Results of the BATADAL are now available [here](#).

BATTLE FINISHED

© 1 March 2017

We released the solutions for the

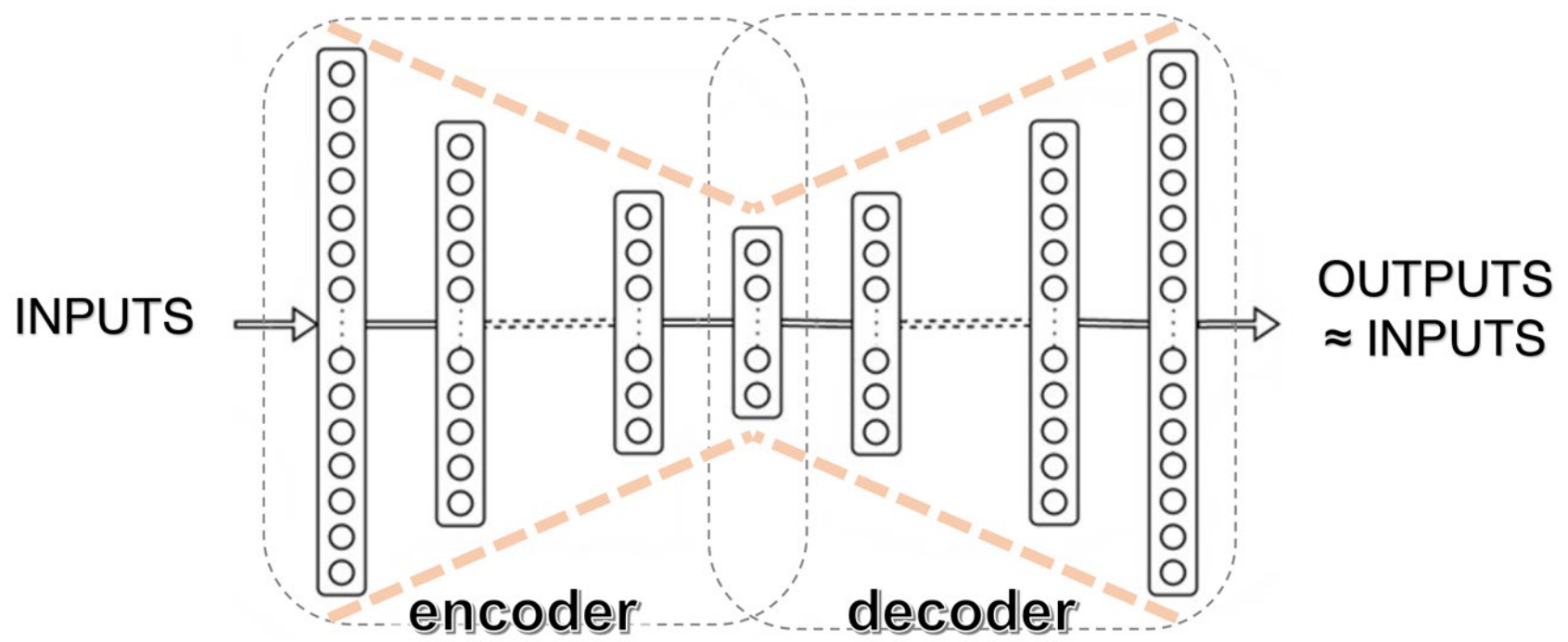
BATADAL: results

PLACE	TEAM	ATTACKS DETECTED	SCORE	ALGORITHM DETAILS
1	Housh and Ohar	7 out of 7	0.970	Process-based approach
2	Abokifa et al.	7 out of 7	0.949	PCA + ANNs
3	Giacomoni et al.	7 out of 7	0.927	PCA + Classifier
4	Brentan et al.	6 out of 7	0.894	Recurrent neural networks
5	Chandy et al.	7 out of 7	0.802	Variational Autoencoders
6	Pasha et al.	7 out of 7	0.773	Multiple approaches
7	Aghashahi et al.	3 out of 7	0.534	Feature extraction + classifier

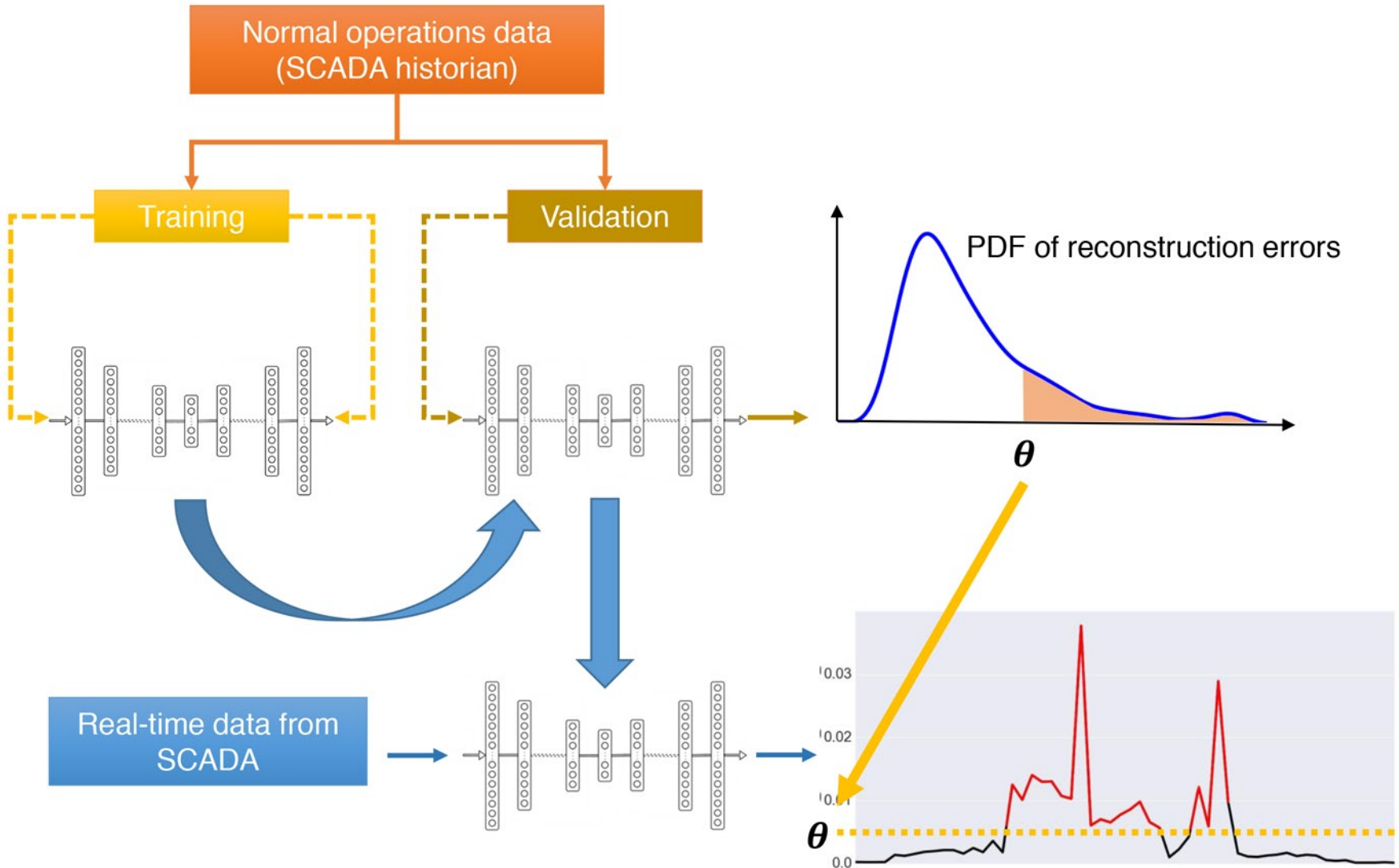
Taormina, R., Galelli, S., Tippenhauer, N.O., Salomons, E., Ostfeld, A., and Ohar, Z., 2018. Battle of the Attack Detection Algorithms: Disclosing Cyber Attacks on Water Distribution Networks. *Journal of Water Resources Planning and Management*, 144 (8), 04018048.

Attack detection with Autoencoders (AE)

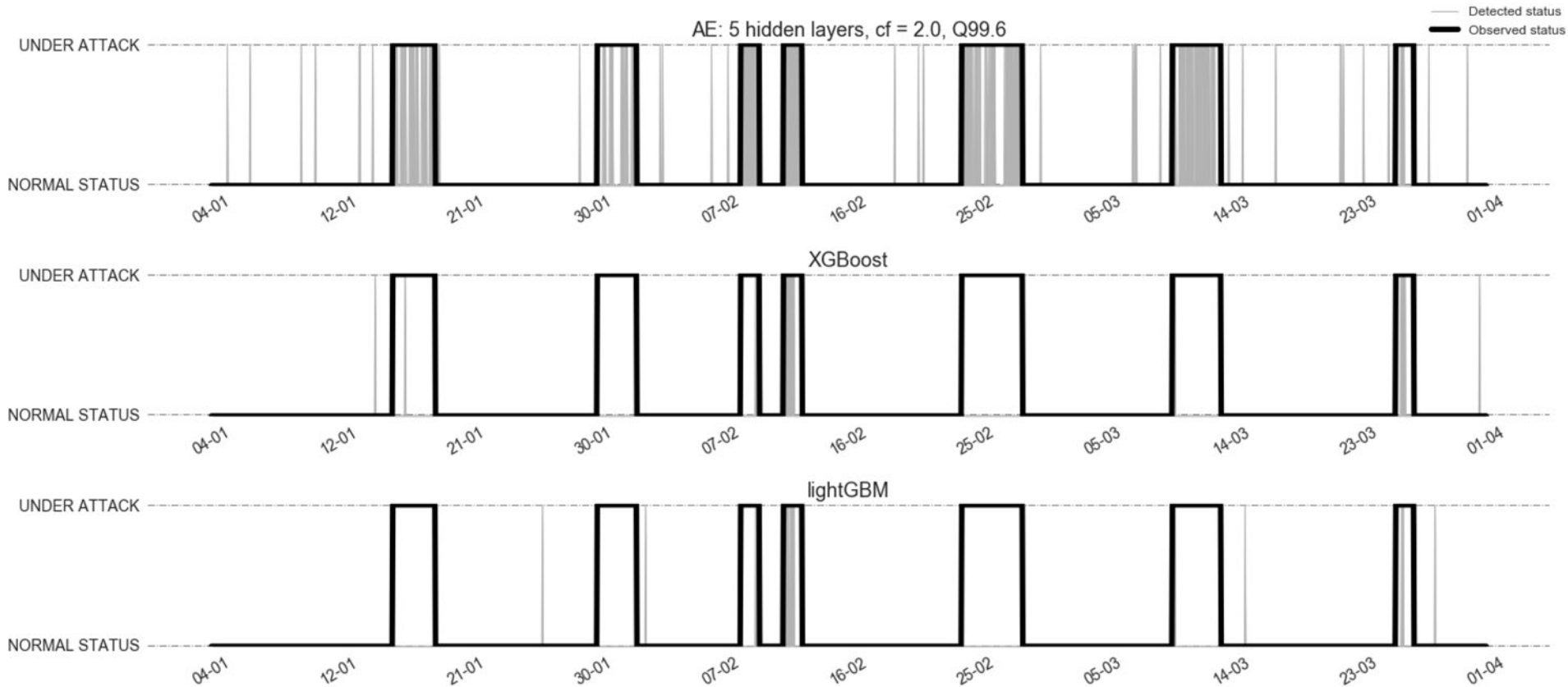
- Symmetric hourglass-shaped architecture made of an **encoder** and a **decoder**.
- The network is trained with the aim of **replicating the inputs**.
- AE learn a compressed representation of the input data.
- $OUTPUTS = INPUTS \rightarrow$ AE are *self-supervised learning models* (no labels).
- **Reconstruction error** \sim difference between input and its reconstruction.



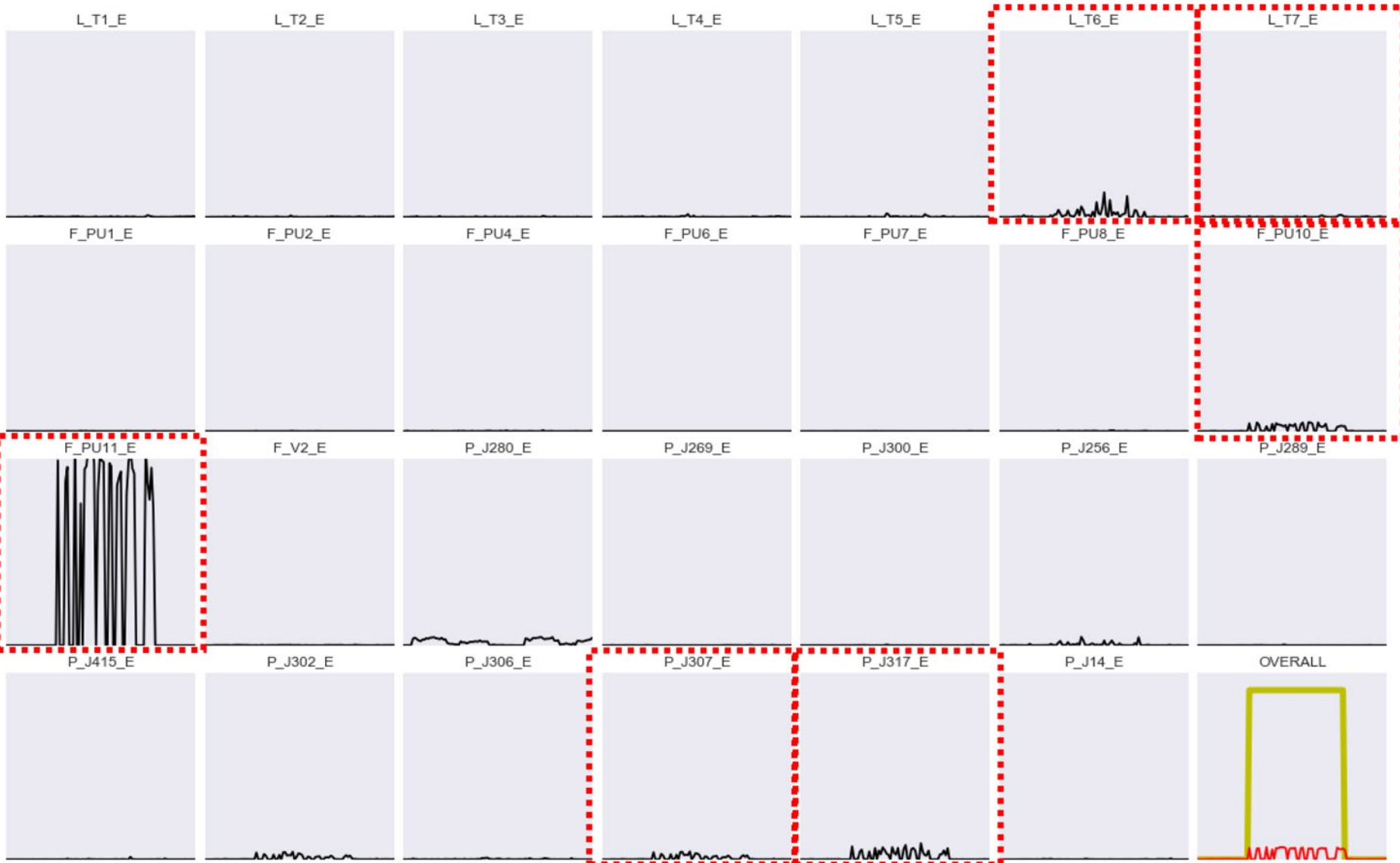
Attack detection with Autoencoders (AE)



Results on BATADAL dataset

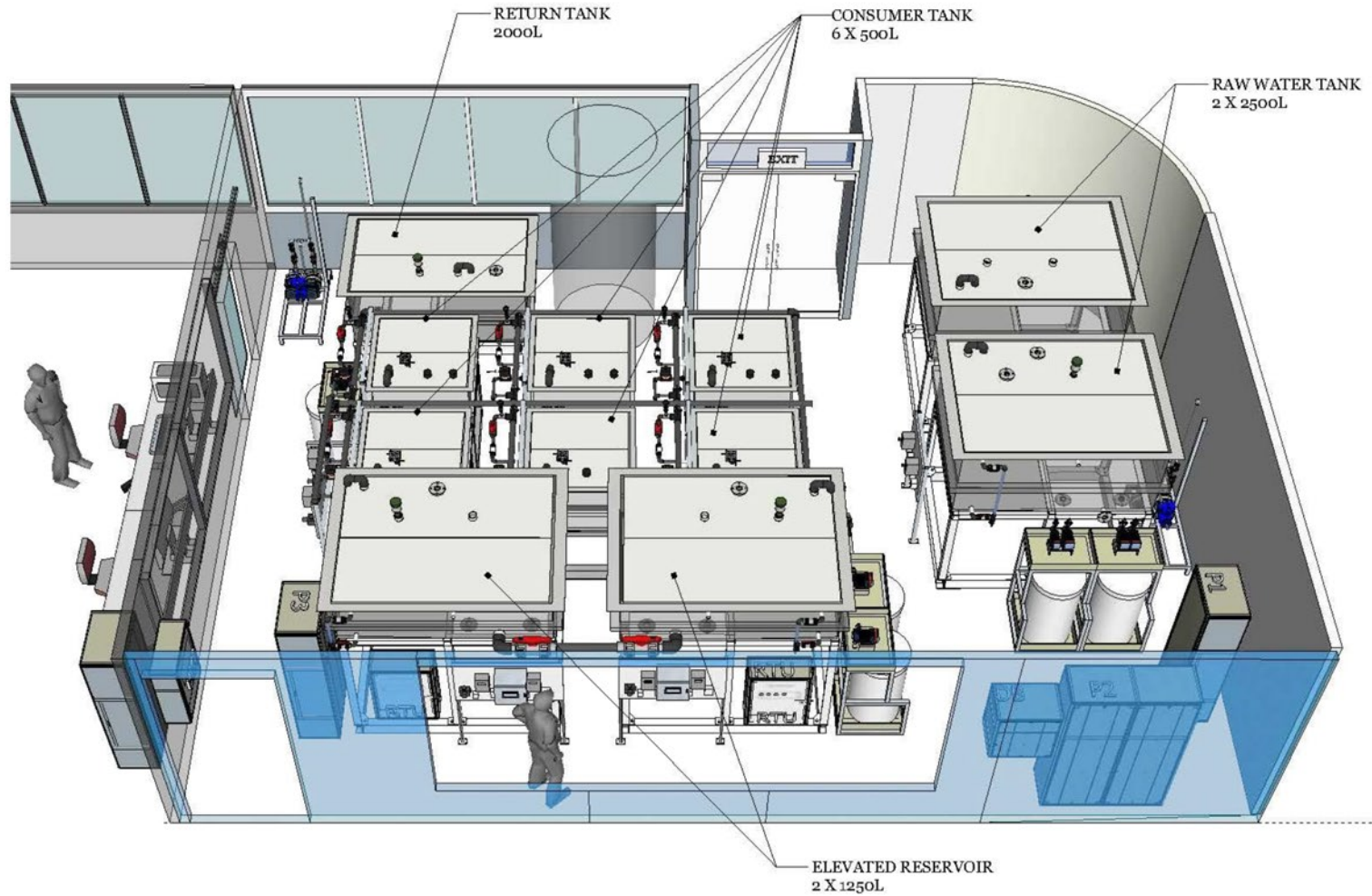


Attack localization



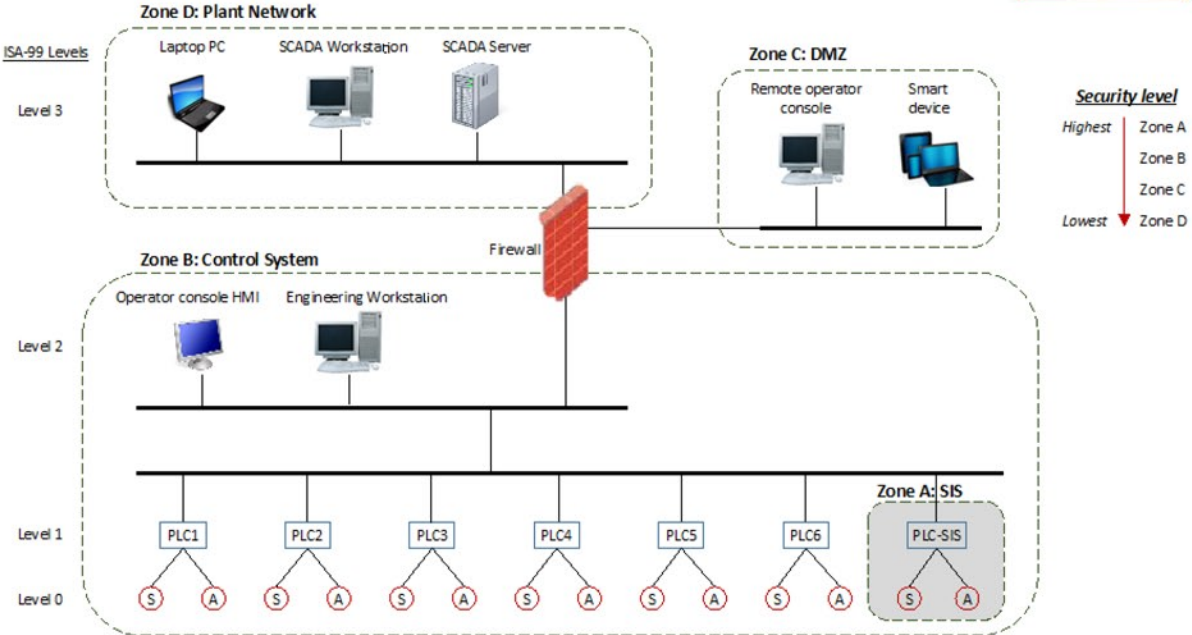
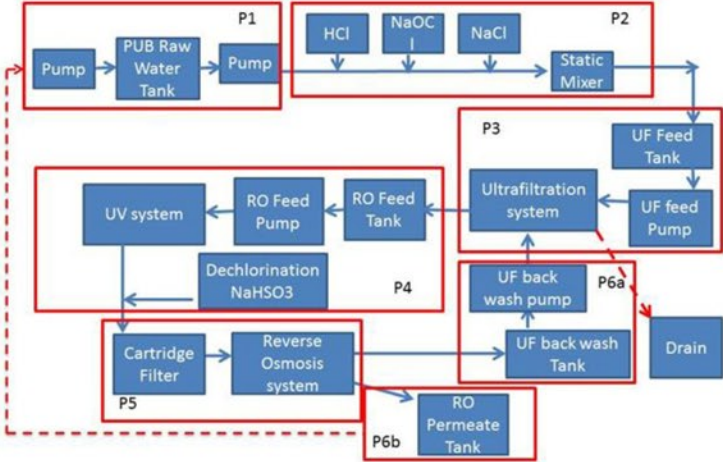
Part III: Testbeds

Water Distribution (WADI) Testbed




- SCADA
- 3 PLCs
- HMI
- 5 Storage Tanks
- 6 Demand Nodes
- Pumps, Valves
- Chemical dosing systems
- Analysers
- Leak Simulator, ...

Secure Water Treatment (SWaT) Testbed



Testbeds at iTrust

Four testbeds at iTrust, SUTD

- WADI, water distribution
 - SWaT, water treatment
 - EPIC, power grid
 - IoT, internet of things
- 
- Interconnected**

- [Datasets](#) with and without attacks available for download.
- Used to carry out workshops and [hacking competitions](#) (attack and defense) for academia and industry.
- Testbeds soon available for paid usage by external parties.

Part IV: Conclusions

Conclusions

- Modern water infrastructures are cyber-physical systems.
- Cyber-layer offers many benefits but lends an attack surface.
- Water sector is the third most targeted critical infrastructure.
- Major vulnerabilities include poor separation of ICS/SCADA from corporate network, lack of awareness and training.
- Guidelines are available but implementation is voluntary.
- We need to better report, study and characterize these attacks.

Conclusions

- Water Distribution Systems are heavily targeted infrastructures.
- Ongoing research to characterize and detect attacks on WDS.
- Simulations can be used to compensate for lack of real data.
- Testbed experiments can provide further insights, generate datasets, and improve the realism of simulations.
- Major advancements will require collaboration with utilities.

Thanks!

Riccardo Taormina

riccardo_taormina@sutd.edu.sg

iTrust@SUTD

<https://itrust.sutd.edu.sg/>

Related publications

Douglas, H.C., Taormina, R. and Galelli, S., 2018. Pressure-Driven Modeling of Cyber-Physical Attacks on Water Distribution Systems. *Journal of Water Resources Planning and Management (in press)*.

Taormina, R. and Galelli, S., 2018. Real-Time Detection of Cyber-Physical Attacks on Water Distribution Systems Using Deep Learning. *Journal of Water Resources Planning and Management*, 144 (10), 04018065.

Taormina, R., Galelli, S., Douglas, H.C., Tippenhauer, N.O., Salomons, E. and Ostfeld, A., 2018. Modeling Cyber-Physical Attacks on Water Networks with epanetCPA. In *WDSA/CCWI Joint Conference Proceedings*, 1.

Taormina, R., Galelli, S., Tippenhauer, N.O., Salomons, E., Ostfeld, A., and Ohar, Z., 2018. Battle of the Attack Detection Algorithms: Disclosing Cyber Attacks on Water Distribution Networks. *Journal of Water Resources Planning and Management*, 144 (8), 04018048.

Taormina, R., Galelli, S., Tippenhauer, N.O., Salomons, E. and Ostfeld, A., 2017. Characterizing Cyber-Physical Attacks on Water Distribution Systems. *Journal of Water Resources Planning and Management*. 143 (5), 04017009

Taormina, R. and Galelli, S., 2017, May. Real-Time Detection of Cyber-Physical Attacks on Water Distribution Systems Using Deep Learning. In *Proceedings of World Congress on Environmental & Water Resources* (pp. 469-479).

Taormina, R., Galelli, S., Tippenhauer, N.O., Salomons, E. and Ostfeld, A., 2016, May. Assessing the Effect of Cyber-Physical Attacks on Water Distribution Systems. In *Proceedings of World Congress on Environmental & Water Resources* (pp. 436-442).

Taormina, R., Galelli, S., Tippenhauer, N.O., Ostfeld, A. and Salomons, E., 2016, January. Simulation of cyber-physical attacks on water distribution systems with EPANET. In *Proceedings of the Singapore Cyber-Security Conference (SG-CRC) 2016: Cyber-Security by Design* (Vol. 14, p. 123). IOS Press.