Research Ideas from [1], [2]

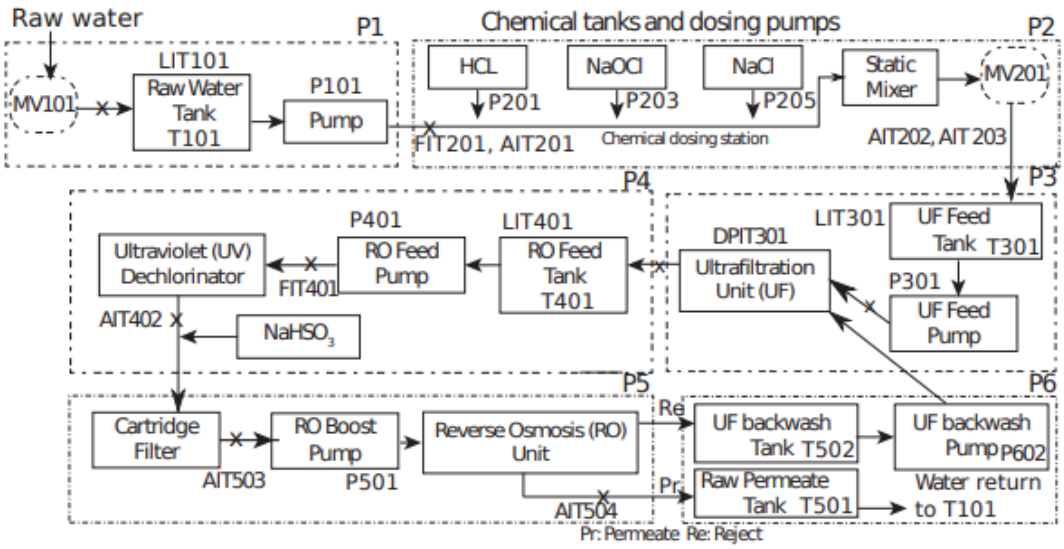
Create a more comprehensive (than the simplified version in [2]) totally virtualized, containerized water treatment testbed to do experiments with different industrial communication protocols and collect data for many more vulnerabilities that what is described (namely DoS, MITM) in these two papers. Maybe use these data to train ML models for anomaly detection.

Why the problem is important: It is important for the same reason that has been described in these papers - to minimize time/cost/effort by virtualization and containerizing.

What is missing currently: The water treatment testbed is not comprehensive [2]. Each paper describes scenarios for only one communication protocol. Wind turbine experiment [1] collects data for only one kind of malfunction of turbine (increase of speed above normal level) after cyber attack. Water treatment testbed uses only DoS and MITM attack for honeypot scenario.

What I am proposing:

1. Implement more comprehensive version of the water treatment testbed described in paper [3].



2. Experiment with different communication protocols.
3. Generate large scale attack data using approach described in [1] (use nmap, hping, kafka broker).
4. ML models probably can be trained for anomaly detection.
5. More attack scenarios than DoS, MITM
6. If we want to stretch Honeypot concept, maybe we can go into game theory.

7. Maybe we can simulate multiple testbeds and experiment with how networks of water treatment plants or water networks will work.

[1] Daniel L. Marino; Chathurika S. Wickramasinghe; Vivek Kumar Singh . *The Virtualized Cyber-Physical Testbed for Machine Learning Anomaly Detection: A Wind Powered Grid Case Study.*

[2] Marco Lucchese , Francesco Lupia , Massimo Merro , Federica Paci , Nicola Zannone. *HoneyICS: A High-interaction Physics-aware Honeynet for Industrial Control Systems.*

[3] Aditya P. Mathur, Nils Ole Tippenhauer. *SWaT: A Water Treatment Testbed for Research and Training on ICS Security.*