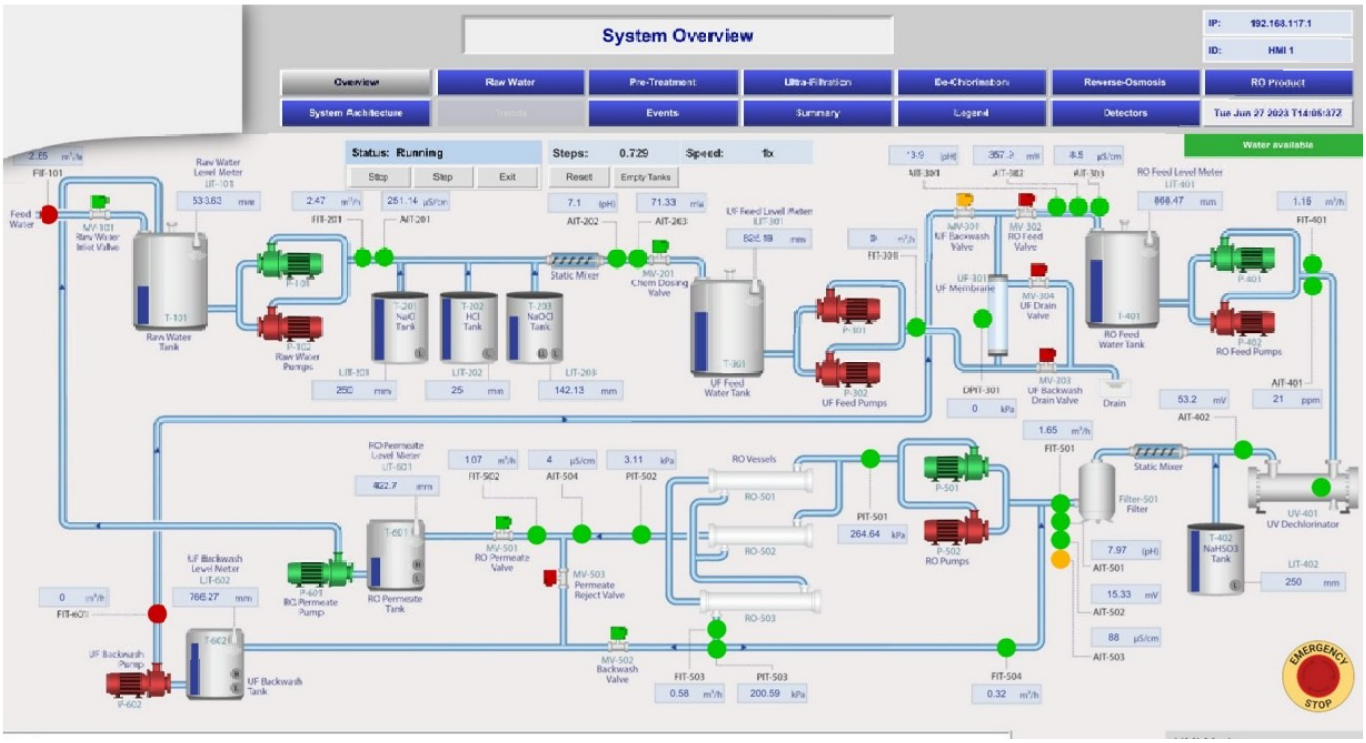
TECH OFFER

Cyber-Physical Attack Simulation on Critical Infrastructure for Educational Learning



KEY INFORMATION

TECHNOLOGY CATEGORY:
Infocomm - Educational Technology
Infocomm - Computer Simulation & Modeling

TECHNOLOGY READINESS LEVEL (TRL): TRL5
COUNTRY: SINGAPORE
ID NUMBER: TO175284

OVERVIEW

The rise of digitalization of infrastructures via digital twins and increased industrial automation, there is an increased need for better prepared for cyber and physical attacks. The digitalization trends also underscore the increased threat of cyber or physical ("cyber-physical") attacks that can now easily crimple critical infrastructures if unprepared.

The technology owner leverages on the use of a digital twin and mock-up infrastructure to develop a technology solution that is able to mimic and simulate the behaviors of a physical infrastructure under cyber-physical attack. The realistic simulation and have been developed with a focus on large-scale cyber exercises such as Locked Shields (a cyber defense exercise by NATO CCDCOE) in mind. The digital platform enables users to understand and evaluate potential weakness of existing infrastructure via simulated cyber-physical attacks on operational technology (OT) to improve operation resilience. The digital platform is not dependent on the mock-up infrastructure and can be customized for specific simulations.

The technology owner has successfully emulated a cyber twin of a Secure Water Treatment System (SWaT) with a physical

testbed system for a testbed to launch and study cyber-physical attacks in a realistic water treatment plant. The technology owner is seeking collaboration partners who wish to accelerate understanding and build resilience from potential cyber-physical attack via simulations of critical infrastructures.

TECHNOLOGY FEATURES & SPECIFICATIONS

The technology solution of Secure Water Treatment System (SWaT), comprising of the mock-up IT/OT infrastructure and digital twin, includes the following functionalities:

- Emulation of IT and OT network for a realistic 6-stage water treatment plant with the following stages:
    1. Raw water inlet
    2. Chemical dosing
    3. Ultrafiltration
    4. UV dichlorination
    5. Reverse Osmosis
    6. Backwash
- Customizable learning management platform for specific cyber-physical attack simulations
- Launch attacks for both OT and IT attacks with integrated IT/OT anomaly detector
- Conduct simulated and live-firing exercises using a configurable classroom orchestrator software within a physical, remote, or hybrid setting (with remote monitoring of participants)
- Ability to enhance learning using AR/VR emerging technology

POTENTIAL APPLICATIONS

This technology solution of simulating cyber-physical attacks can be used for enhancing cyber resilience in critical infrastructure such as:

- **Energy and Utilities:** Power plants, electrical grids, water treatment facilities, renewable energy systems.
- **Oil and Gas:** Drilling operations, refining processes, pipeline monitoring, distribution networks.
- **Transportation and Logistics:** Automated control systems for railways, ports, warehouses, and supply chain management.
- **Chemical Processing:** Reaction monitoring, safety systems, quality control in chemical production.
- **Manufacturing:** Production lines, assembly processes, quality control systems.

UNIQUE VALUE PROPOSITION

The technology solution provides the capability to accelerate understanding of cyber-physical attacks by supporting live-firing cyber simulations at the scale of Locked Shields (from NATO CCDCOE). The solution platform enables customisable digital twin of infrastructures with a configurable management software to facilitate multi-modal learning. Due to the integrated IT and OT anomaly detector, specific IT or OT attack launcher can be provide simulate realistic scenarios to improve operational resilience.