Secure Water Treatment

Background

Secure Water Treatment (SWaT) is a testbed for research in the area of cyber security. The testbed, funded by MINDEF, is utilised by two projects, namely, Cyber Physical System Protection and Advancing Security of Public Infrastructure using Resilience and Economics. Both projects targeted the protection of Cyber Physical Systems (CPS) such as those for water treatment, power generation and distribution, and oil and natural gas refinement. The testbed will serve as a key asset for researchers in Singapore and abroad who are aiming at the design of secure CPS.

SWaT Architecture

SWaT consists of a modern six-stage process. The process begins by taking in raw water, adding necessary chemicals to it, filtering it via an Ultrafiltration (UF) system, de-chlorinating it using UV lamps, and then feeding it to a Reverse Osmosis (RO) system. A backwash process cleans the membranes in UF using the water produced by RO. The cyber portion of SWaT consists of a layered communications network, Programmable Logic Controllers (PLCs), Human Machine Interfaces (HMIs), Supervisory Control and Data Acquisition (SCADA) workstation, and a Historian. Data from sensors is available to the SCADA system and recorded by the Historian for subsequent analysis.

Click here for a virtual tour of SWaT

Research
‹ Projects
Publications
Reports
‹ **Testbeds**
Electric Power and Intelligent Control
Internet of Things Automatic Security Testbed
Secure Water Treatment
Water Distribution

Research

In the first phase of this research, models of SWaT will be created using advanced tools such as LabView and Simulink. Models so created will be used to conduct initial experiments aimed at understanding the response of SWaT to a variety of cyber attacks. Attacks by insiders and outsiders will be considered. This first round of experiments will lead to an understanding of the strengths and weaknesses of the existing defense mechanism in SWaT.

In the second stage, a small set of cyber attacks will be tried in the testbed using carefully designed experiments that ensure no damage to the physical system. Such experiments are aimed at verifying whether that what is learnt in simulation applies to the physical testbed. These experiments will lead to an understanding of the weaknesses of the defense mechanism of SWaT.

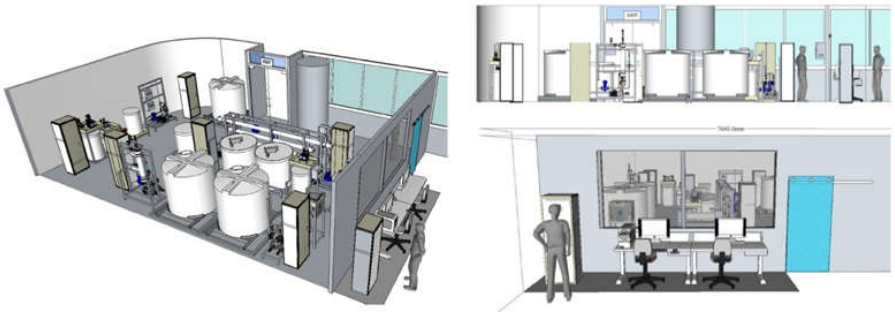
The third stage is expected to lead to enhancement of the defence mechanism using a redesign of the hardware and updated PLC and SCADA software. The redesigned defence mechanism will then be tested against a variety of attacks in the updated simulation model and the testbed.

The **SWaT Dataset** – systematically generated from the testbed over 7 days under normal

operation and 4 days with attack scenarios is available here.

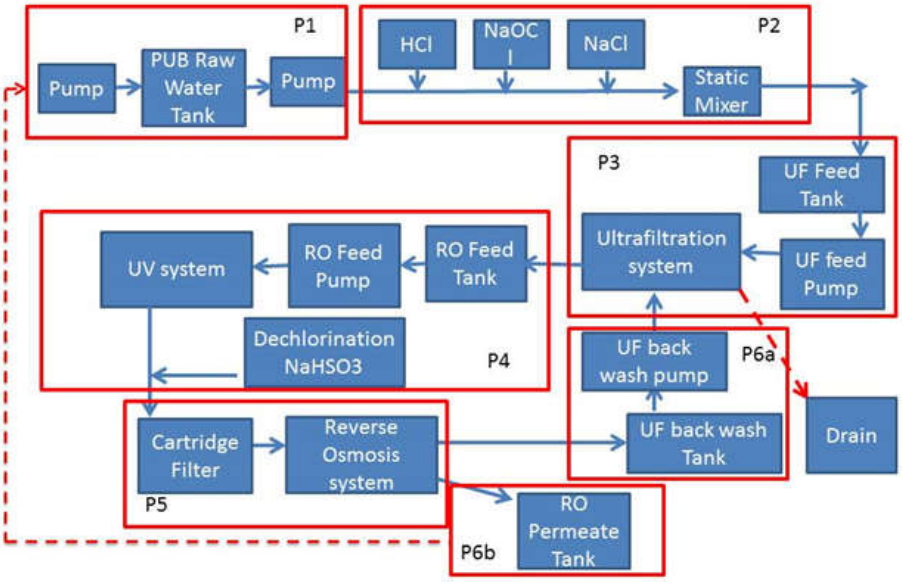
Collaboration

iTrust is collaborating with CISCO, National Instruments, NEC and StarHub, as well as several Singapore government agencies. PUB is a key partner in the design of SWaT. iTrust researchers will work closely with PUB engineers in all stages of this research.

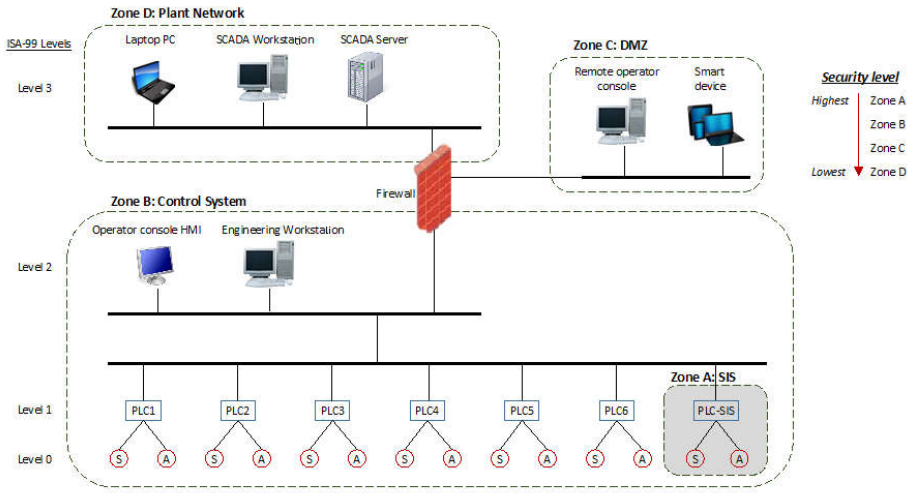


SWaT Installation Layout

Left: Ultra Filtration | Right: Overall Process Layout



SWaT Architecture



SWaT Architecture

Click here for more details.
