INTRODUCTION

Aim

This documentation provides readers with an in-depth understanding of how the Secure Water Treatment (SWaT) testbed works, the capabilities it is equipped with as a platform for **research and experimentation, education and training and testing.** Included in this document also are the technical details relating to the operation, components, drawings, equipment list and control and communication network of SWaT.

Background

Operational since March 2015, SWaT is a key asset for researchers aiming at the design of **safe and secure cyber-physical systems (CPS.)** The testbed consists of a modern six-stage water treatment process that closely mimics a real world treatment plant. Stage 1 of the **physical process** begins by taking in raw water, followed by chemical dosing (Stage 2), filtering it through an Ultrafiltration (UF) system (Stage 3), dechlorination using UV lamps (Stage 4), and then feeding it to a Reverse Osmosis (RO) system (Stage 5). A backwash process (Stage 6) cleans the membranes in UF using the RO permeate.

The **cyber portion** of SWaT consists of a layered communications network, Allen-Bradley 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.

Research and Experimentation

Notable aspects of the testbeds include segmented communications networks, wired and wireless communications, distributed dynamic control, interconnection among the testbeds, and complete access to the control logic inside the PLCs and HMIs. Access to them allows researchers to develop their own code and upload it in the controllers for research and experimentation. It also allows them to demonstrate their technologies in a **safe, controlled and realistic environment.**

Our **SWaT dataset** consists of 11 days of continuous operation – of which 7 days' worth of data was collected under normal operation while 4 days' worth of data was collected with attack scenarios. During the data collection, all network traffic, sensor and actuator data were collected. The dataset (available upon request) is highly sought after, with requests from more than 140 researchers from over 30 countries.

Education and Training

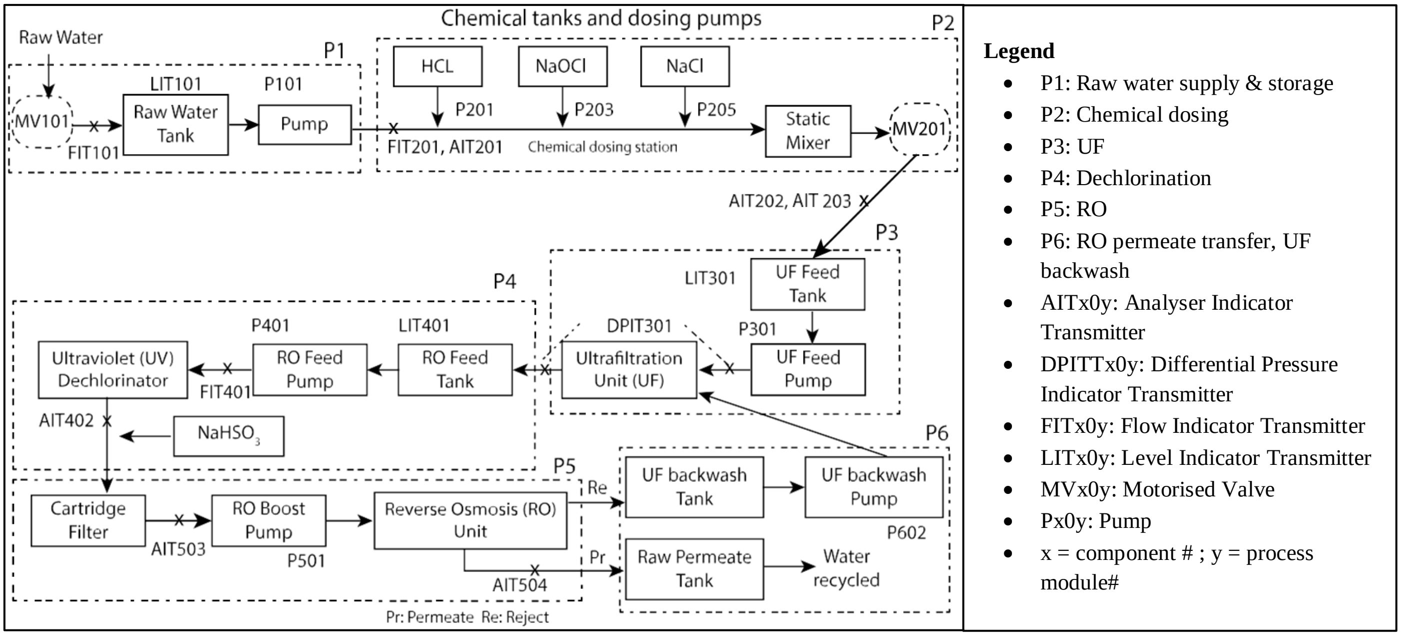
SWaT is being used by students from SUTD's Master of Science Security by Design (MSSD) programme as an **education and training platform** to cement and bring to life concepts introduced in the classroom. It is also offered to organisations in training their **operational technology (OT) personnel** in cyber incidents.

Testing

iTrust has organised two international competitions, named SUTD Security Showdown (S3), attracting researchers and engineers from US, Europe, and Asia to attack SWaT and enabling iTrust researchers and companies to **test their technologies** when a testbed is under attack by independent attackers. At the request of our collaborators, iTrust has also been involved in the **proof-of-concept** of defensive technologies installed on SWaT.

PROCESS AND SYSTEM OVERVIEW

Each of the six sub-processes, referred to as P1 through P6, is controlled by a set of dual Allen-Bradley PLCs, a primary and a redundant hot-standby. The operation status of the PLCs is monitored by the SCADA system. These sub-processes are shown in Figures 1 and 2.



Legend

- P1: Raw water supply & storage
- P2: Chemical dosing
- P3: UF
- P4: Dechlorination
- P5: RO
- P6: RO permeate transfer, UF backwash
- AITx0y: Analyser Indicator Transmitter
- DPITTx0y: Differential Pressure Indicator Transmitter
- FITx0y: Flow Indicator Transmitter
- LITx0y: Level Indicator Transmitter
- MVx0y: Motorised Valve
- Px0y: Pump
- x = component # ; y = process module#

Figure 1: SWaT's six-stage processes

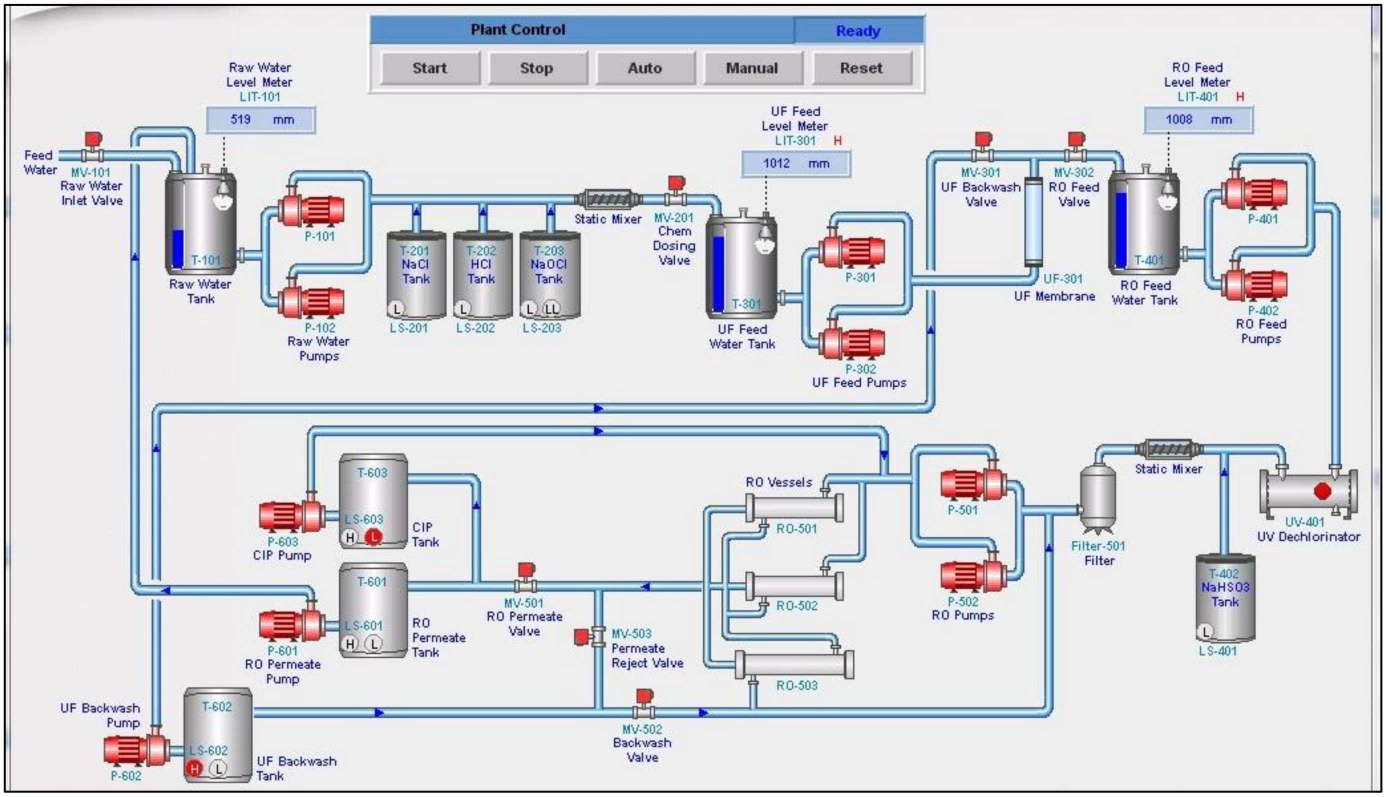


Figure 2: HMI/SCADA screenshot