SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

iTrust Centre for Research in Cyber Security

Water Distribution (WADI) Testbed

Version: 1.2
Last updated: 16 October 2018
Contact information: itrust@sutd.edu.sg
Website: https://itrust.sutd.edu.sg/

INTRODUCTION

Aim

This documentation provides readers with an in-depth understanding of how the Water Distribution (WADI) 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 WADI.

Background

Operational since July 2016, WADI is a key asset for researchers aiming at the design of **safe and secure cyber-physical systems (CPS.)** WADI is a natural extension of SWaT, comprising two elevated reservoir tanks, six consumer tanks, two raw water tanks and a return tank. It also comes equipped with chemical dosing systems, booster pumps and valves, instrumentation and analysers. WADI takes in a portion of SWaT's reverse osmosis permeate and raw water, thus forming a complete and realistic water treatment, storage and distribution network. The combination of these two testbeds allow researchers to witness the cascading effects of cyber attacks on one testbed to another.

Unlike a water treatment system plant which is typically contained in a secured location, a distribution system comprises numerous pipelines spanning across a large, and often less secured, area. This highly increases the risk of physical attacks on a distribution network. Thus, in addition to attacks and defences being carried out on the PLCs and networks, WADI has the capabilities to simulate the effects of **physical attacks** such as water leakage and malicious chemical injections. Together with SWaT, WADI provides opportunities for researchers to work on a full spectrum of possible cyber and physical attacks on a water treatment and distribution plant.

The **cyber portion** of WADI consists of a layered communications network, three National Instruments Programmable Logic Controllers (PLCs) and two Schneider Electric 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. In WADI, we consciously opted for a different PLC brand from SWaT, so that researchers can verify our defence models on different PLC brands. Exposing our defence models to a variety of PLC brands also helps us determine how robust our models are.

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 **WADI datasets** consist of 14 days of continuous normal operation and 2 days' worth of data was collected with attack scenarios. During the data collection for normal operation, all sensor and actuator data were collected. For attack scenarios, the attack scenarios and impact on the plant was recorded. The dataset (available upon request) is highly sought after, with requests from more than 150 researchers from over 30 countries.

Education and Training

WADI, like the other testbeds, is being offered to organisations for joint research programs and usage.

PROCESS AND SYSTEM OVERVIEW

Each of the processes, referred to as P1 through P3, is controlled by a set of National Instruments PLCs. The operation status of the PLCs is monitored by the SCADA system. These processes are shown in Figures 1 and 2.

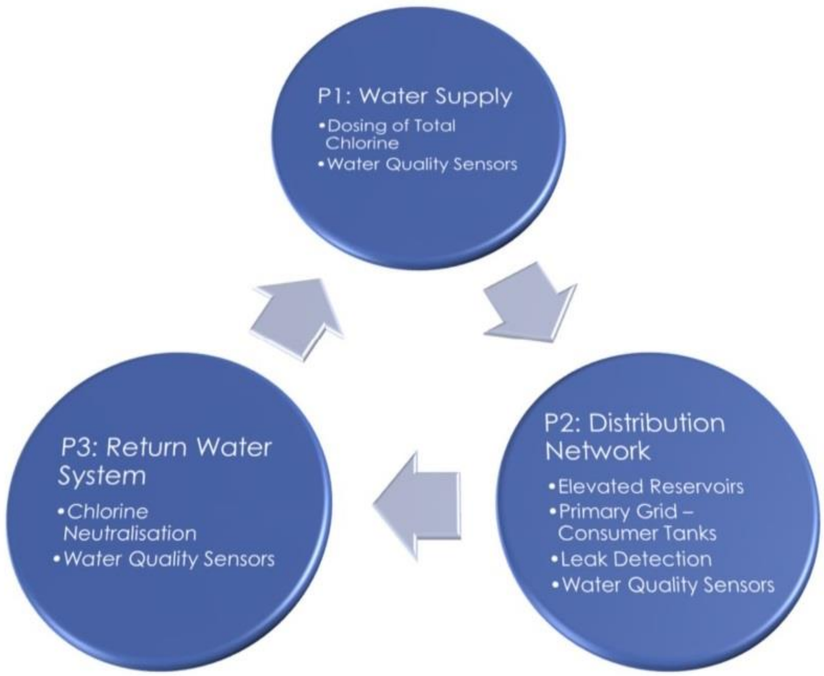

Figure 1: WADI's three-stage processes

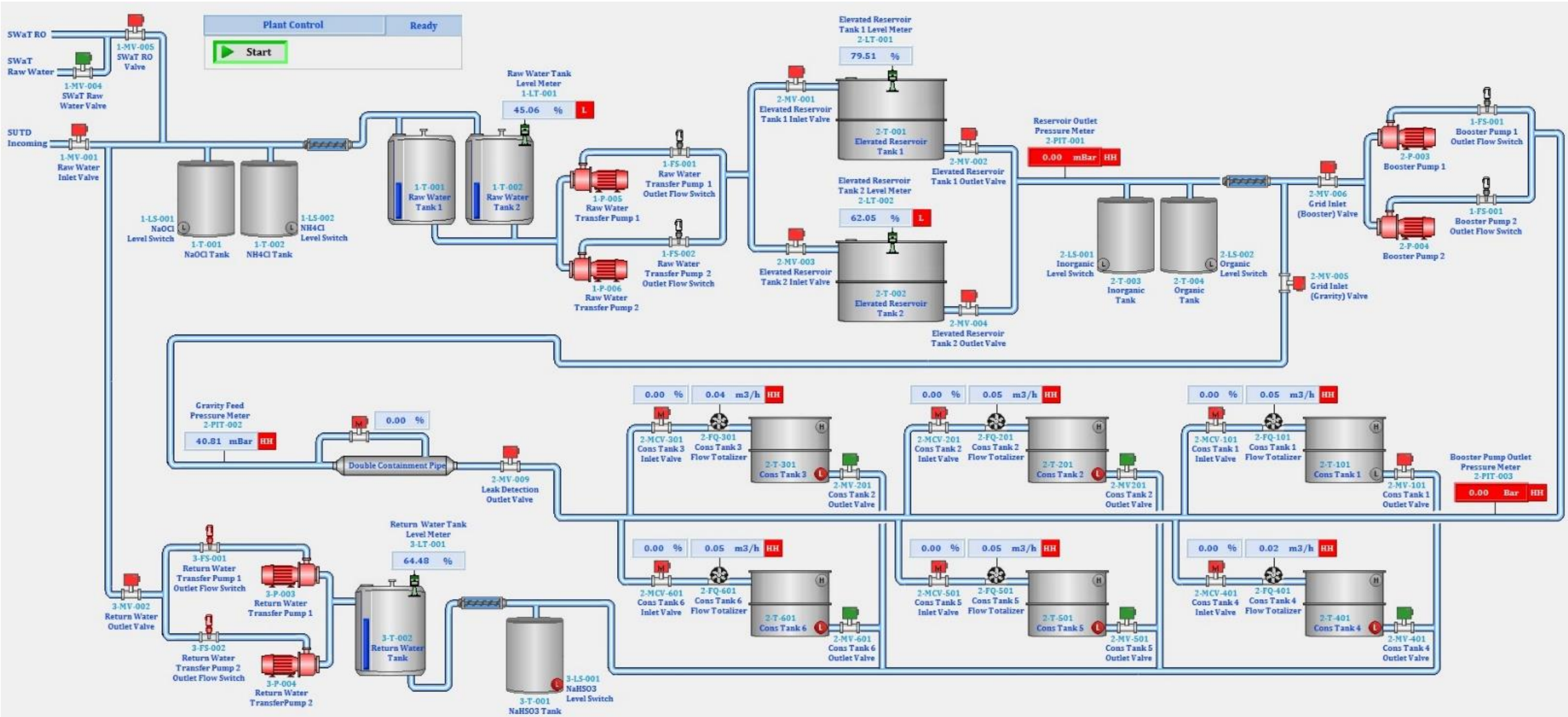

Figure 2: HMI/SCADA screens

COMPONENTS (SENSORS AND ACTUATORS)

WADI consists of an array of monitoring sensors to ensure its safe operations. These are:

- Level Transmitter (measured in %)
- Flow Indication Transmitter (m^3/hr)
- Analyser Indicator Transmitter
  - Conductivity (µS/cm)
  - pH
  - Oxidation Reduction Potential (mV)
  - Turbidity (NTU)
  - Total Residual Chlorine (mg/L)
- Pressure Meter (mBar)
- Flow Totalizer (m^3/hr)
- Modulating Valve (%)

The sensors and actuators associated with each PLC are shown in Table 1 and Figure 3 below:

Table 1: PLC Brands for WADI Processes

PLC	Brand	Process
P1	National Instruments	Primary Grid (Water Supply)
P2A	Schneider Electric	Elevated Reservoir
P2B	Schneider Electric	Booster Station
P2C	National Instruments	Consumer Tank
P3	National Instruments	Return Water

Figure 3: Sensors and actuators associated with each PLC

PIPING AND INSTRUMENTATION DIAGRAMS (P&ID)

A piping and instrumentation diagram (P&ID) shows the piping and vessels in the process flow, together with the instrumentation and control devices. This website explains the common symbols found in P&ID diagrams.

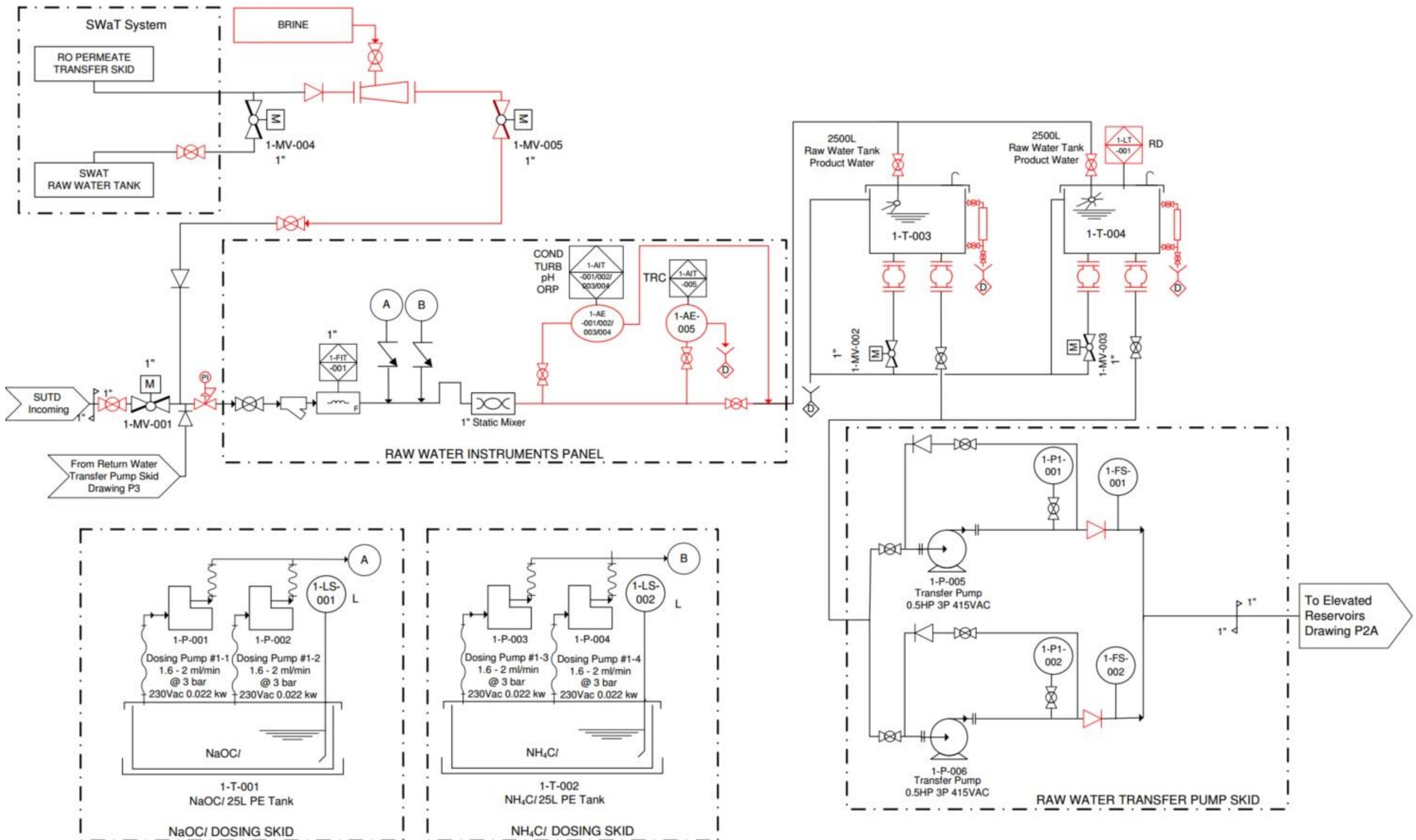

Figure 4: P&ID for P1 (Water Supply)

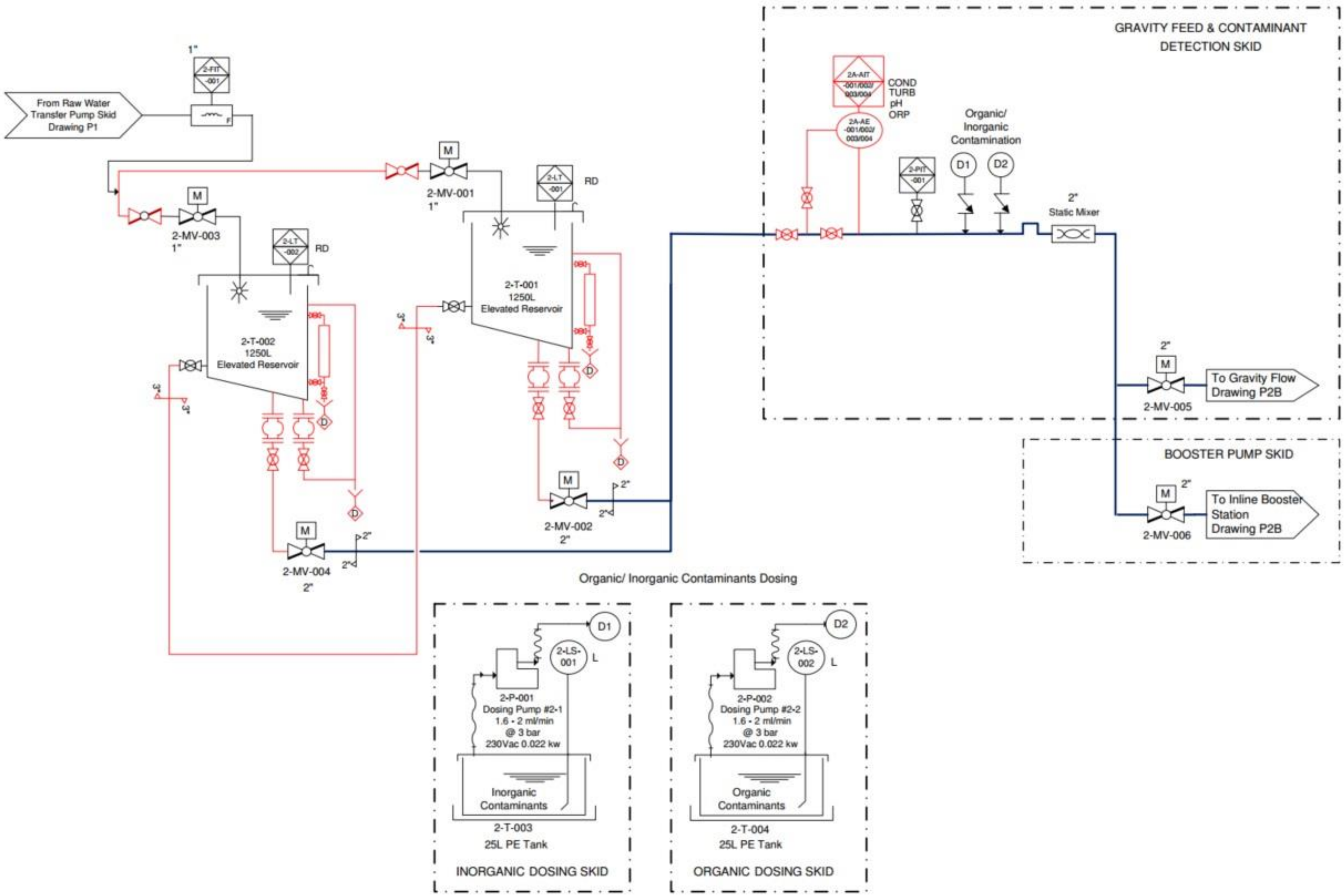

Figure 5: P&ID for P2A (Elevated Reservoir and Contaminant Dosing)

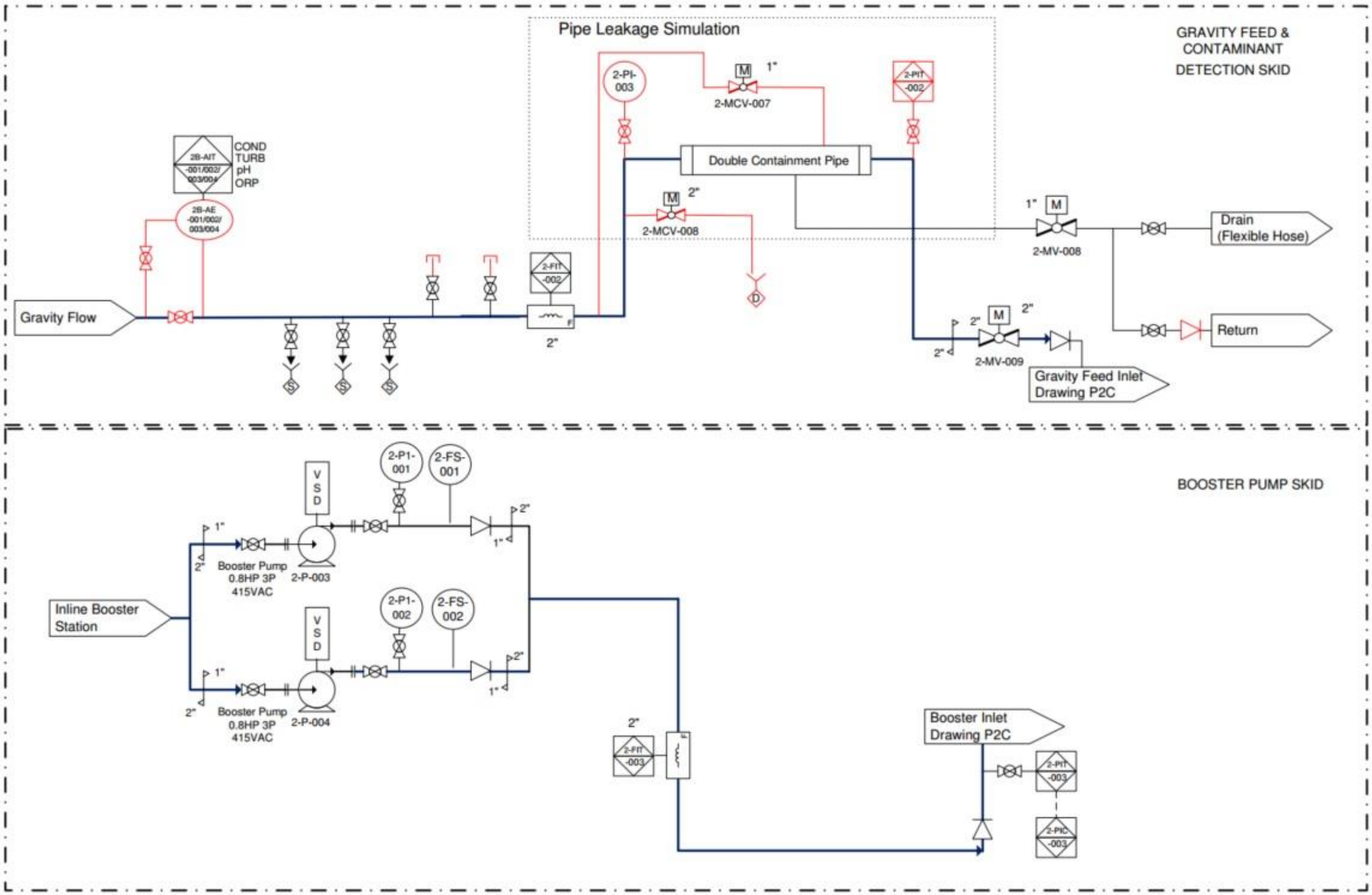

Figure 6: P&ID for P2B (Booster Station and Pipe Leakage Simulation)

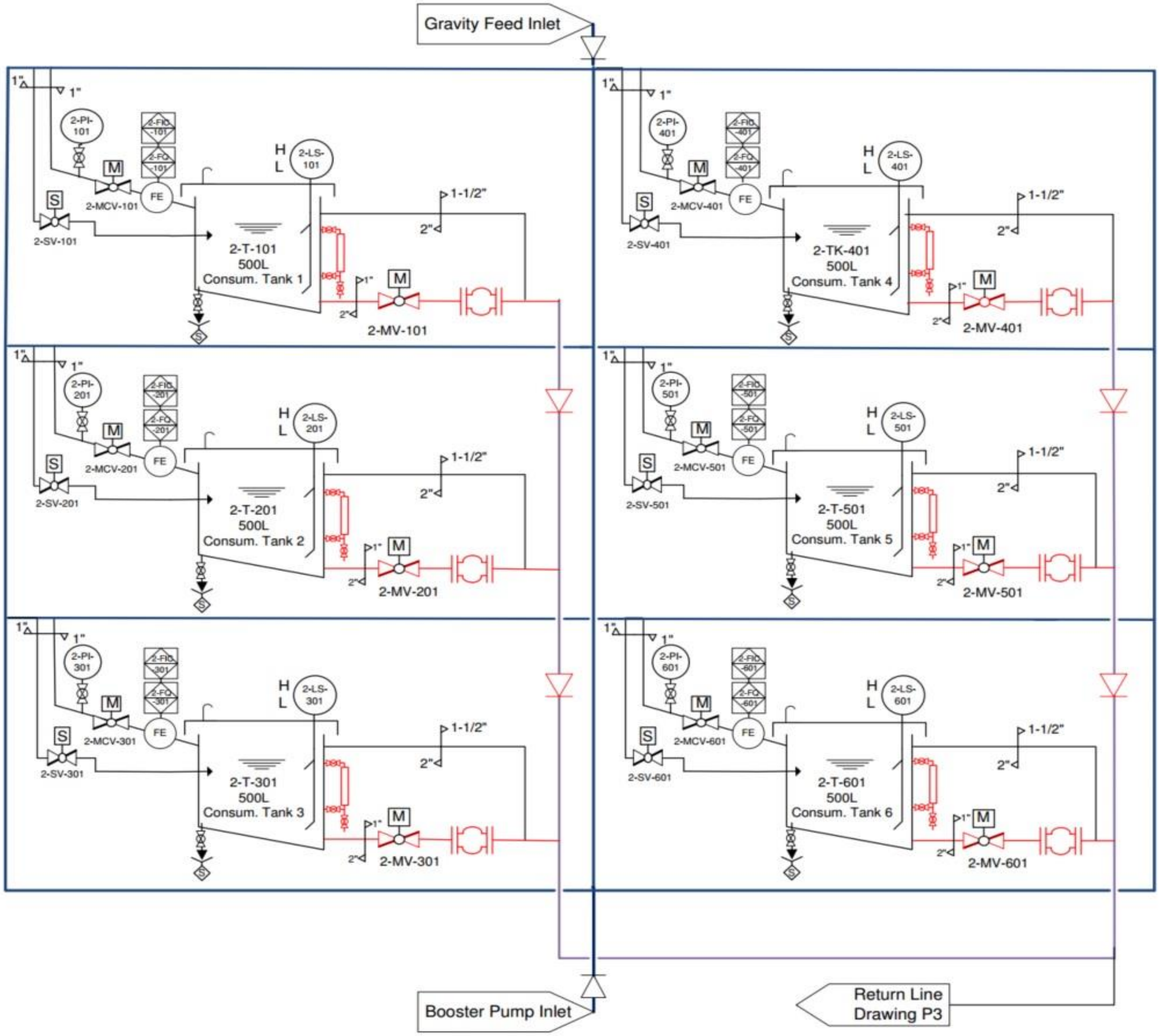

Figure 7: P&ID for P2C (Consumer Tank Grid)

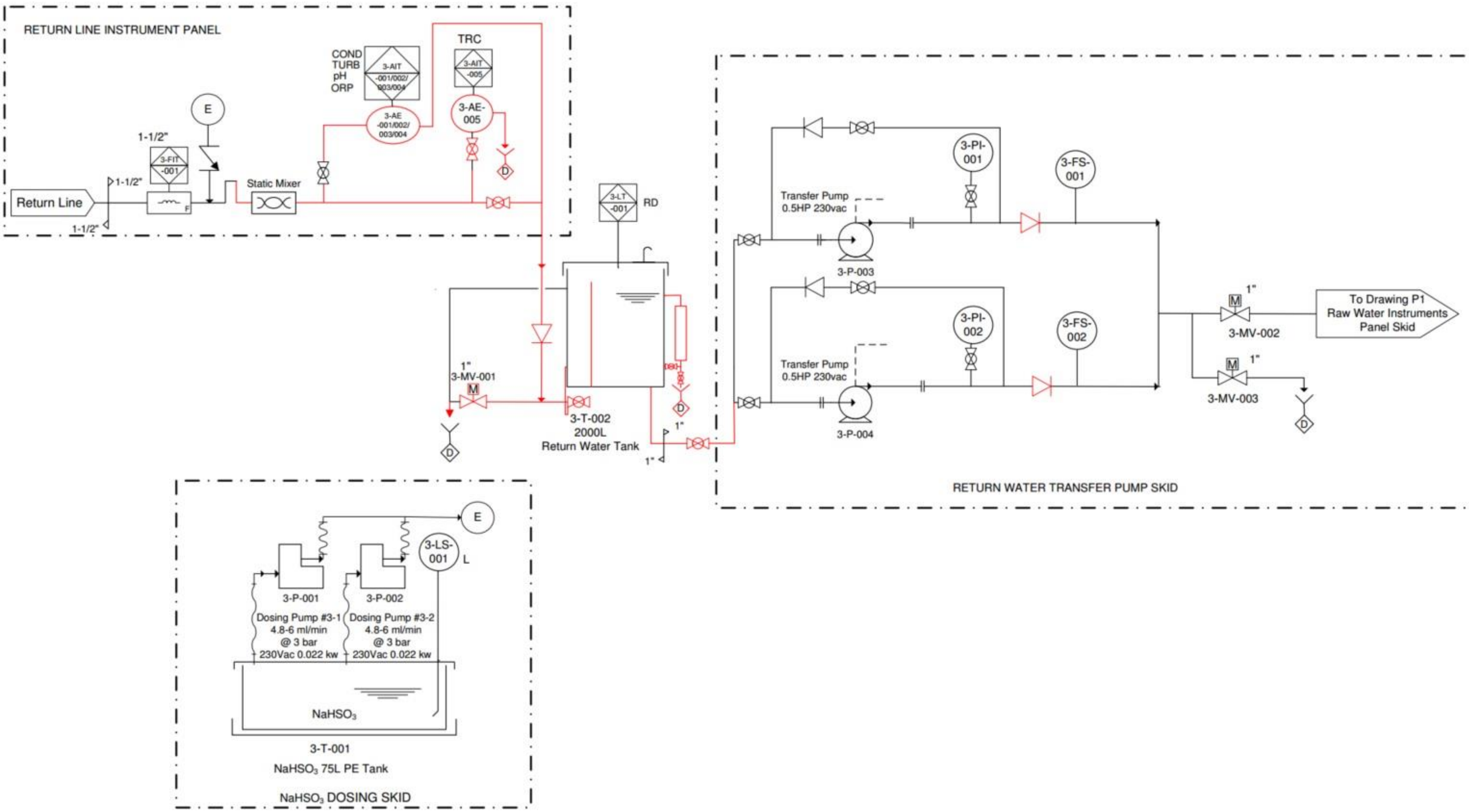

Figure 8: P&ID for P3 (Return Water System)

EQUIPMENT LIST

Table 2: Equipment list for P1 (Water Supply)

Description	Design Specification	Material	Qty	Brand & Model	Remarks
Pumps & Tanks					
Raw Water Tank	Capacity: 2.5m³	Tank Wall: FRP Stand & Base: Mild Steel	2	Customised	With Drain Valve at Bottom
Raw Water Transfer Pump	Duty: 2.5 m³/h @ 20m	Casing: Chrome Nickel SS Impeller: Noryl Shaft: SS	2	CALPEDA MXH 203	
Chemical Dosing Pumps	Capacity : 0.78 l/h @ 5 bar	Liquid end : Plexiglas Diaphragm : PTFE faced	4	Prominent GALa1601	
Instrumentation					
Level Transmitters	Radar, Range 0.2 to 6m	Non Contact	1	iSOLV RD 700	
Flow Transmitter	Electromagnetic DN40	PTFE	1	iSOLV EFS803/CFT183	
Multi Probe Analyser	pH/ ORP/ Conductivity & Turbidity		1	Hydrolab HL4	
Total Chlorine Analyser	TRC 0-5ppm		1	W&T Depolox 3	
Piping & Accessories					
Piping	SCH80	PVC	Lot		
On/Off Valve	DN 25, Electric Actuated	PVC	3	Burkert Type 3003	

Table 3: Equipment list for P2 (Elevated Reservoir, Contaminant Dosing, Leakage Simulation, Consumer Grid)

Description	Design Specification	Material	Qty	Brand & Model	Remarks
Pumps & Tanks					
Elevated Reservoir Water Tank	Capacity: 1.25 m³	Tank Wall: FRP Stand & Base: Mild Steel	2	Customised	With Drain Valve at Bottom
Consumer Water Tank	Capacity: 0.5 m³	Tank Wall: FRP Stand & Base: Mild Steel	6	Customised	With Drain Valve at Bottom
Inline Booster Pump	Duty: 2.5 m³/h @ 40m	Casing: Chrome Nickel SS Impeller: Noryl Shaft: SS	2	CALPEDA MXV25	With VSD Control
Contaminant Dosing Pumps	Capacity : 0.78 l/h @ 5 bar	Liquid end : Plexiglas Diaphragm : PTFE faced	2	Prominent GALa1601	
Instrumentation					
Level Transmitter	Radar, Range 0.2 to 6m	Non Contact	1	iSOLV RD 700	
Flow Transmitter	Electromagnetic DN50	PTFE	1	iSOLV EFS803/CFT183	
Multi Probe Analyser	pH/ ORP/ Conductivity & Turbidity		2	Hydrolab HL4	
Pressure Transmitter	0-10 Bar		3	iSOLV SPT 200	
Piping & Accessories					
Piping	SCH80	PVC	Lot		
On/Off Valve	DN 25, Electric Actuated	PVC	3	Burkert Type 3003	
On/Off Valve	DN 50, Electric Actuated	PVC	4	Burkert Type 3003	
Modulating Valve	DN 25, 4-20mA	PVC	7	Burkert Type 3003	
Modulating Valve	DN 50, 4-20mA	PVC	1	Burkert Type 3003	
Solenoid Valve	DN 25, 2/2 Way, NC	Brass	6	Burkert Type 6213	

Table 4: Equipment list for P3 (Return Water System)

Description	Design Specification	Material	Qty	Brand & Model	Remarks
Pumps & Tanks					
Return Water Tank	Capacity: 2 m^3	Tank Wall: FRP Stand & Base: Mild Steel	1	Customised	With Drain Valve at Bottom
Return Water Transfer Pump	Duty: 2.5 m^3/h @ 20m	Casing: Chrome Nickel SS Impeller: Noryl Shaft: SS	2	CALPEDA MXH 203	
Sodium Bisulfite Dosing Pumps	Capacity : 0.78 l/h @ 5 bar	Liquid end : Plexiglas Diaphragm : PTFE faced	2	Prominent GALa1601	
Instrumentation					
Level Transmitter	Radar, Range 0.2 to 6m	Non Contact	1	iSOLV RD 700	
Flow Transmitter	Electromagnetic DN40	PTFE	1	iSOLV EFS803/CFT183	
Multi Probe Analyser	pH/ ORP/ Conductivity & Turbidity		1	Hydrolab HL4	
Total Chlorine Analyser	TRC 0-5ppm		1	W&T Depolox 3	
Piping & Accessories					
Piping	SCH80	PVC	Lot		
On/Off Valve	DN 25, Electric Actuated	PVC	2	Burkert Type 3003	

CONTROL AND COMMUNICATION NETWORK

The network architecture for WADI complies with the [Industrial Automation and Control Systems Security- ISA99](), a security standard for industrial automation and control systems. This standard suggests a core concept which is "Zone and Conduits" and "Layer". It offers a level of segmentation and traffic control inside the Control and Communication Network, and is designed to support both wired and wireless network communication.

<u>Layers</u>

- Layer 3.5 – Demilitarised Zone (DMZ)
- Layer 3 – Operation Management (Historian)
- Layer 2 – Supervisory Control (Touch Panel, Engineering Workstation, HMI Control Clients)
- Layer 1 – Plant Control Network (PLCs) (Star Topology)
- Layer 0 – Process (Actuator/Sensors and Input/output modules)

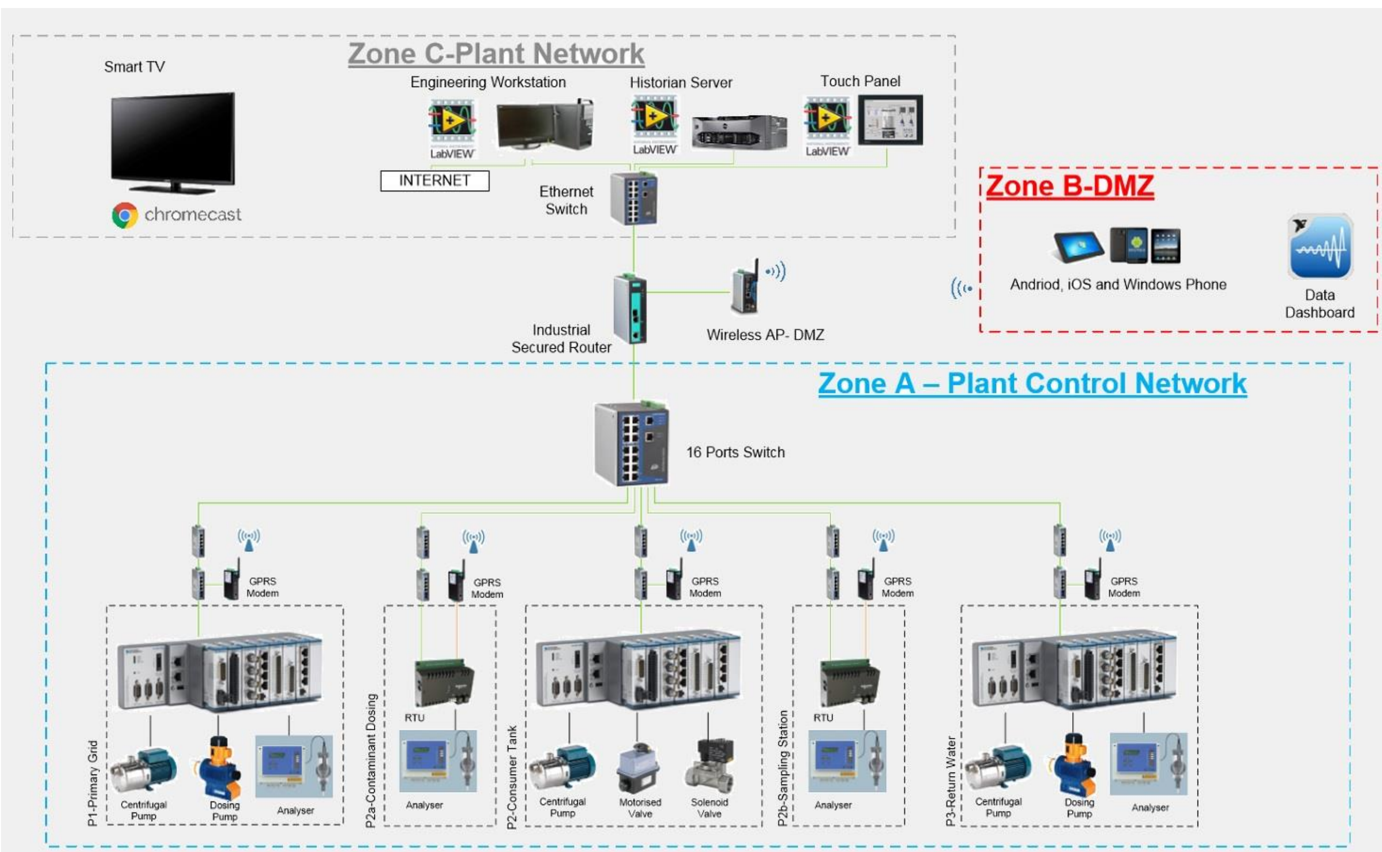

Figure 6: WADI Network Architecture

NETWORK PROTOCOL

All network communication between PLCs in Layer 1 and above use the industrial EtherNet/IP (EN/IP) and Common Industrial Protocol (CIP) stack.

For Layer 0, electrical signals/feedbacks of both Actuators and Transmitters are sent to the PLC directly (the PLC and RIO modules are integrated together), unlike SWaT. Digital signals (actuators) are of DC24V electrical signals, and Analog Signals (Transmitters) are of 4-20 mA electrical signals.

For water quality analysers (pH, ORP, Conductivity, Turbidity), Modbus RS485 communication is used.

Wireless Communication High Speed Packet Access (HSPA) is provided as a wireless option for Layer 1 Network.

IP ADDRESS

The IP addresses of the five PLCs and SCADA in WADI are shown in Table 5 below.

Table 5: IP address of PLCs

System	Device	IP Address
P1 - Primary Grid	cRIO Adapter Port 1	192.168.10.10
	cRIO Adapter Port 2	207.117.40.241
	GPRS Modem	192.168.10.11
P1 - Consumer Tank	cRIO Adapter Port 1	192.168.10.20
	cRIO Adapter Port 2	207.117.40.242
	GPRS Modem	192.168.10.21
P2A - Contaminants Dosing	SCADAPack 334 RTU	192.168.10.30
	GPRS Modem	192.168.10.31
P2B - Sampling Station	SCADAPack 334 RTU	192.168.10.40
	GPRS Modem	192.168.10.41
P3 - Return Water	cRIO Adapter Port 1	192.168.10.50
	cRIO Adapter Port 2	207.117.40.243
	GPRS Modem	192.168.10.51
Touch Screen	12" Touch Panel	192.168.20.100
SCADA	Industrial Secured Router	192.168.10.100
	Wireless Access Point	192.168.20.30
	Historian Server	192.168.20.200
	Engineering Workstation	192.168.20.201

iTrust
Centre for Research
in Cyber Security