Secure Water Treatment (SWaT) Testbed

Version: 4.2
Last updated: 5 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 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.

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.

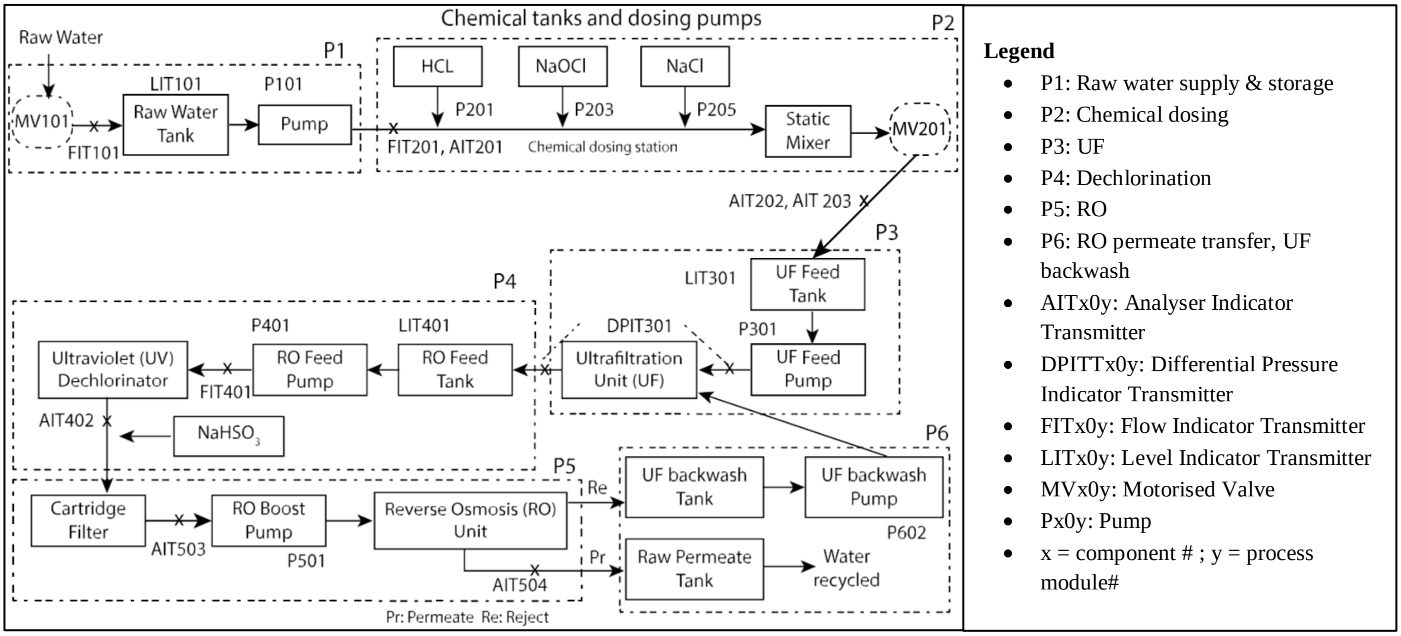

Figure 1: SWaT's six-stage processes

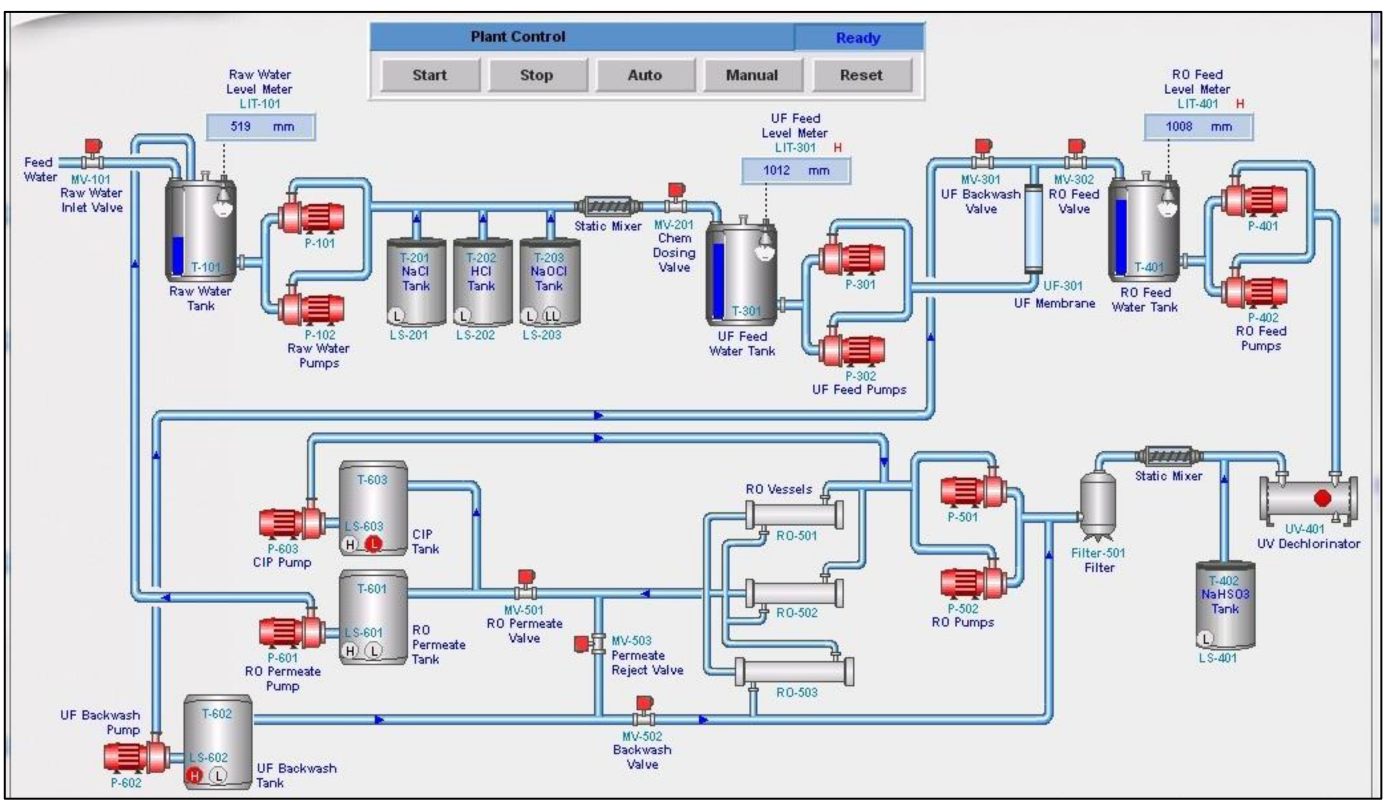

Figure 2: HMI/SCADA screenshot

COMPONENTS (SENSORS AND ACTUATORS)

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

- Level Indication Transmitter (measured in mm)
- Flow Indication Transmitter (m^3/hr)
- Analyser Indicator Transmitter
  - Conductivity (µS/cm)
  - pH
  - Oxidation Reduction Potential (mV)
- Differential Pressure Indicator Transmitter (kPa)
- Pressure Indicator Transmitter (kPa)

The sensors and actuators associated with each PLC are shown in Figure 3 below.

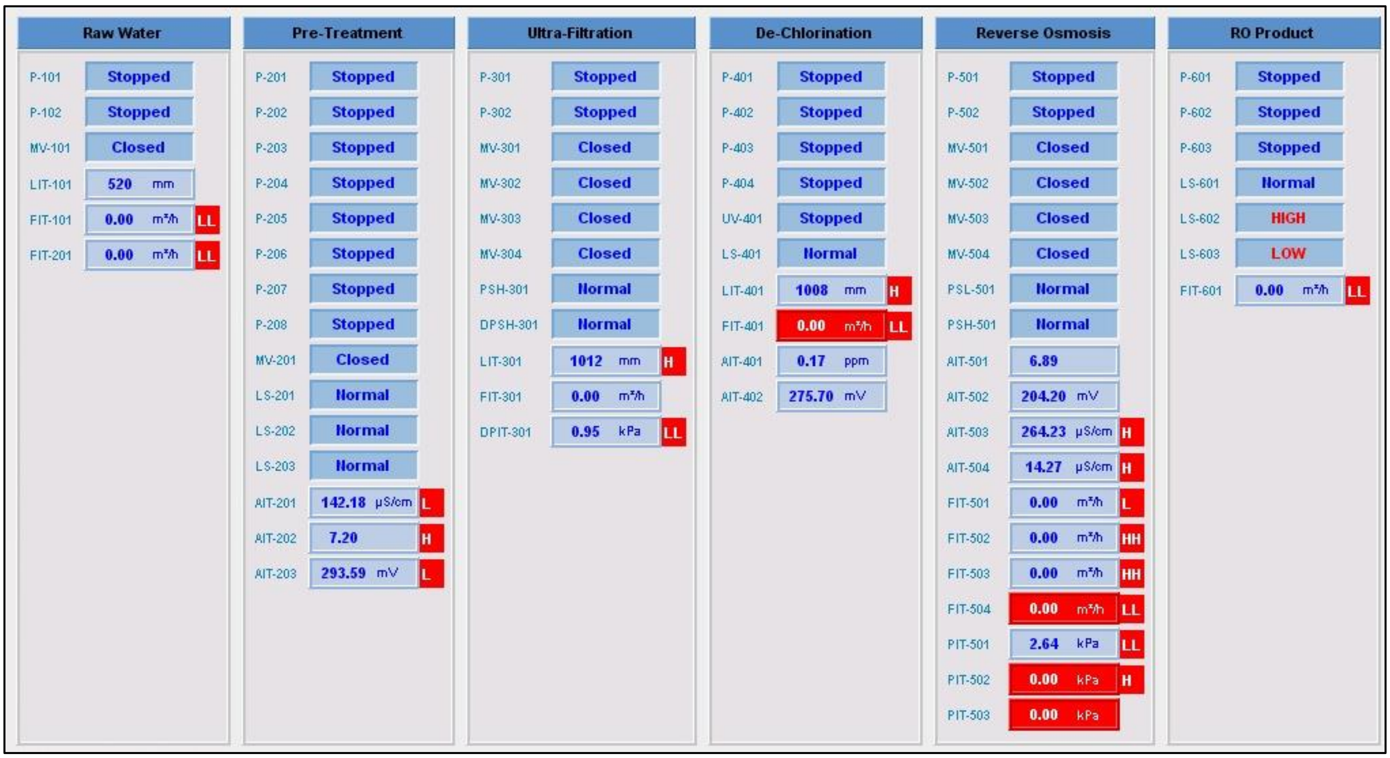

Figure 3: Sensors and actuators associated with each PLC

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.

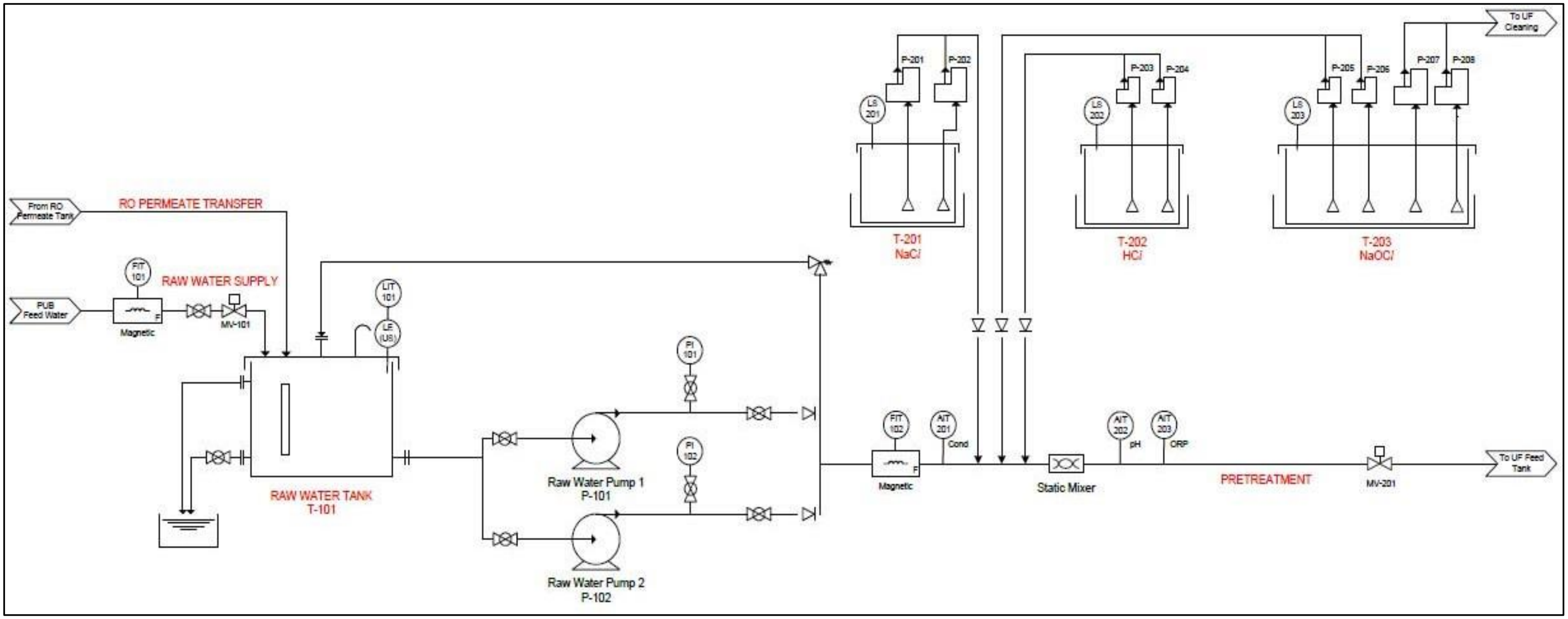

Figure 4: P&ID for P1 (raw water) and P2 (chemical dosing)

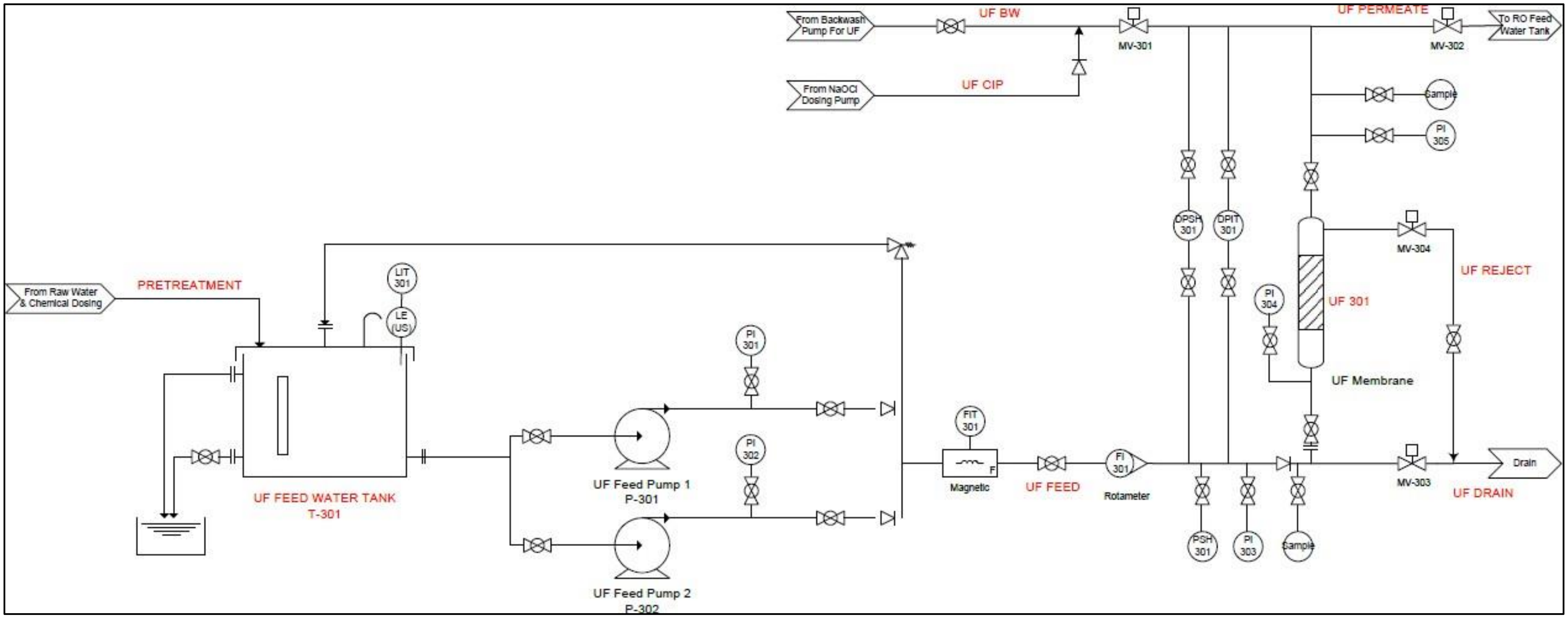

Figure 5: P&ID for P3 (ultrafiltration)

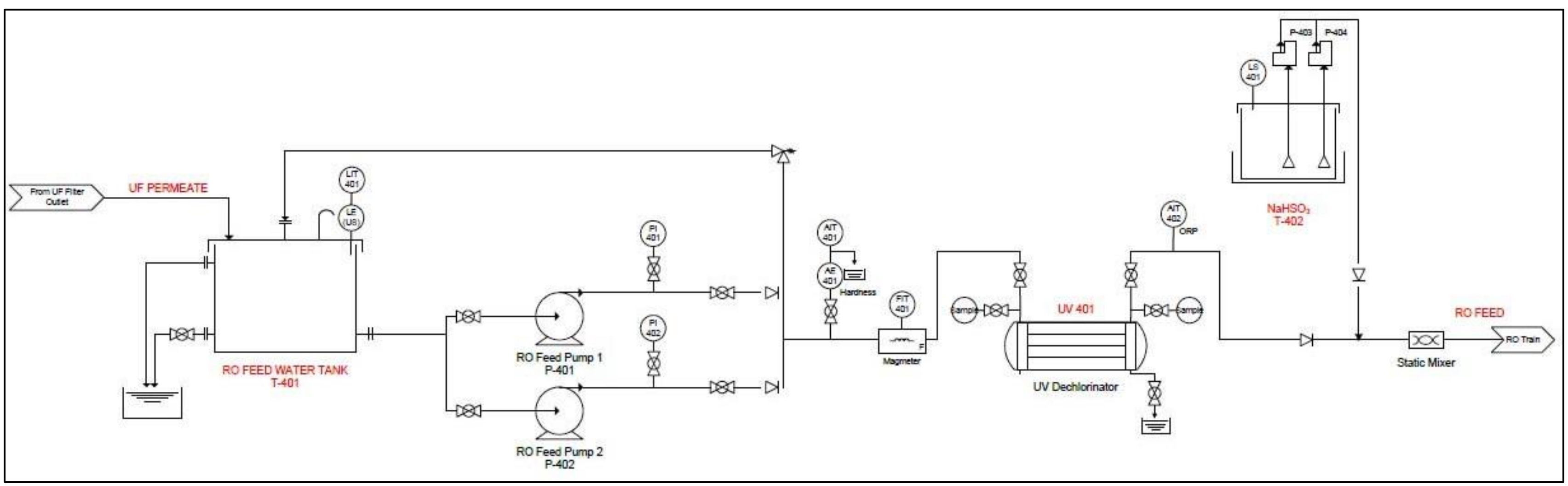

Figure 6: P&ID for P4 (dechlorination)

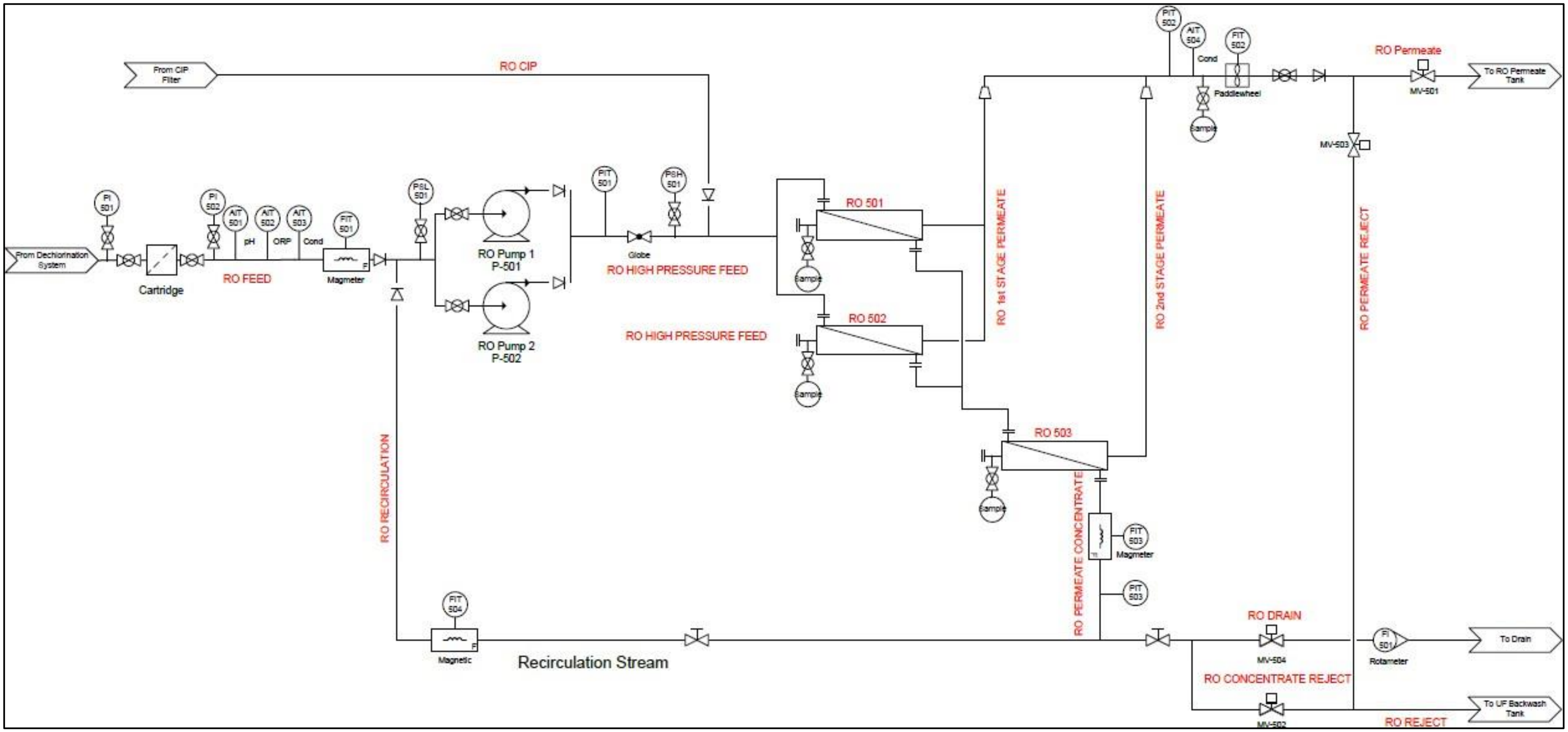

Figure 7: P&ID for P5 (RO)

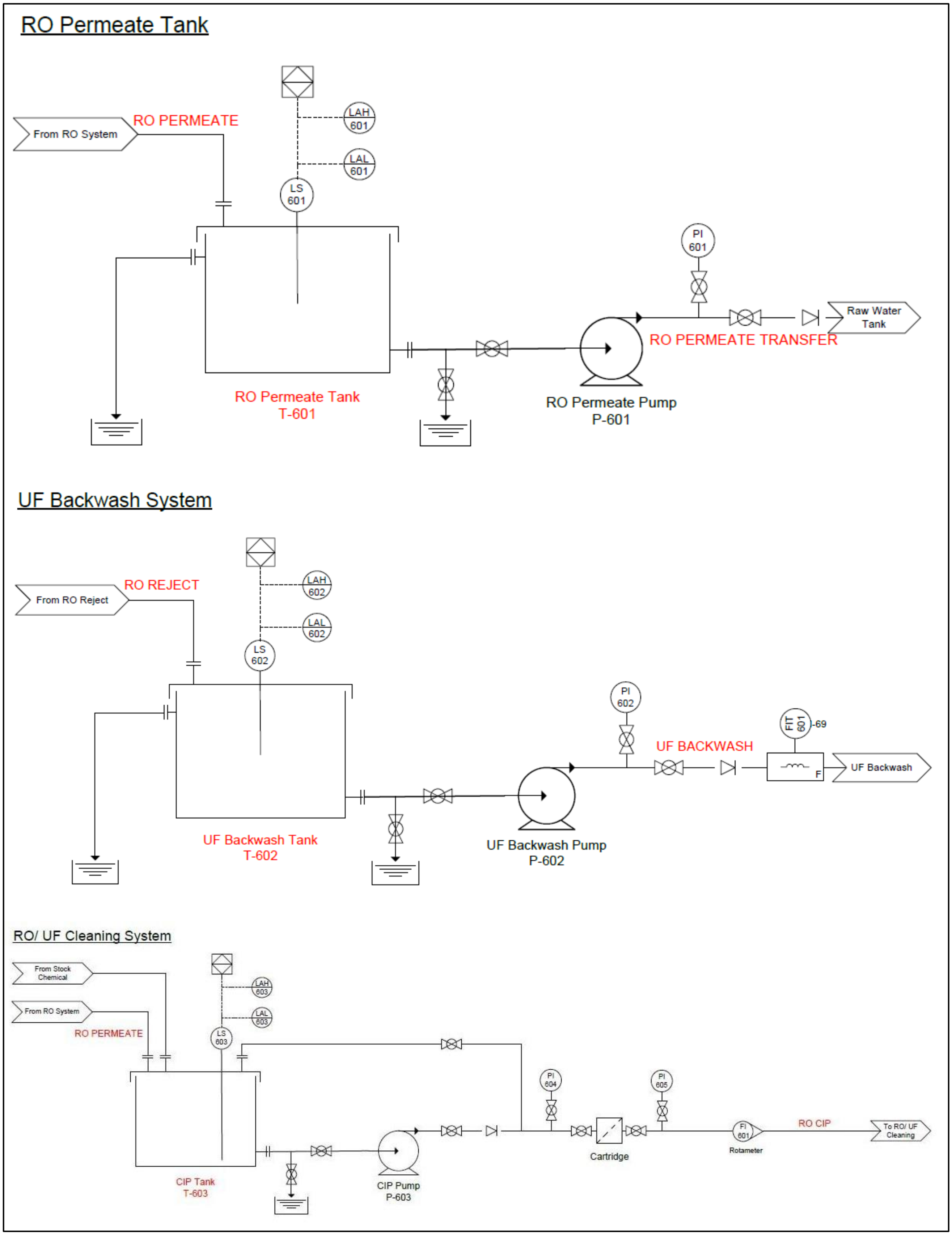

Figure 8: P&ID for (from top) P6_1 (RO Permeate Module), P6_2 (UF Backwash module) and P6_3 (RO/UF Cleaning Module)

EQUIPMENT LIST

Table 1: Equipment list for P1 (raw water)

Description	Design Specification	Material	Qty	Brand & Model	Remarks
Pumps & Tanks					
Raw Water Tank	Capacity: 1.8m³ Dia xH= 1.38 x 1.36	PE	1	Rotamas CPE 1800	**T101**
Raw Water Transfer Pump	Duty: 2.5 m³/h @ 20m	Casing: Chrome Nickel SS Impeller: Noryl Shaft: SS	2	CALPEDA MXH 203	**P101/102**
Instrumentation					
Raw Water Tank LIT	Ultrasonic, Range 0.2 to 6m	Non Contact	1	iSOLV LevelWizard II	**LIT101**
Raw Water FIT	Electromagnetic DN25	PTFE	1	iSOLV EFS803/CFT183	**FIT101**
Piping & Accessories					
Piping	SCH80	PVC	Lot	Glywed	
Raw Water Inlet On/Off Valve	DN 25, Electric Actuated	PVC	1	Burkert EV2650	**MV101**
PRV	DN 25	PVC	1	Prominent DHV-DM PVC	

Table 2: Equipment list for P2 (chemical dosing)

Description	Design Specification	Material	Qty	Brand & Model	Remarks
Pumps & Tanks					
NaC*l* Tank	Capacity: 250*l*	PE	1	Rotamas CGD 250	
NaC*l*Dosing Pump	Capacity : 50 *l*/h @ 10 bar	Liquid end : PVDF Diaphragm : PTFE faced	2	Prominent Sigma S1Ba	**P201/202**
HC*l* Tank	Capacity: 250*l* Capacity: 25*l* (9% HC*l*)	PE	1	Rotamas CGD 250 25L Carboy	Double Containment
HC*l*Dosing Pump	Capacity : 0.78 *l*/h @ 08 bar	Liquid end : Plexiglas Diaphragm : PTFE faced	2	Prominent GALa1601	**P203/204**
NaOC*l* Tank	Capacity: 250*l*	PE	1	CGD 250	
NaOC*l*Dosing Pump (FAC)	Capacity : 0.78 *l*/h @ 8 bar	Liquid end : Plexiglas Diaphragm : PTFE faced	2	Prominent GALa1601	**P205/206**
NaOC*l*Dosing Pump (UF Cleaning)	Capacity : 65*l*/h @ 7 bar	Liquid end : PVDF Diaphragm : PTFE faced	2	Prominent Sigma S1Ba	**P207/208**
Instrumentation					
Static Mixer	2" NPT M/ 12 elements	PVC	1	Omega	
Raw Water to UF Feed Tank FIT	Electromagnetic DN25	PTFE	1	iSOLV EFS803/CFT183	**FIT201**
AIT - Conductivity	Up to 1000µS/cm	-	1	Mettler Toledo M200 Single/ easySense Cond 71	**AIT201**
AIT – pH & ORP	pH: 0-14 ORP: -800mV to 800mV	-	1	Mettler Toledo M200 Dual/ easySense pH 32 & ORP 41	**AIT202/203**
NaC*l* Level Switch	Low Alarm	PVC	1	iSOLV LS880	**LS201**
HC*l* Level Switch	Low Alarm	PVC	1	iSOLV LS880	**LS202**
NaOC*l* Level Switch	Low Alarm	PVC	1	iSOLV LS880	**LS203**
Piping & Accessories					
Piping	SCH80	PVC	Lot	Glywed	
Raw Water Tank Outlet On/Off Valve	DN 25, Electric Actuated	PVC	1	Burkert EV2650	**MV201**

Table 3: Equipment list for P3 (ultrafiltration)

Description	Design Specification	Material	Qty	Brand & Model	Remarks
UF Membranes					
UF Membranes	2.5 m^3/h	PVDF	1	TORAY HFU-2020	
Pumps & Tanks					
UF Feedwater Tank	Capacity: 1.8m^3 Dia xH= 1.38 x 1.36	PE	1	Rotamas CPE 1800	**T301**
UF Feedwater Pump	Duty: 2.5 m^3/h @ 20m	Casing: Chrome Nickel SS Impeller: Noryl Shaft: SS	2	CALPEDA MXH 203	**P301/302**
Instrumentation					
UF Feed Water Tank LIT	Ultrasonic, Range 0.2 to 6m	Non Contact	1	iSOLV LevelWizard II	**LIT301**
UF Feed Water FIT	Electromagnetic DN25	PTFE	1	iSOLV EFS803/CFT183	**FIT301**
UF Feed Water FI	Rotameter, 1"	PVC	1	FSIV Flowmeter	**FI301**
Pressure Switch	Switch High/ 0-7 Bar Adjustable	SS316 Port	1	CCS 604GZ	**PSH301**
Differential Pressure Switch	Switch High/ 0-1 Bar	SS316 Port	1	CCS 604DZ	**DPSH301**
Differential Pressure Indicating Transmitter	Range: 0-2 Bar	SS316 Port	1	SPT 100 DP	**DPIT301**
Piping & Accessories					
Piping & Manual Valves	SCH80	PVC	Lot	Glywed	
PRV	DN 25	PVC	1	Prominent DHV-DM PVC	
Backwash On/Off Valve	DN 25, Electric Actuated	PVC	4	Burkert EV2650	**MV301/2/3/4**

Table 4: Equipment list for P4 (dechlorination)

Description	Design Specification	Material	Qty	Brand & Model	Remarks
Pumps & Tanks					
RO Feedwater Tank	Capacity: 1.8m^3 Dia xH= 1.38 x 1.36	PE	1	Rotamas CPE 1800	**T401**
RO Feedwater Pump	Duty: 2.5 m^3/h @ 20m	Casing: Chrome Nickel SS Impeller: Noryl Shaft: SS	2	CALPEDA MXH 203	**P401/402**
$NaHSO_3$ Tank	Capacity: 250*l* Capacity: 25*l* (10% $NaHSO_3$)	PE	1	Rotamas CGD 250 25L Carboy	Double Containment
$NaHSO_3$ Dosing Pump	Capacity : 0.78 *l*/h @ 8 bar	Liquid end : Plexiglas Diaphragm : PTFE faced	2	Prominent GALa1601	**P403/404**
UV Chlorine Destruction Unit					
UV Unit	Removal up to 0.5ppm 2.3m^3/h	SS316	1	Aquafine Optima 200	**UV401**
Instrumentation					
RO Feed Water Tank LIT	Ultrasonic, Range 0.2 to 6m	Non Contact	1	iSOLV LevelWizard II	**LIT401**
Hardness Monitor	Range: 0-10ppm	-	1	HACH APA 6000	**AIT401**
AIT –ORP	ORP: -800mV to 800mV	-	1	Mettler Toledo M200 SingleI/ easySense ORP 41	**AIT402**
RO Feed FIT	Electromagnetic DN25	PTFE	1	iSOLV EFS803/CFT183	**FIT401**

Table 5: Equipment list for P5 (RO)

Description	Design Specification	Material	Qty	Brand & Model	Remarks
RO Membranes					
Pre RO Cartridge Filter	Heavy Duty Multi-Cartridge Housing Max Pressure: 125PSI Number of Cartridges &Size: (4) 10" Flowrate: 28 GPM Element: 1 Micron	SS304 Housing	1	Graver 4MC1-VB-316L-1.5N-B	
RO Membrane	As Per Design Considerations	-	3+3 4	Toray TMH10A	
RO Vessel	-	Shell: Epoxy/Glass Composites	3	Pentair Codeline40S30	
Pumps					
High Pressure RO Pump With VSD	Duty: 2m³/h @ 5bar	Casing: Chrome Nickel SS Impeller: Noryl Shaft: SS	2	CALPEDA MXH206	**P501/5**
Instrumentation					
AIT – Conductivity (RO Feed)	Up to 1000µS/cm	-	1	Mettler Toledo M200 Dual/ easySense Cond 71	**AIT503**
AIT – Conductivity (RO Permeate)	Range: 0.02 to 20 µS/cm	-	1	easySense Cond 71	**AIT504**

Description	Design Specification	Material	Qty	Brand & Model	Remarks
AIT – pH & ORP (RO Feed)	pH: 0-14 ORP: -800mV to 800mV	-	1	Mettler Toledo M200 Dual/ easySense pH 32 & ORP 41	**AIT501 / 502**
Pressure Switch (Before High Pressure RO Pump)	Low Alarm, 0-10 Bar (Adjustable)	SS316 Port	1	CCS 604GZ	**PSL501**
Pressure Switch (After High Pressure RO Pump)	High Alarm, 0-10 Bar (Adjustable)	SS316 Port	1	CCS 604GZ	**PSH501**
PIT (After High Pressure RO Pump)	0-10 Bar	SS316 Port	1	iSOLV SPT 100	**PIT501**
PIT (RO Concentrate)	0-10 Bar	SS316 Port	1	iSOLV SPT 100	**PIT503**
PIT (RO Permeate)	0-10 Bar	SS316 Port	1	iSOLV SPT 100	**PIT502**
FIT (RO Concentrate)	Electromagnetic DN25	PTFE	1	iSOLV EFS803/CFT183	**FIT503**
FIT (RO Recirculation)	Electromagnetic DN25	PTFE	1	iSOLV EFS803/CFT183	**FIT504**

Table 6: Equipment list for P6 (RO permeate transfer, UF backwash)

Description	Design Specification	Material	Qty	Brand & Model	Remarks
Pumps & Tanks					
RO Permeate Tank	Capacity: 1.2m³ DiaxH = 1.16 x 1.24	PE	1	Rotamas CPE 1200	**T601**
RO Permeate Transfer Pump	Duty: 2.5 m³/h @ 20m	Casing: Chrome Nickel SS Impeller: Noryl Shaft: SS	1	CALPEDA MXP 203	**P601**
UF Backwash Tank	Capacity: 1.2m³ DiaxH = 1.16 x 1.24	PE	1	Rotamas CPE 1200	**T602**
UF Backwash Tank Pump	Duty: 2.5 m³/h @ 20m	Casing: Chrome Nickel SS Impeller: Noryl Shaft: SS	1	CALPEDA MXP 203	**P602**
CIP Tank (UF/RO)	Capacity: 550*l*	PE	1	CGD 550	
CIP Pump	Duty: 2.5 m³/h @ 20m	Casing: Chrome Nickel SS Impeller: Noryl Shaft: SS	1	CALPEDA MXP 203	**P603**

Description	Design Specification	Material	Qty	Brand & Model	Remarks
Cartridge Filter					
Pre RO Cartridge Filter	Heavy Duty Multi-Cartridge Housing Max Pressure: 125PSI Number of Cartridges &Sze: (4) 10" Flowrate: 28 GPM Element: 1 Micron	SS304 Housing	1	Graver 4MC1-VB-316L-1.5N-B	
Instrumentation					
RO Permeate Tank Level Switch	Low & High Alarm	PVC	1	iSOLV LS880	**LS601**
UF Backwash Tank Level Switch	Low & High Alarm	PVC	1	iSOLV LS880	**LS602**
CIP Tank Level Switch	Low & High Alarm	PVC	1	iSOLV LS880	**LS603**
FIT (UF Backwash)	Electromagnetic DN25	PTFE	1	iSOLV EFS800/CFT180	**FIT601**
FI (RO/UF Cleaning)	Rotameter, 1"	PVC	1	FSIV Flowmeter	**FI601/2**

CONTROL AND COMMUNICATION NETWORK

The network architecture for SWaT 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.

Layers

- 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 Network)
- Layer 0 – Process (Actuator/Sensors and Input/output modules) (Ring Network)

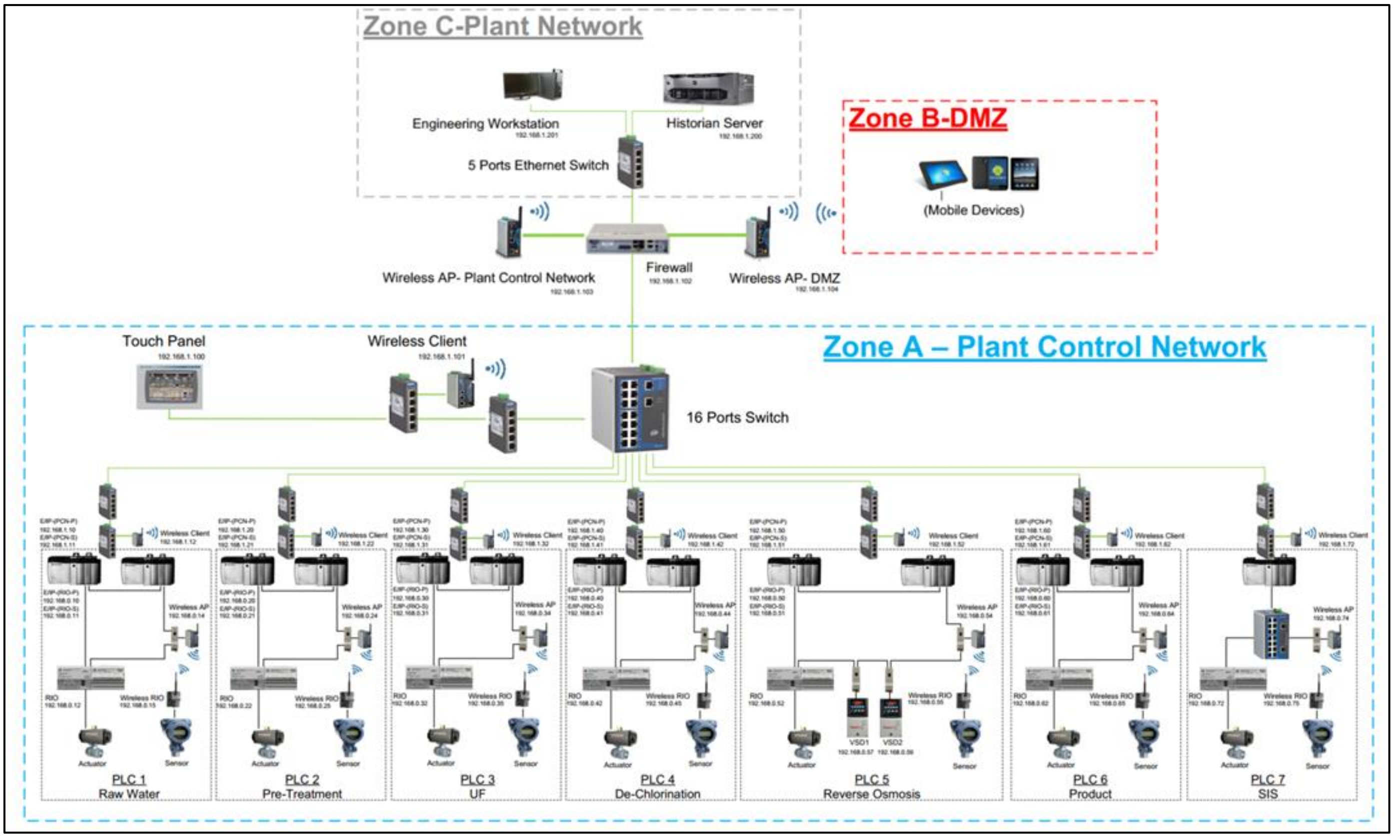

Figure 9: SWaT network architecture (PLC7 is for training/testing)

NETWORK PROTOCOL AND MONITORING AND DECODING

Network Protocol

All network communication by PLCs, sensors and actuators in SWaT is using the industrial EtherNet/IP and Common Industrial Protocol (CIP) stack. Specifically:

1) CIP[1] over EtherNet/IP (Network level 1)

2) EtherNet/IP (Network level 0 i.e. between PLC and remote I/O)

Network Monitoring and Decoding

Researchers perform network traffic monitoring and decoding, using tools such as Wireshark (monitoring/listening), Scapy (decoding, Ethernet/IP reverse-engineering) and Ettercap (network sniffing, MITM attacks). Examples of these processes are shown below.

```
Almost every second, there will be packets coming from HMI to PLC1 which look
like this eg:     hex-offset   hex-packet (read from top-left to right-bottom)::

    0000   80 1d 9c c8 bd e7 00 1d 9c c6 72 e8 08 00 45 00
    0010   00 5e 2f 95 40 00 80 06 47 46 c0 a8 01 64 c0 a8
    0020   01 0a c2 03 af 12 8e 7a 43 87 01 bd 1e 5e 50 18
    0030   82 9c 2a 07 00 00 70 00 1e 00 02 00 16 00 00 00
    0040   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    0050   00 00 00 00 02 00 a1 00 04 00 20 42 b5 ff b1 00
    0060   0a 00 8a 07 4c 03 20 b2 25 00 22 00

and right after, a response from PLC1 to HMI::

    0000   80 1d 9c c6 72 e8 00 1d 9c c8 bd e7 08 00 45 00
    0010   00 b8 12 13 40 00 40 06 a4 6e c0 a8 01 0a c0 a8
    0020   01 64 af 12 c2 03 01 bd 1e 5e 8e 7a 43 bd 50 18
    0030   20 00 e8 5f 00 00 70 00 78 00 02 00 16 00 00 00
    0040   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    0050   00 00 00 00 02 00 a1 00 04 00 9d 36 00 80 b1 00
    0060   64 00 8a 07 cc 00 00 00 01 00 00 00 00 00 eb 14
    0070   d3 43 01 00 01 00 01 00 02 00 0c 00 00 00 40 40
    0080   00 00 80 40 00 00 80 3f 00 00 00 3f 24 00 00 48
    0090   44 00 80 89 44 00 00 2f 44 00 00 7a 43 13 01 00
    00a0   0b 01 00 01 0b 01 00 01 00 01 00 00 00 00 03 00
    00b0   00 04 00 01 00 01 05 00 eb 14 d3 43 06 00 00 00
    00c0   00 00 52 66 14 42

Once decoded with scapy, these packets become::

    ###[ Ethernet ]###
      dst       = 00:1d:9c:c8:bd:e7
      src       = 00:1d:9c:c6:72:e8
      type      = 0x800
    ###[ IP ]###
         version   = 4L
         ihl       = 5L
         tos       = 0x0
         len       = 94
         id        = 12181
         flags     = DF
         frag      = 0L
         ttl       = 128
         proto     = tcp
         chksum    = 0x4746
         src       = 192.168.1.100
         dst       = 192.168.1.10
         \options   \
    ###[ TCP ]###
            sport     = 49667
            dport     = EtherNet_IP_2
            seq       = 2390377351
            ack       = 29171294
            dataofs   = 5L
            reserved  = 0L
            flags     = PA
            window    = 33436
            chksum    = 0x2a07
            urgptr    = 0
            options   = []
```

[1] The Common Industrial Protocol (CIP) and the Family of CIP Networks gives a comprehensive look at how CIP and its network implementations are designed. The guide is a great starting point for those who are new to CIP Networks.

```
    ###[ ENIP_TCP ]###
              command_id= SendUnitData
              length     = 30
              session    = 1441794
              status     = success
              sender_context= 0
              options    = 0
    ###[ ENIP_SendUnitData ]###
                 interface_handle= 0
                 timeout    = 0
                 count      = 2
                 \items      \
                  |###[ ENIP_SendUnitData_Item ]###
                  |  type_id    = conn_address
                  |  length     = 4
                  |###[ ENIP_SendUnitData_Item ]###
                  |  type_id    = conn_packet
                  |  length     = 100
                  |###[ ENIP_ConnectionPacket ]###
                  |     sequence  = 1930
                  |###[ CIP ]###
                  |        direction = response
                  |        service   = Read_Tag_Service
                  |        \path      \
                  |        \status    \
                  |         |###[ CIP_ResponseStatus ]###
                  |         |  reserved  = 0x0
                  |         |  status    = success
                  |         |  additional_size= 0x0
                  |         |  additional= ''
                  |###[ Raw ]###
                  |           load      = '\x01\x00\x00 [[ SNIPPED ]] \x14B'

Therefore:

* HMI is requesting to read tag ``class 0xb2,instance 0x22`` on PLC1.  In this
  request, the class ID never change but the instance ID may change.
* PLC1 is responding with a successful status and a binary blob of data.  This
  data is the concatenation of several tags, and it is only needed to find the
  offset where the water level is reported to be able to modify it (there is
  no authentication nor integrity check of the result).
```

Figure 10: Sample network packet monitoring and decoding using Wireshark and Scapy respectively

```
As ettercap works from the TCP payload, here is this payload from another
network capture, with some important values::

    0000   70 00 ------------------------------------------ ENIP Send Unit Data command
      02         65 00 02 00 25 00 00 00 00 00 00 00 00 00
    0010   00 00 00 00 00 00 00 00 00 00 00 00 00 00
      1e                                            02 00 - ENIP item count
    0020   a1 00 ------------------------------------------ ENIP first item: Connected Address Item
      22         04 00 ------------------------------------                 length = 4 bytes
      24               db e8 00 80
      28                           b1 00 ------------------ ENIP second item: Connected Data Item
      2a                                 51 00 ------------ Size of CIP packet: 81 bytes (= 0x51)
      2c                                       78 ed
      2e                                            cc 00 - CIP response to Read Tag Service
    0030   00 00 ------------------------------------------ CIP response status: OK
      32         01 00 00 00 00 00
      38                           c5 8e 6d 44 ------------ Water level (LIT101 tag): 0x446d8ec5 = 950.23
      3c                                       01 00 ------ Motored Valve MV101 off (on is "02 00")
      3e                                            02 00 - Pump P101 state: open
    0040   01 00 ------------------------------------------ Pump P102 state: closed
      42         02 00 0c 00 00 00 40 40 00 00 80 40 00 00
    0050   80 3f 00 00 00 3f 22 00 00 48 44 00 80 89 44 00
    0060   00 fa 43 00 00 7a 43 13 01 00 0b 02 00 01 0b 01
    0070   00 01 01 01 00 00 00 00 03 00 02 00 01

The water level is encoded in little-endian single-precision floating-point
format (IEE 754, https://en.wikipedia.org/wiki/Single-precision_floating-point_format),
so bytes ``c5 8e 6d 44`` can be decoded in a simple Python program::

program::
=======

    import binascii, struct
    print(struct.unpack('<f', binascii.unhexlify('c58e6d44'))[0])

which displays ``950.2307739257812``.

To find the offset of this value, it is possible to quickly scroll in Wireshark
the CIP payloads of packets matching the filter
``cip.service == 0xcc && cip.class == 0xb2``, and two bytes would keep changing
a lot between packets, which would be the first bytes of ``c5 8e 6d 44`` here,
as they encode a part of the fraction part of the float number linked to a
real sensor.

Once the offset is found, it is possible to modify the bytes in an ettercap
filter, as it is done in ``mitm-b2cls_rdtag.ecf``.  For example value 420 is
encoded in bytes ``00 00 d2 43`` so this etterfilter code modifies the water
level to 420::
```

Figure 11: Sample process of modifying bytes in an Ettercap filter to modify tag values

IP ADDRESS

The IP addresses of the seven PLCs and SCADA in SWaT are shown below.

P1 - Raw Water	
Device	**IP Address**
E/IP (PCN) - Primary	192.168.1.10
E/IP (PCN) - Secondary	192.168.1.11
Wireless Client (PCN)	192.168.1.12
E/IP (RIO) - Primary	192.168.0.10
E/IP (RIO) - Secondary	192.168.0.11
RIO Adaptor	192.168.0.12
RIO Access Point	192.168.0.14
Wireless Adaptor	192.168.0.15

P2 - Pre-Treatment	
Device	**IP Address**
E/IP (PCN) - Primary	192.168.1.20
E/IP (PCN) - Secondary	192.168.1.21
Wireless Client (PCN)	192.168.1.22
E/IP (RIO) - Primary	192.168.0.20
E/IP (RIO) - Secondary	192.168.0.21
RIO Adaptor	192.168.0.22
RIO Access Point	192.168.0.24
Wireless Adaptor	192.168.0.25

P3 - Ultra-Filtration	
Device	**IP Address**
E/IP (PCN) - Primary	192.168.1.30
E/IP (PCN) - Secondary	192.168.1.31
Wireless Client (PCN)	192.168.1.32
E/IP (RIO) - Primary	192.168.0.30
E/IP (RIO) - Secondary	192.168.0.31
RIO Adaptor	192.168.0.32
RIO Access Point	192.168.0.34
Wireless Adaptor	192.168.0.35

P4 - De-Chlorination	
Device	**IP Address**
E/IP (PCN) - Primary	192.168.1.40
E/IP (PCN) - Secondary	192.168.1.41
Wireless Client (PCN)	192.168.1.42
E/IP (RIO) - Primary	192.168.0.40
E/IP (RIO) - Secondary	192.168.0.41
RIO Adaptor	192.168.0.42
RIO Access Point	192.168.0.44
Wireless Adaptor	192.168.0.45

P5 - Reverse Osmosis	
Device	**IP Address**
E/IP (PCN) - Primary	192.168.1.50
E/IP (PCN) - Secondary	192.168.1.51
Wireless Client (PCN)	192.168.1.52
E/IP (RIO) - Primary	192.168.0.50
E/IP (RIO) - Secondary	192.168.0.51
RIO Adaptor	192.168.0.52
RIO Access Point	192.168.0.54
Wireless Adaptor	192.168.0.55
ETAP (VSD 1)	192.168.0.56
VSD 1	192.168.0.57
ETAP (VSD 2)	192.168.0.58
VSD 2	192.168.0.59

P6 - RO Product	
Device	**IP Address**
E/IP (PCN) - Primary	192.168.1.60
E/IP (PCN) - Secondary	192.168.1.61
Wirelss Client (PCN)	192.168.1.62
E/IP (RIO) - Primary	192.168.0.60
E/IP (RIO) - Secondary	192.168.0.61
RIO Adaptor	192.168.0.62
RIO Access Point	192.168.0.64
Wireless Adaptor	192.168.0.65

P7 - SIS	
Device	**IP Address**
E/IP (PCN) - Primary	192.168.1.70
Wireless Client (PCN)	192.168.1.72
E/IP (RIO) - Primary	192.168.0.70
RIO Adaptor	192.168.0.72
RIO Access Point	192.168.0.74
Wireless Adaptor	192.168.0.75

SCADA System	
Device	**IP Address**
E/IP (PCN) - Primary	192.168.1.100
Wireless Client	192.168.1.101
Firewall	192.168.1.102
PCN Access Point	192.168.1.103
DMZ Access Point	192.168.1.104
Historian Server	192.168.1.200
Engineering Workstation	192.168.1.201

iTrust

Centre for Research in Cyber Security