Kaspersky Industrial Cybersecurity Conference 2019

September 18-20, 2019, Sochi, Russia

Validating defense mechanisms of cyber-physical systems via attack tools

Francisco Furtado

Salimah Liyakkathali

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

iTrust Centre for Research in Cyber Security

Agenda

iTrust

Cyber physical attacks & defense

A6 Tool

Demo

Findings & Conclusion

WHO WE ARE

FUNDING

NATIONAL RESEARCH FOUNDATION
PRIME MINISTER'S OFFICE
SINGAPORE

SINGAPORE UNIVERSITY OF
TECHNOLOGY AND DESIGN

iTrust
Centre for Research
in Cyber Security

COLLABORATORS

CARNEGIE MELLON UNIVERSITY PITTSBURGH PENNSYLVANIA 1900

PRINCETON UNIVERSITY 1746

Ben-Gurion University of the Negev

MISSOURI S&T

Imperial College London

NANYANG TECHNOLOGICAL UNIVERSITY

ADSC

WHO WE ARE

FOCUS AREAS

CPS

Enterprise Security

IoT

iTrust
Centre for Research in Cyber Security

DISTINCTIVE VALUES

Applied Research

Testbeds

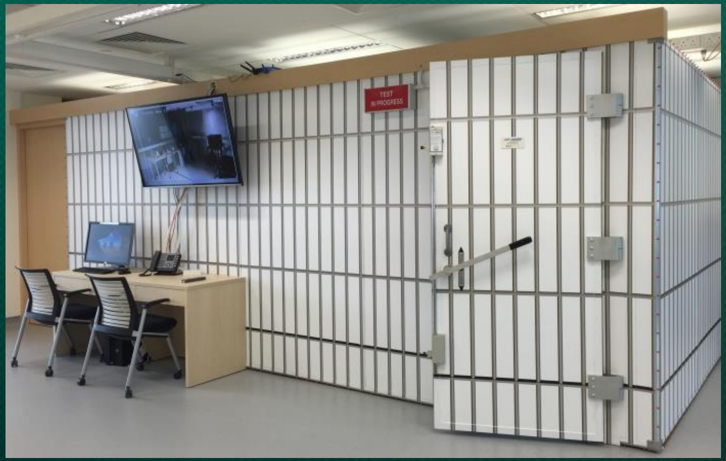
Multi-disciplinary

Students

Industry Collaboration

TESTBEDS

(IoT) Automatic Security



Secure Water Treatment (SWaT)

Electric Power and Intelligent Control (EPIC)

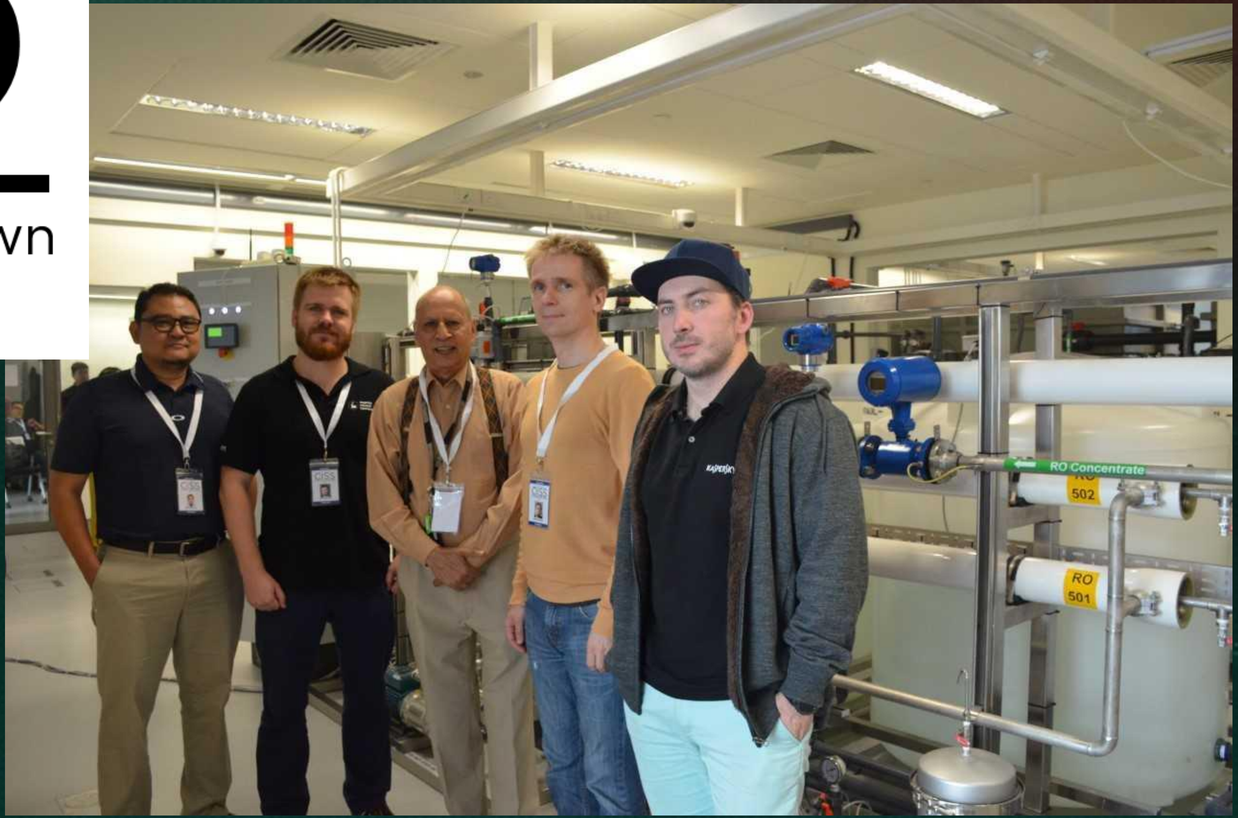
Water Distribution (WADI)

iTrust Event

CISS

Critical Infrastructure Security Showdown

2019



Cyber physical attacks

Maroochy shire sewage

Blaster worm

13 US auto plants

Offshore oil platform

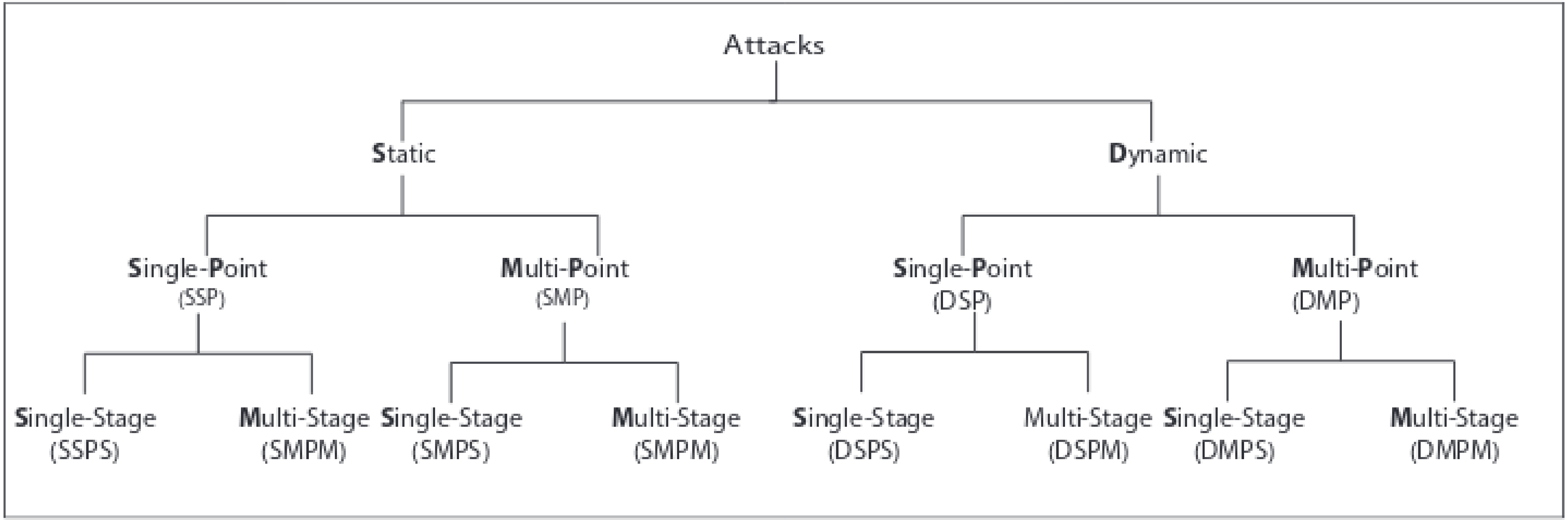
Petro chemical plant

Discovery of Stuxnet

Ukraine power grids

TRITON attack

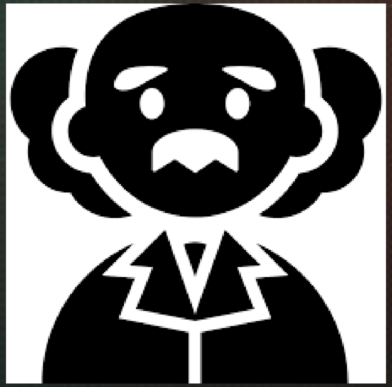
Attacks in ICS

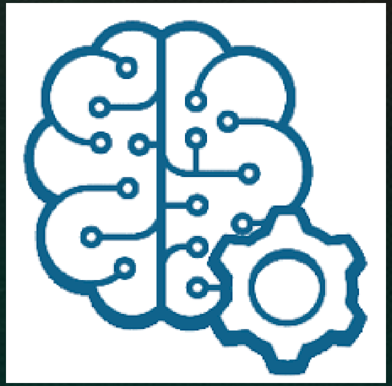


Goh, Jonathan, et al. "A dataset to support research in the design of secure water treatment systems." *International Conference on Critical Information Infrastructures Security*. Springer, Cham, 2016.

Cyber physical defence mechanism

- Anomaly Detection Mechanisms (ADM)
  - Design-based
  - Machine learning-based





Distributed Attack Detection (DAD)

- Design based ADM
- Uses invariants obtained from plant design
- Invariants cannot be compromised
- Attacks: 56 , Detected: 45

EFFECTIVENESS OF DAD IN DETECTING ATTACKS

Experiments	Attack Type	Attacks	Detected
Exp-A	SS	10	10
	SM	5	5
	DS	3	5
	DM	2	2
	Total	**20**	**20**
Exp-I	SS	11	9
	SM	1	1
	SS: Physical	1	1
	DoS (HMI)	3	0
	DoS (SCADA)	1	0
	DoS (PLC-HMI)	1	0
	Total	**18**	**11**
Exp-S	S1 (SS)	4	0
	S2 (SS)	13	13
	Total	**17**	**13**
Exp-DoS	DoS (PLC)	1	1
	Total	**1**	**1**

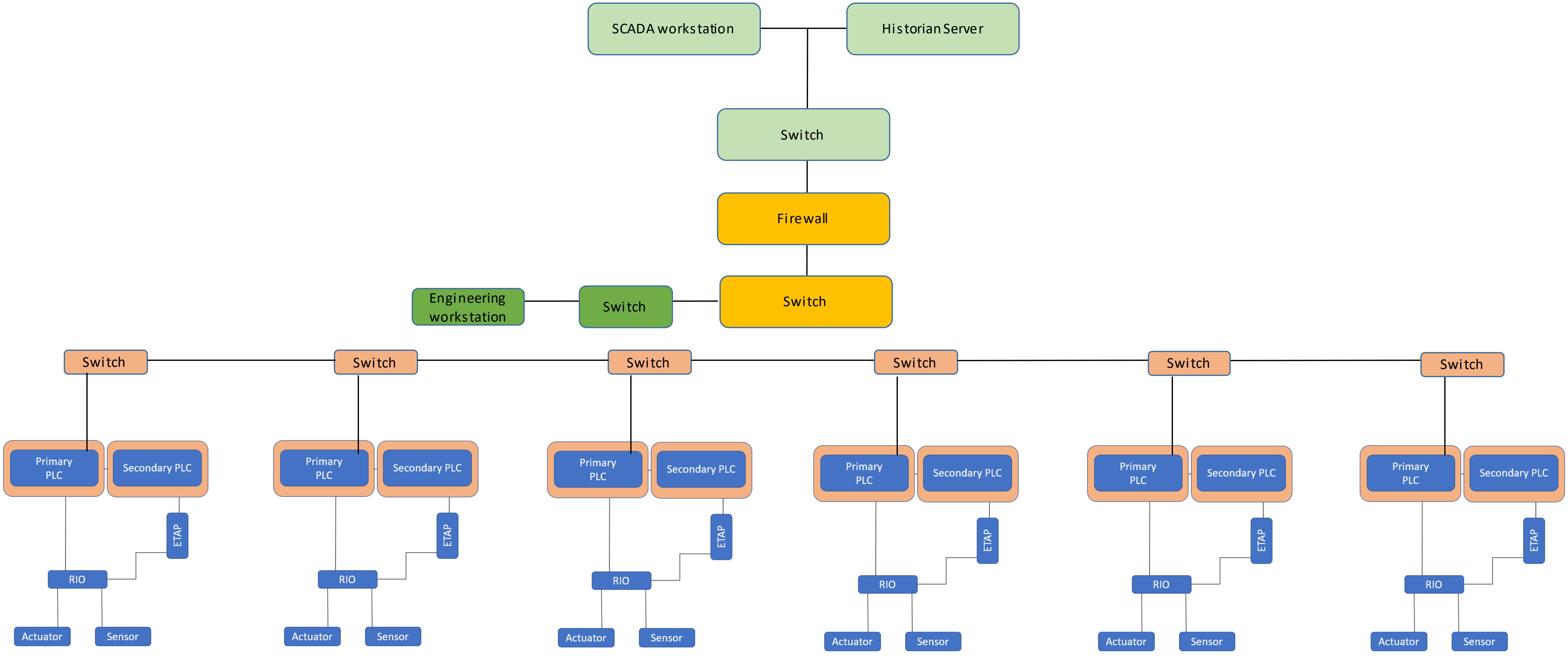
Sridhar Adepu, and Aditya Mathur. "Distributed detection of single-stage multipoint cyber attacks in a water treatment plant." *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*. ACM, 2016.

Sridhar Adepu, and Aditya Mathur. "Distributed Attack Detection in a Water Treatment Plant: Method and Case Study". *IEEE Transactions on Dependable and Secure Computing,2018*

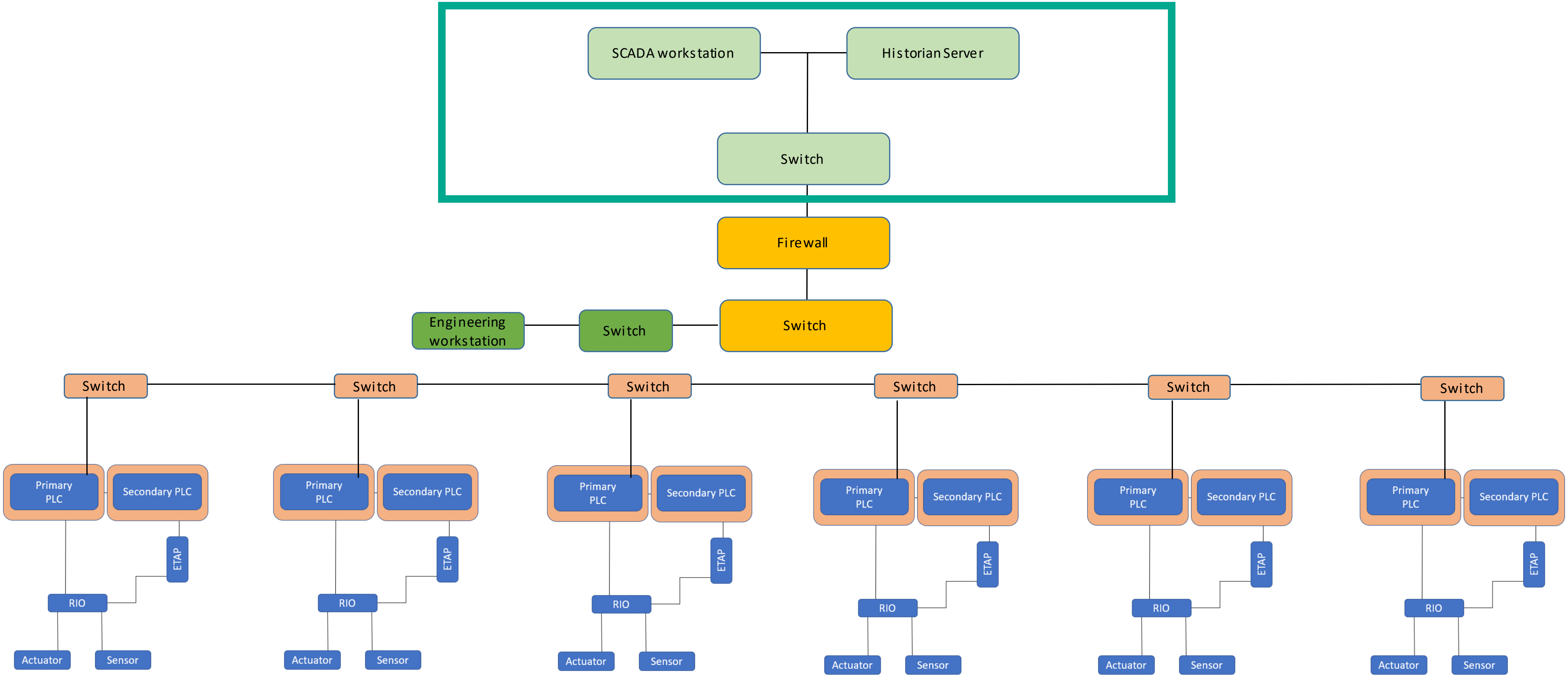
Why is there a need for an

attack tool ?

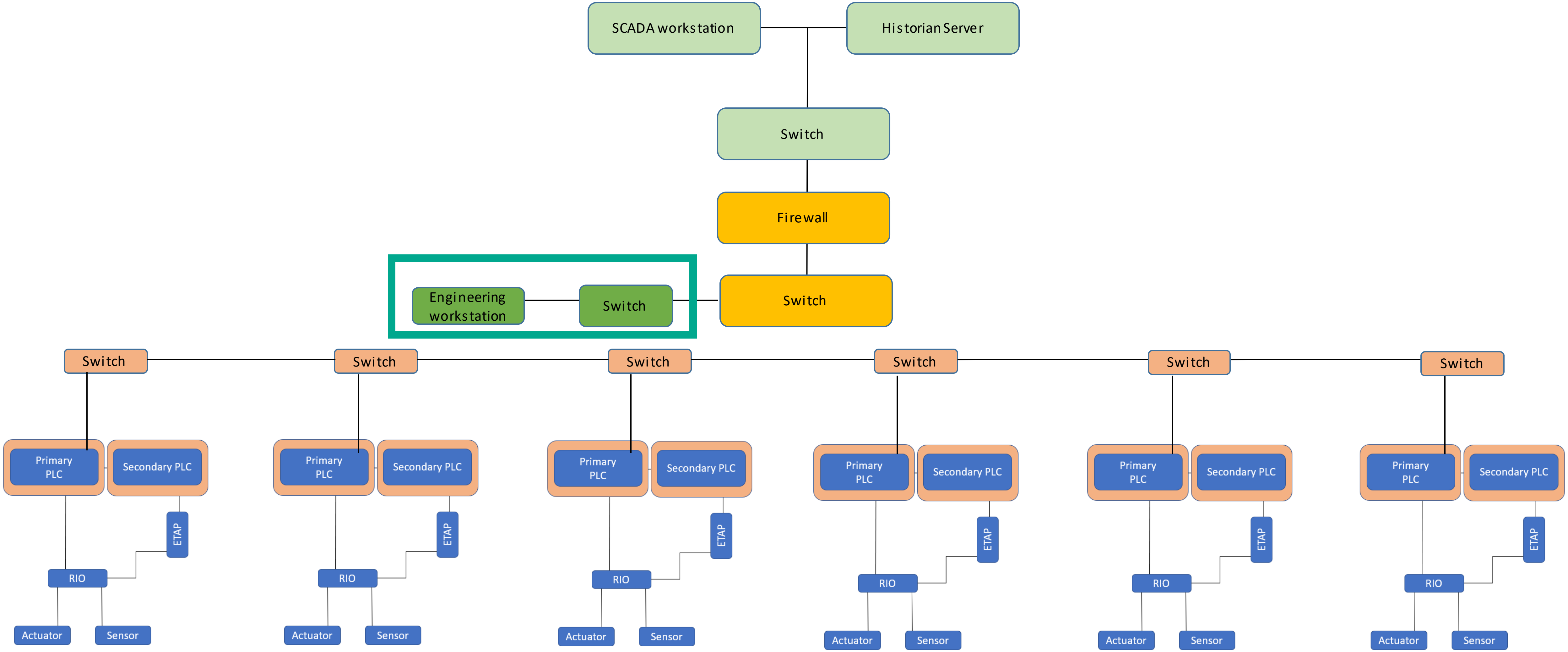
SWaT Network Architecture



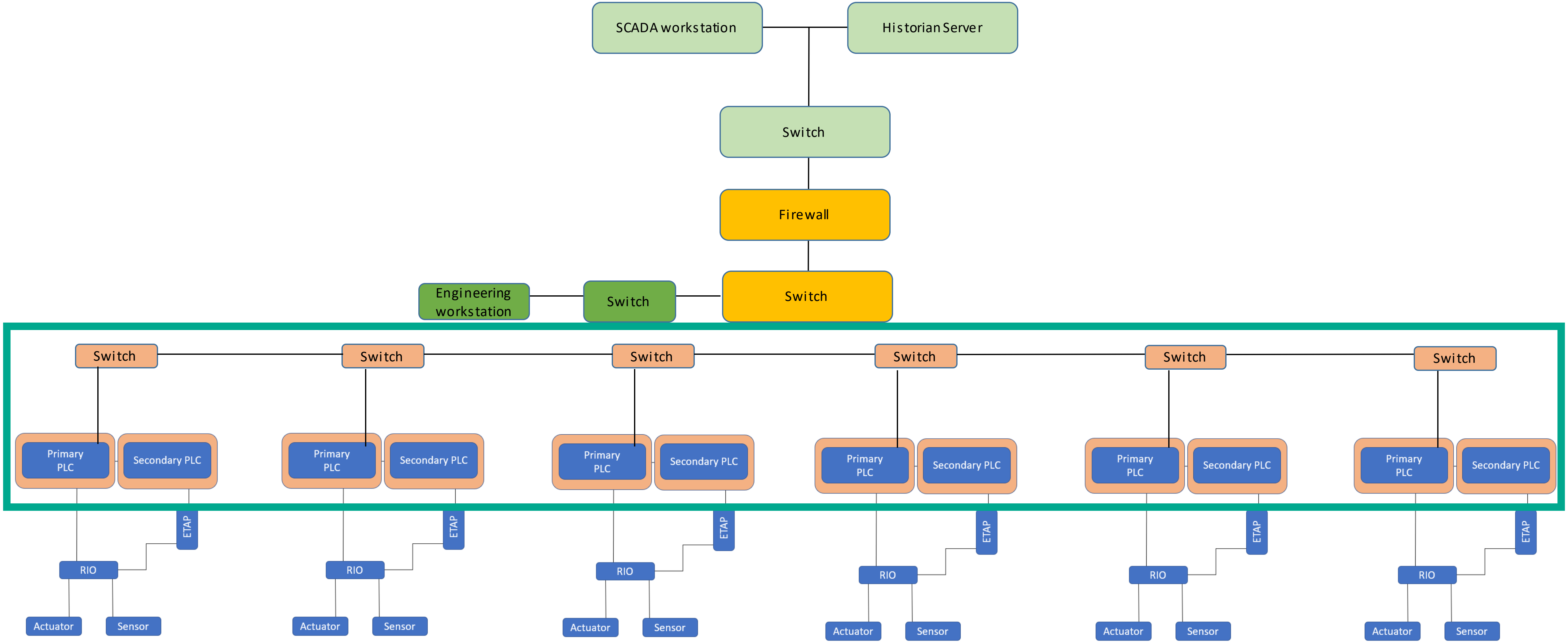
Level 3 – Operation Management



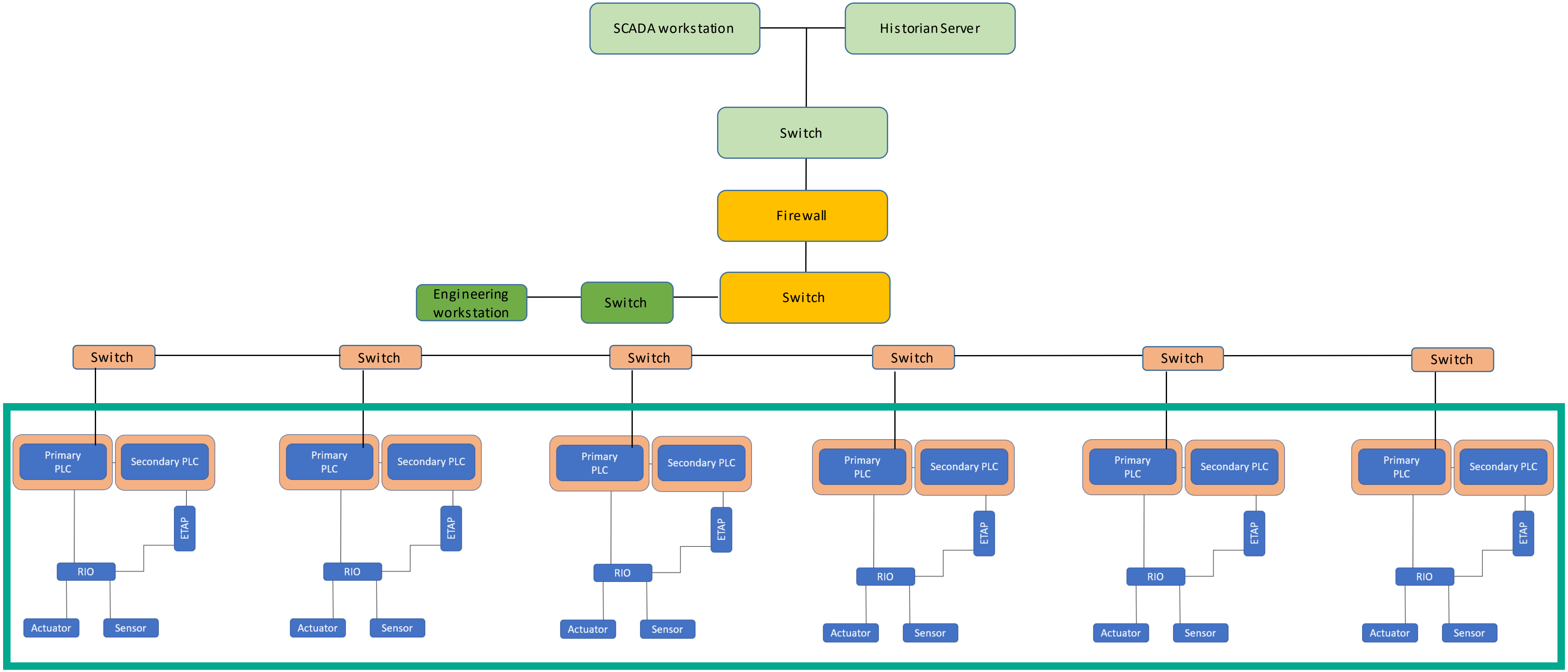
Level 2 – Supervisory Control

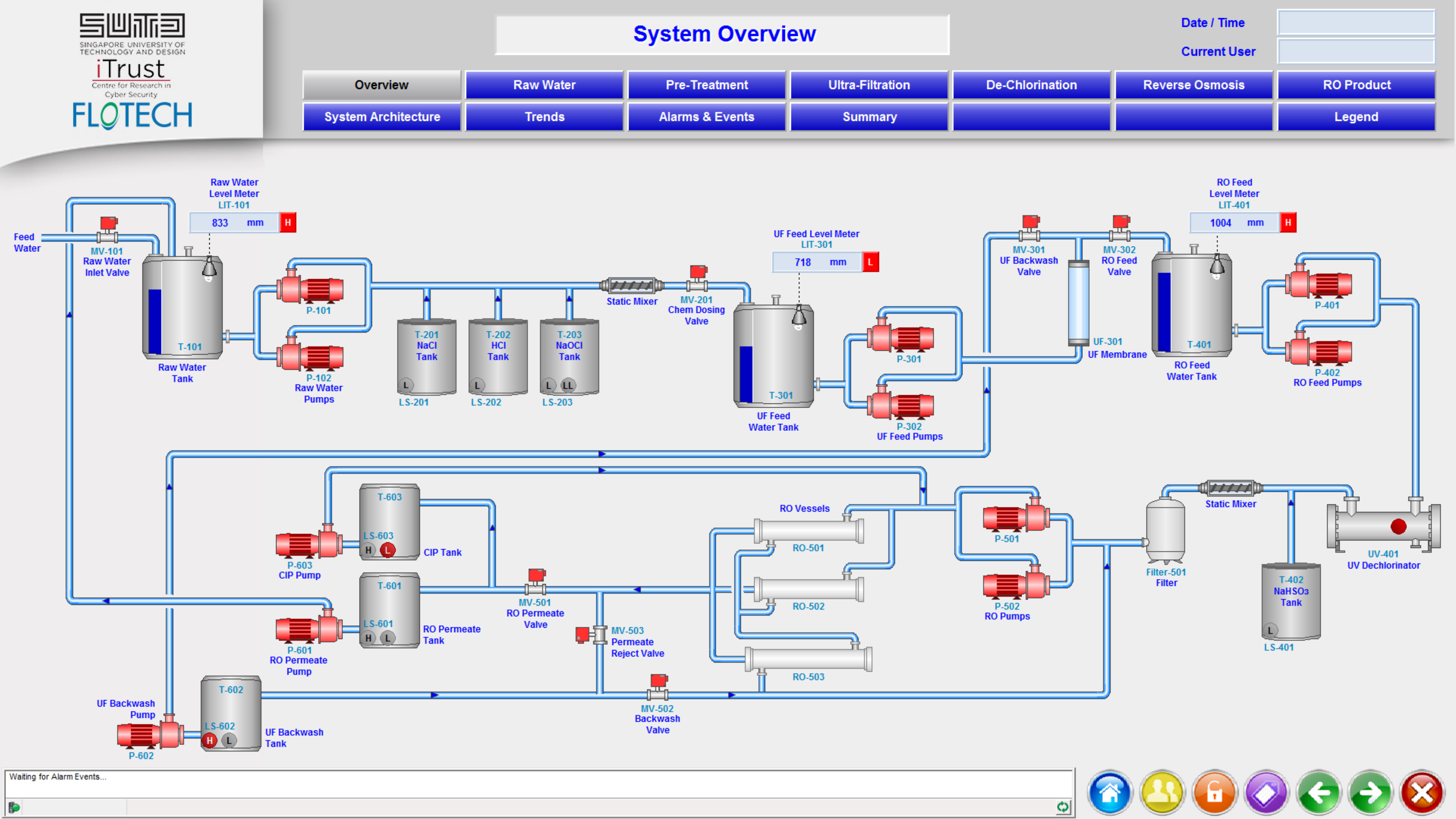


Level 1 – Plant control network

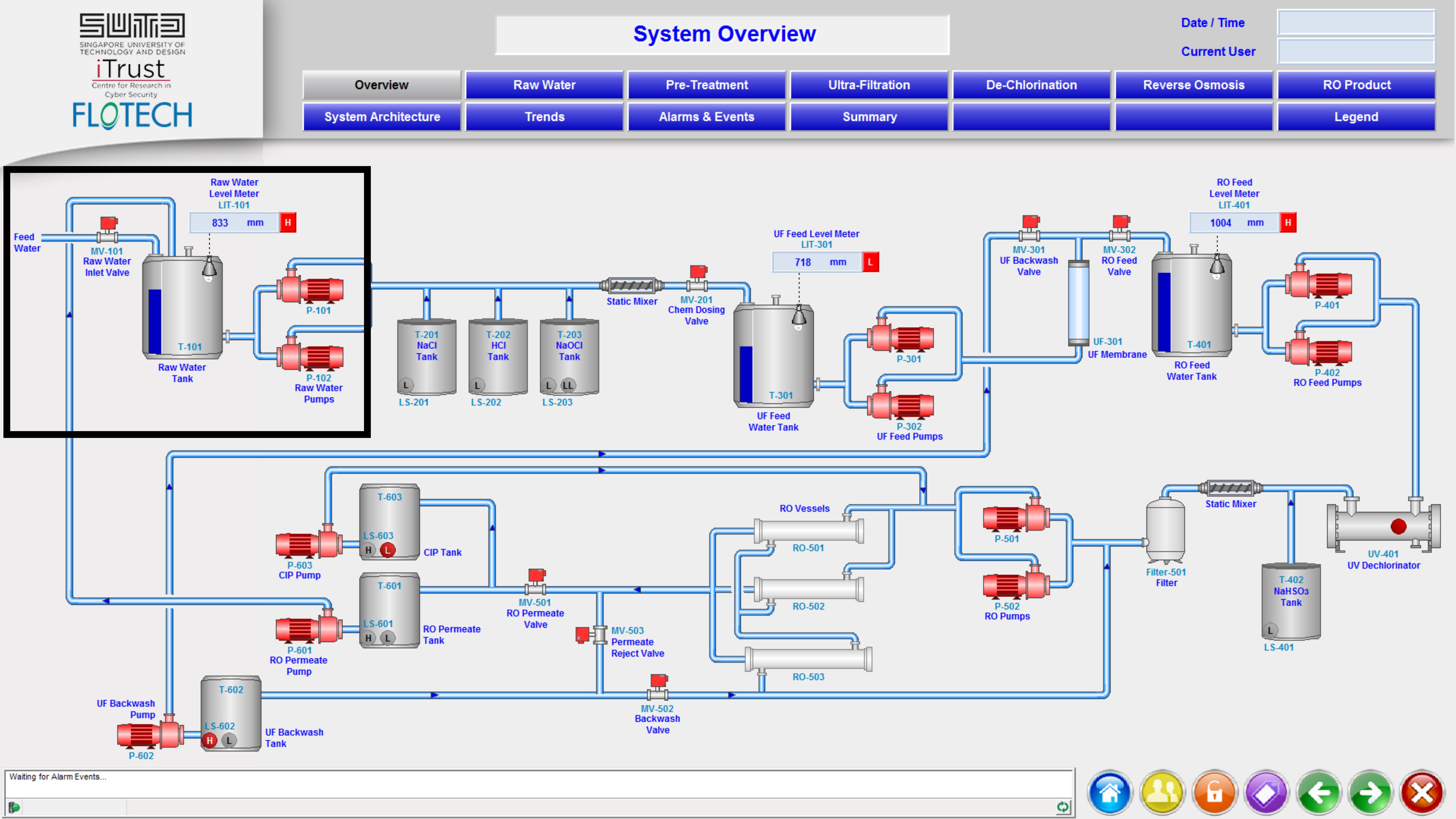


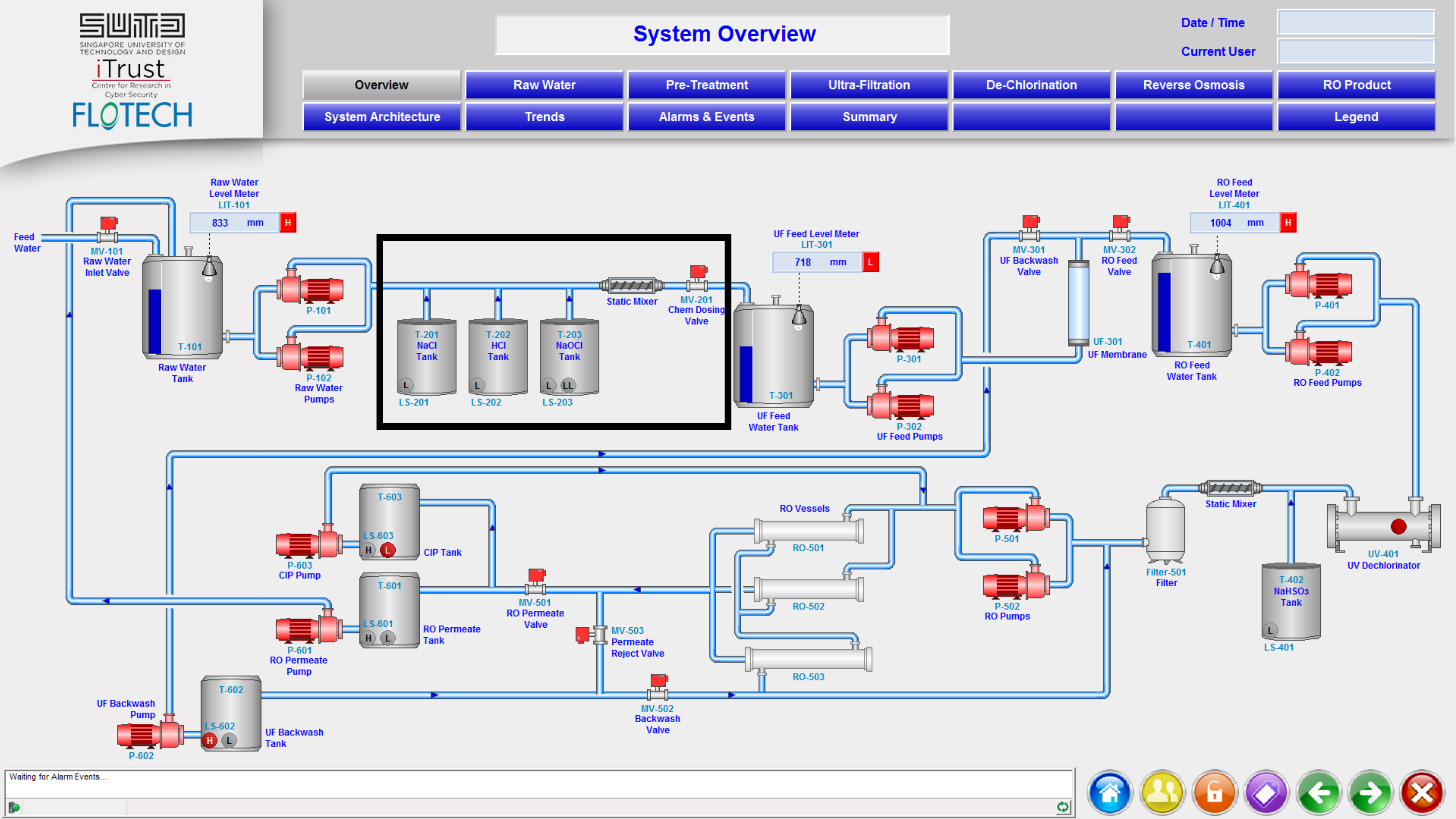
Level 0 - Process

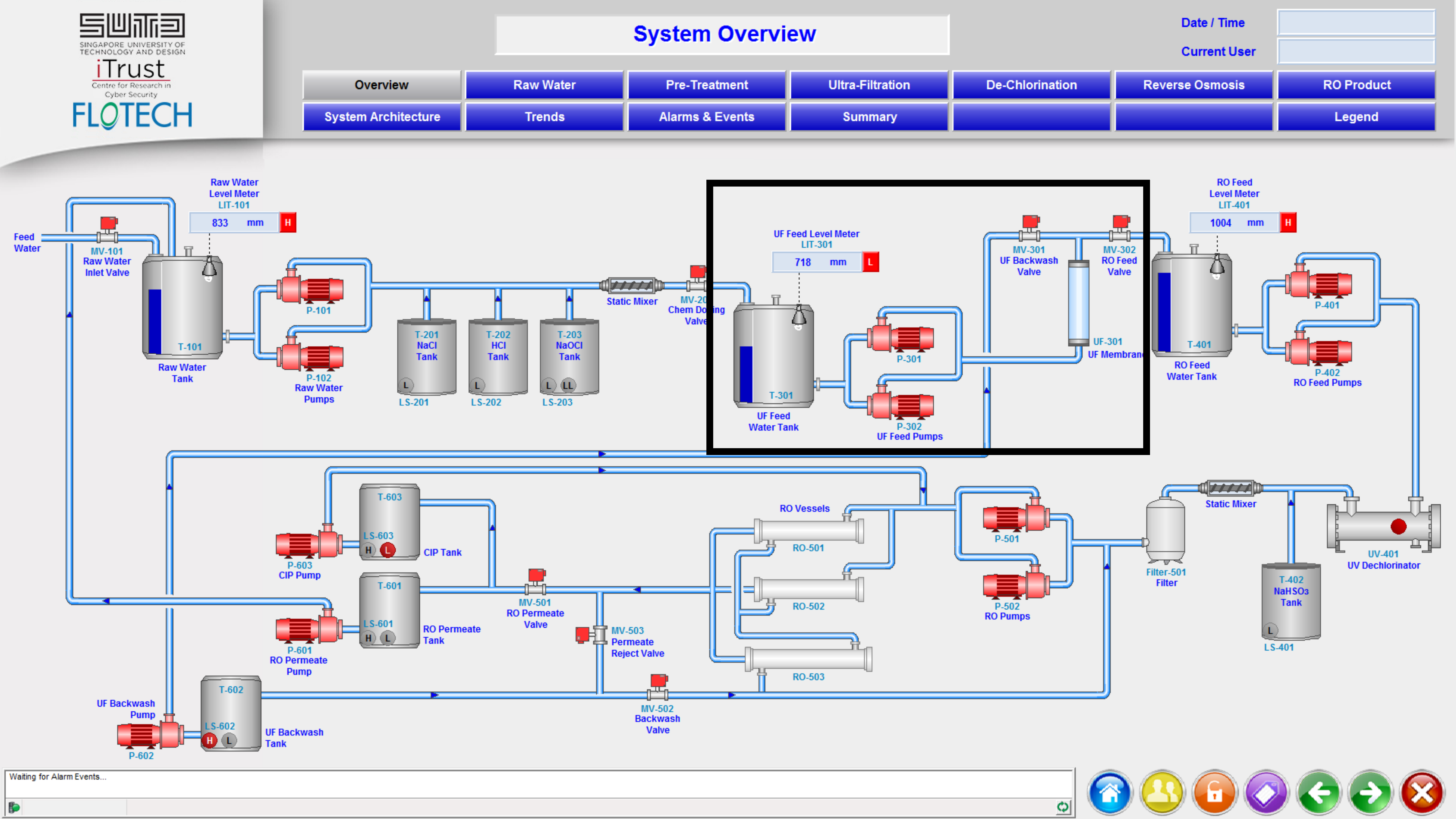




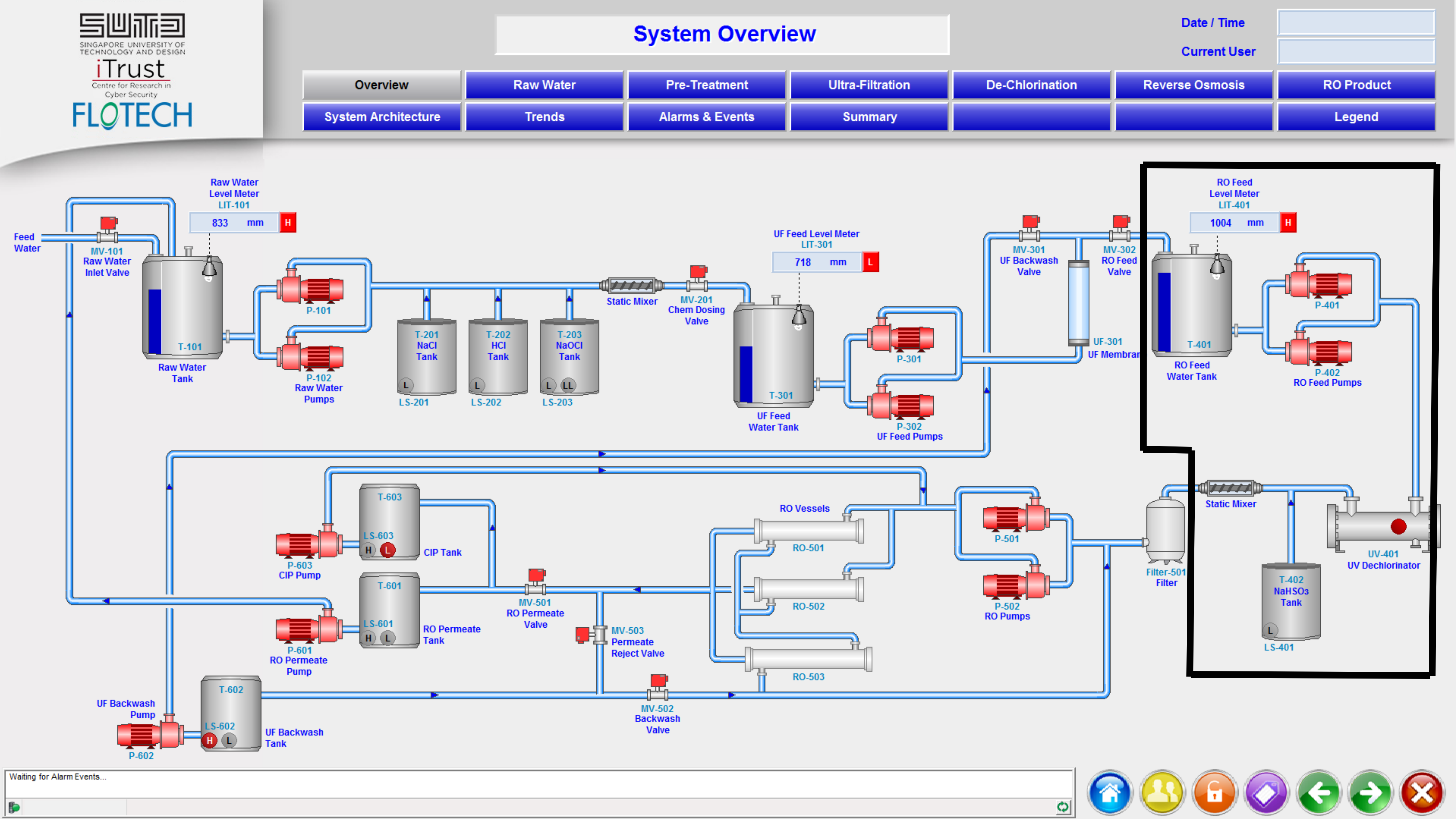
SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN
iTrust
Centre for Research in Cyber Security
FLOTECH
System Overview
Date / Time
Current User
Overview
Raw Water
Pre-Treatment
Ultra-Filtration
De-Chlorination
Reverse Osmosis
RO Product
System Architecture
Trends
Alarms & Events
Summary
Legend
Feed Water
MV-101 Raw Water Inlet Valve
Raw Water Level Meter LIT-101
833 mm
H
T-101
Raw Water Tank
P-101
P-102 Raw Water Pumps
T-201 NaCl Tank
T-202 HCl Tank
T-203 NaOCl Tank
LS-201
LS-202
LS-203
Static Mixer
MV-201 Chem Dosing Valve
UF Feed Level Meter LIT-301
718 mm
L
T-301
UF Feed Water Tank
P-301
P-302 UF Feed Pumps
MV-301 UF Backwash Valve
MV-302 RO Feed Valve
UF-301 UF Membrane
RO Feed Level Meter LIT-401
1004 mm
H
T-401
RO Feed Water Tank
P-401
P-402 RO Feed Pumps
T-603
LS-603
CIP Tank
P-603 CIP Pump
RO Vessels
RO-501
RO-502
RO-503
P-501
P-502 RO Pumps
Static Mixer
Filter-501 Filter
UV-401 UV Dechlorinator
T-402 NaHSO3 Tank
LS-401
T-601
LS-601
RO Permeate Tank
P-601 RO Permeate Pump
MV-501 RO Permeate Valve
MV-503 Permeate Reject Valve
T-602
LS-602
UF Backwash Tank
UF Backwash Pump
P-602
MV-502 Backwash Valve
Waiting for Alarm Events...

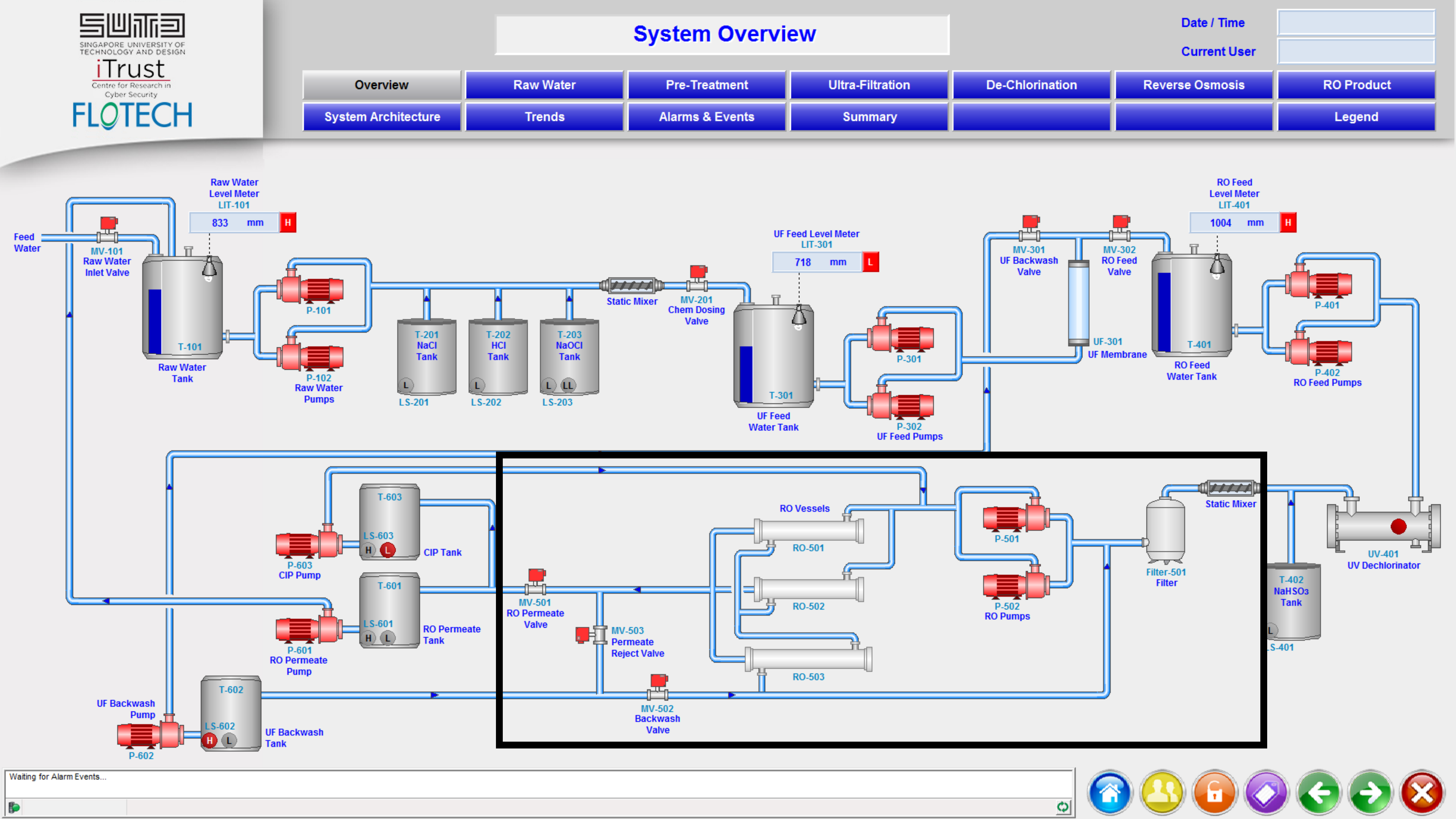

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN
iTrust
Centre for Research in Cyber Security
FLOTECH
System Overview
Date / Time
Current User
Overview
Raw Water
Pre-Treatment
Ultra-Filtration
De-Chlorination
Reverse Osmosis
RO Product
System Architecture
Trends
Alarms & Events
Summary
Legend
Raw Water Level Meter LIT-101
833 mm H
Feed Water
MV-101 Raw Water Inlet Valve
T-101
Raw Water Tank
P-101
P-102 Raw Water Pumps
T-201 NaCl Tank
T-202 HCl Tank
T-203 NaOCl Tank
LS-201
LS-202
LS-203
Static Mixer
MV-201 Chem Dosing Valve
UF Feed Level Meter LIT-301
718 mm L
T-301
UF Feed Water Tank
P-301
P-302 UF Feed Pumps
MV-301 UF Backwash Valve
MV-302 RO Feed Valve
UF-301 UF Membrane
RO Feed Level Meter LIT-401
1004 mm H
T-401
RO Feed Water Tank
P-401
P-402 RO Feed Pumps
T-603
LS-603
CIP Tank
P-603 CIP Pump
T-601
LS-601
RO Permeate Tank
P-601 RO Permeate Pump
MV-501 RO Permeate Valve
MV-503 Permeate Reject Valve
RO Vessels
RO-501
RO-502
RO-503
P-501
P-502 RO Pumps
Filter-501 Filter
Static Mixer
T-402 NaHSO3 Tank
LS-401
UV-401 UV Dechlorinator
T-602
LS-602
UF Backwash Pump
P-602
UF Backwash Tank
MV-502 Backwash Valve
Waiting for Alarm Events...

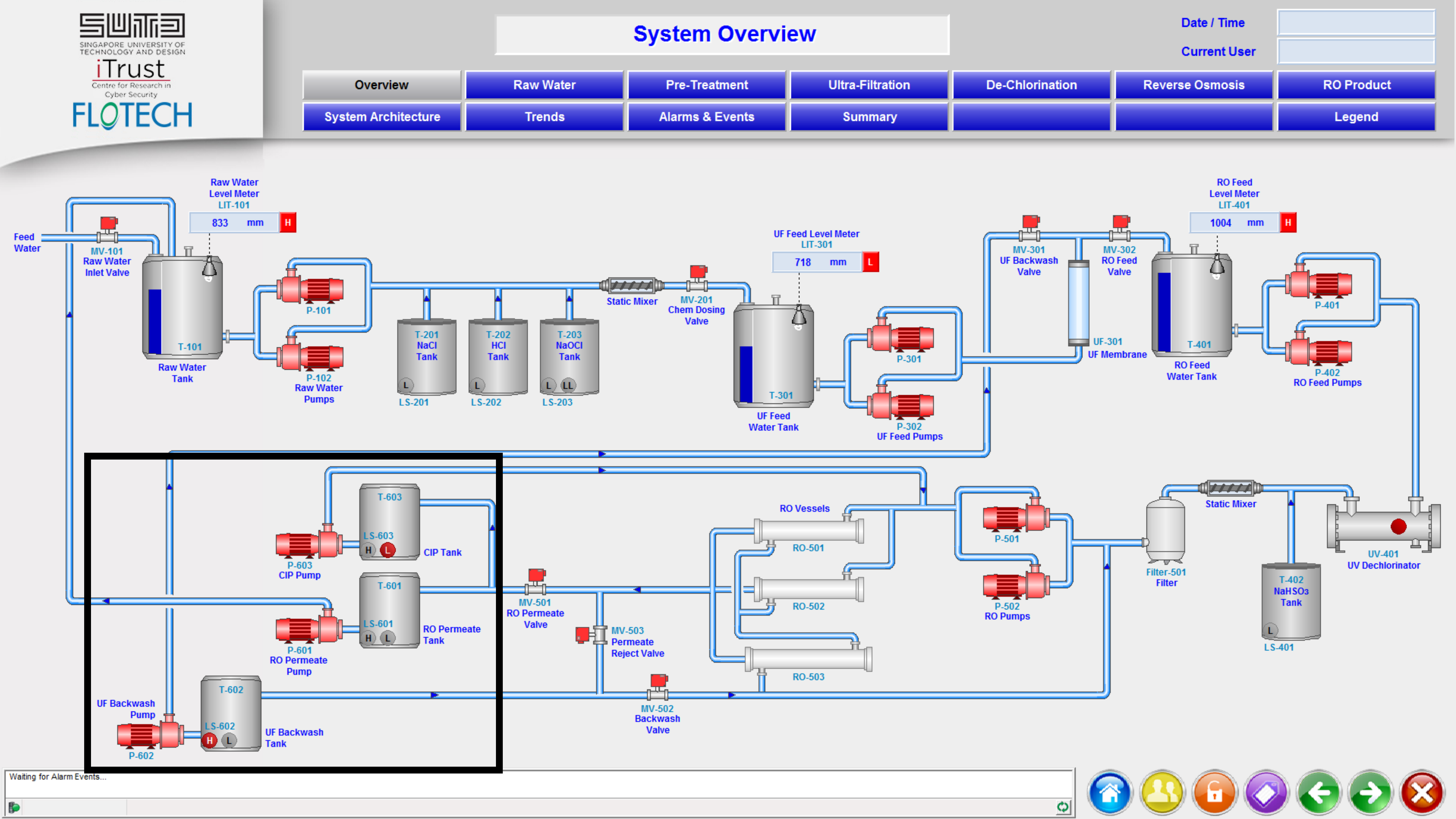

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN
iTrust
Centre for Research in Cyber Security
FLOTECH
System Overview
Date / Time
Current User
Overview
Raw Water
Pre-Treatment
Ultra-Filtration
De-Chlorination
Reverse Osmosis
RO Product
System Architecture
Trends
Alarms & Events
Summary
Legend
Feed Water
MV-101 Raw Water Inlet Valve
Raw Water Level Meter LIT-101
833 mm
H
T-101
Raw Water Tank
P-101
P-102
Raw Water Pumps
T-201 NaCl Tank
T-202 HCl Tank
T-203 NaOCl Tank
LS-201
LS-202
LS-203
Static Mixer
MV-201 Chem Dosing Valve
UF Feed Level Meter LIT-301
718 mm
L
T-301
UF Feed Water Tank
P-301
P-302
UF Feed Pumps
MV-301 UF Backwash Valve
MV-302 RO Feed Valve
UF-301
UF Membrane
RO Feed Level Meter LIT-401
1004 mm
H
T-401
RO Feed Water Tank
P-401
P-402
RO Feed Pumps
T-603
LS-603
CIP Tank
P-603 CIP Pump
T-601
LS-601
RO Permeate Tank
P-601 RO Permeate Pump
MV-501 RO Permeate Valve
MV-503 Permeate Reject Valve
RO Vessels
RO-501
RO-502
RO-503
P-501
P-502
RO Pumps
Static Mixer
Filter-501 Filter
T-402 NaHSO3 Tank
LS-401
UV-401 UV Dechlorinator
UF Backwash Pump
P-602
T-602
LS-602
UF Backwash Tank
MV-502 Backwash Valve
Waiting for Alarm Events...



SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN
iTrust
Centre for Research in Cyber Security
FLOTECH
System Overview
Date / Time
Current User
Overview
Raw Water
Pre-Treatment
Ultra-Filtration
De-Chlorination
Reverse Osmosis
RO Product
System Architecture
Trends
Alarms & Events
Summary
Legend
Feed Water
MV-101 Raw Water Inlet Valve
Raw Water Level Meter LIT-101
833 mm H
T-101
Raw Water Tank
P-101
P-102 Raw Water Pumps
T-201 NaCl Tank
T-202 HCl Tank
T-203 NaOCl Tank
LS-201
LS-202
LS-203
Static Mixer
MV-20
Chem Do ing
Valve
UF Feed Level Meter LIT-301
718 mm L
T-301
UF Feed Water Tank
P-301
P-302 UF Feed Pumps
MV-301 UF Backwash Valve
MV-302 RO Feed Valve
UF-301
UF Membran
RO Feed Level Meter LIT-401
1004 mm H
T-401
RO Feed Water Tank
P-401
P-402 RO Feed Pumps
T-603
LS-603
CIP Tank
P-603 CIP Pump
T-601
LS-601
RO Permeate Tank
P-601 RO Permeate Pump
MV-501 RO Permeate Valve
MV-503 Permeate Reject Valve
RO Vessels
RO-501
RO-502
RO-503
P-501
P-502 RO Pumps
Filter-501 Filter
Static Mixer
T-402 NaHSO3 Tank
LS-401
UV-401 UV Dechlorinator
UF Backwash Pump
P-602
T-602
LS-602
UF Backwash Tank
MV-502 Backwash Valve
Waiting for Alarm Events...

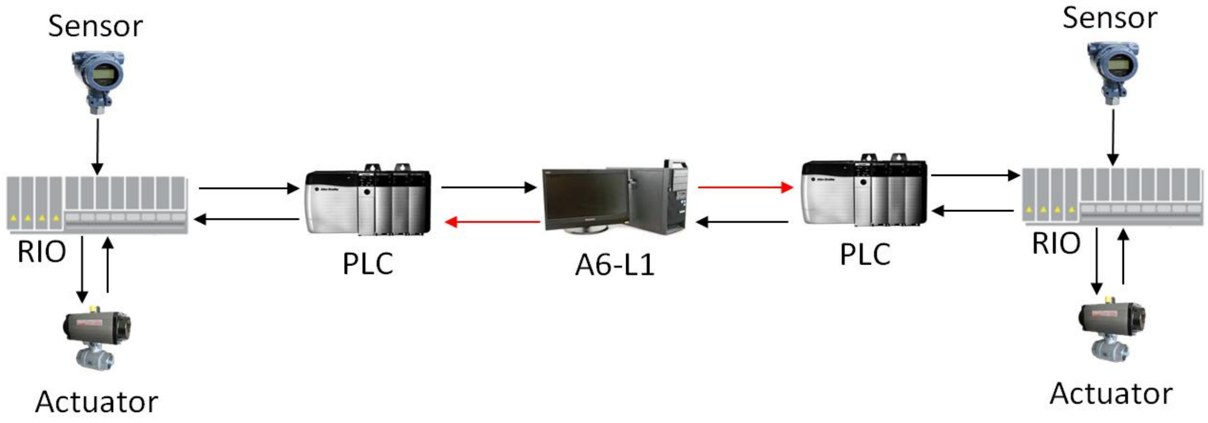

SUTD SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN
iTrust Centre for Research in Cyber Security
FLOTECH
System Overview
Date / Time
Current User
Overview
Raw Water
Pre-Treatment
Ultra-Filtration
De-Chlorination
Reverse Osmosis
RO Product
System Architecture
Trends
Alarms & Events
Summary
Legend
Feed Water
MV-101 Raw Water Inlet Valve
Raw Water Level Meter LIT-101
833 mm H
T-101
Raw Water Tank
P-101
P-102 Raw Water Pumps
T-201 NaCl Tank
T-202 HCl Tank
T-203 NaOCl Tank
LS-201
LS-202
LS-203
Static Mixer
MV-201 Chem Dosing Valve
UF Feed Level Meter LIT-301
718 mm L
T-301
UF Feed Water Tank
P-301
P-302 UF Feed Pumps
MV-301 UF Backwash Valve
MV-302 RO Feed Valve
UF-301 UF Membran
RO Feed Level Meter LIT-401
1004 mm H
T-401
RO Feed Water Tank
P-401
P-402 RO Feed Pumps
Static Mixer
T-402 NaHSO3 Tank
LS-401
UV-401 UV Dechlorinator
Filter-501 Filter
P-501
P-502 RO Pumps
RO Vessels
RO-501
RO-502
RO-503
T-603
LS-603
CIP Tank
P-603 CIP Pump
T-601
LS-601
RO Permeate Tank
P-601 RO Permeate Pump
MV-501 RO Permeate Valve
MV-503 Permeate Reject Valve
T-602
LS-602
UF Backwash Tank
UF Backwash Pump
P-602
MV-502 Backwash Valve
Waiting for Alarm Events...


SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN
iTrust
Centre for Research in Cyber Security
FLOTECH
System Overview
Date / Time
Current User
Overview
Raw Water
Pre-Treatment
Ultra-Filtration
De-Chlorination
Reverse Osmosis
RO Product
System Architecture
Trends
Alarms & Events
Summary
Legend
Feed Water
MV-101 Raw Water Inlet Valve
Raw Water Level Meter LIT-101
833 mm
H
T-101
Raw Water Tank
P-101
P-102
Raw Water Pumps
T-201 NaCl Tank
T-202 HCl Tank
T-203 NaOCl Tank
LS-201
LS-202
LS-203
Static Mixer
MV-201 Chem Dosing Valve
UF Feed Level Meter LIT-301
718 mm
L
T-301
UF Feed Water Tank
P-301
P-302
UF Feed Pumps
MV-301 UF Backwash Valve
MV-302 RO Feed Valve
UF-301
UF Membrane
RO Feed Level Meter LIT-401
1004 mm
H
T-401
RO Feed Water Tank
P-401
P-402
RO Feed Pumps
T-603
LS-603
CIP Tank
P-603
CIP Pump
T-601
LS-601
RO Permeate Tank
P-601
RO Permeate Pump
T-602
LS-602
UF Backwash Tank
UF Backwash Pump
P-602
MV-501 RO Permeate Valve
MV-503 Permeate Reject Valve
MV-502 Backwash Valve
RO Vessels
RO-501
RO-502
RO-503
P-501
P-502
RO Pumps
Filter-501 Filter
Static Mixer
T-402 NaHSO3 Tank
LS-401
UV-401
UV Dechlorinator
Waiting for Alarm Events...


SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN
iTrust
Centre for Research in Cyber Security
FLOTECH
System Overview
Date / Time
Current User
Overview
Raw Water
Pre-Treatment
Ultra-Filtration
De-Chlorination
Reverse Osmosis
RO Product
System Architecture
Trends
Alarms & Events
Summary
Legend
Feed Water
MV-101 Raw Water Inlet Valve
Raw Water Level Meter LIT-101
833 mm H
T-101
Raw Water Tank
P-101
P-102
Raw Water Pumps
T-201 NaCl Tank
T-202 HCl Tank
T-203 NaOCl Tank
LS-201
LS-202
LS-203
Static Mixer
MV-201 Chem Dosing Valve
UF Feed Level Meter LIT-301
718 mm L
T-301
UF Feed Water Tank
P-301
P-302
UF Feed Pumps
MV-301 UF Backwash Valve
MV-302 RO Feed Valve
UF-301
UF Membrane
RO Feed Level Meter LIT-401
1004 mm H
T-401
RO Feed Water Tank
P-401
P-402
RO Feed Pumps
T-603
LS-603
CIP Tank
P-603
CIP Pump
T-601
LS-601
RO Permeate Tank
P-601
RO Permeate Pump
T-602
LS-602
UF Backwash Tank
UF Backwash Pump
P-602
MV-501 RO Permeate Valve
MV-503 Permeate Reject Valve
MV-502 Backwash Valve
RO Vessels
RO-501
RO-502
RO-503
P-501
P-502
RO Pumps
Filter-501 Filter
Static Mixer
T-402 NaHSO3 Tank
LS-401
UV-401 UV Dechlorinator
Waiting for Alarm Events...

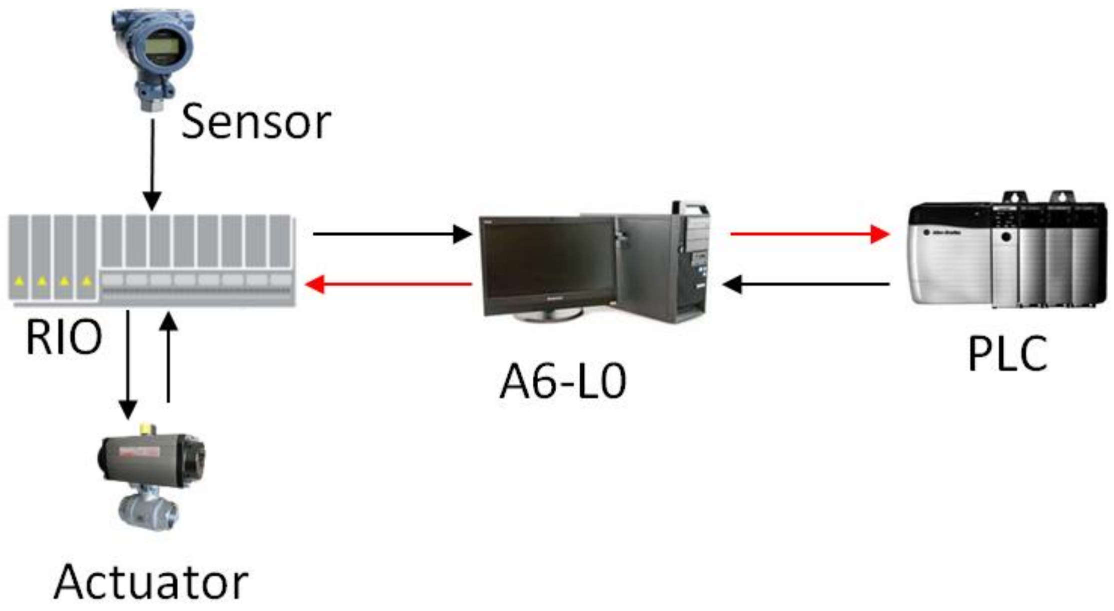
A6 Tool suite tool

A6-L1



A6 Tool suite tool

A6-L0

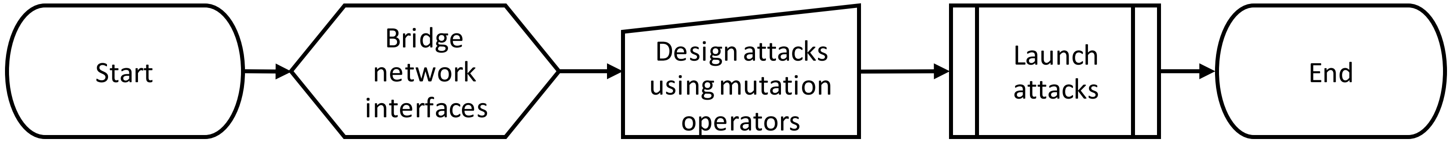


Kaspersky Industrial Cybersecurity Conference 2019

Urbina, David I., et al. "Attacking Fieldbus Communications in ICS: Applications to the SWaT Testbed." *SG-CRC*. 2016.

Attack Design

A6 - L1



A6 – L0

Mutation Operators

Operator	Description	Example
Add Static Delta (ASD)	Adds/subtracts an absolute, unchanging δ to state measurements	ASD(500) ⇒ Before: LIT101=300 After: LIT101=800
Add Limits Delta (ALD)	Adds/subtracts random value between -δ and +δ to state measurements	ALD(10) ⇒ Before: LIT101=300 After: LIT101=307
Add Random Delta (ARD)	Adds/subtracts a random value between δ1 and δ2 to state measurements	ARD(100, 200) ⇒ Before: LIT101=300 After: LIT101=450 ARD(100, 200) ⇒ Before: LIT101=300 After: LIT101=450

Mutation Operators

Operator	Description	Example
Set to Zero	Set state measurement to zero	Before: MV101=1 After: MV101=0
Set to One	Set state measurement to one	Before: P101=0 After: P101=1
Set to Static	Set state measurement to static value	STS(756) ⇒ Before: LIT101=300 After: LIT101=756
Set to Random	Set state measurement to a random value between $\delta 1$ and $\delta 2$	STR(100, 200) ⇒ Before: LIT101=300 After: LIT101=179

Mutation Operators

Operator	Description	Example
Bit Shift Left	State measurement is bit-shifted to left by δ bits	BSL(4) ⇒ Before: LIT101=300 After: LIT101=5982.85
Bit Shift Right	State measurement is bit-shifted to right by δ bits	BSR(4)⇒ Before: LIT101=300 After: LIT101=3356044.00

Command Validators

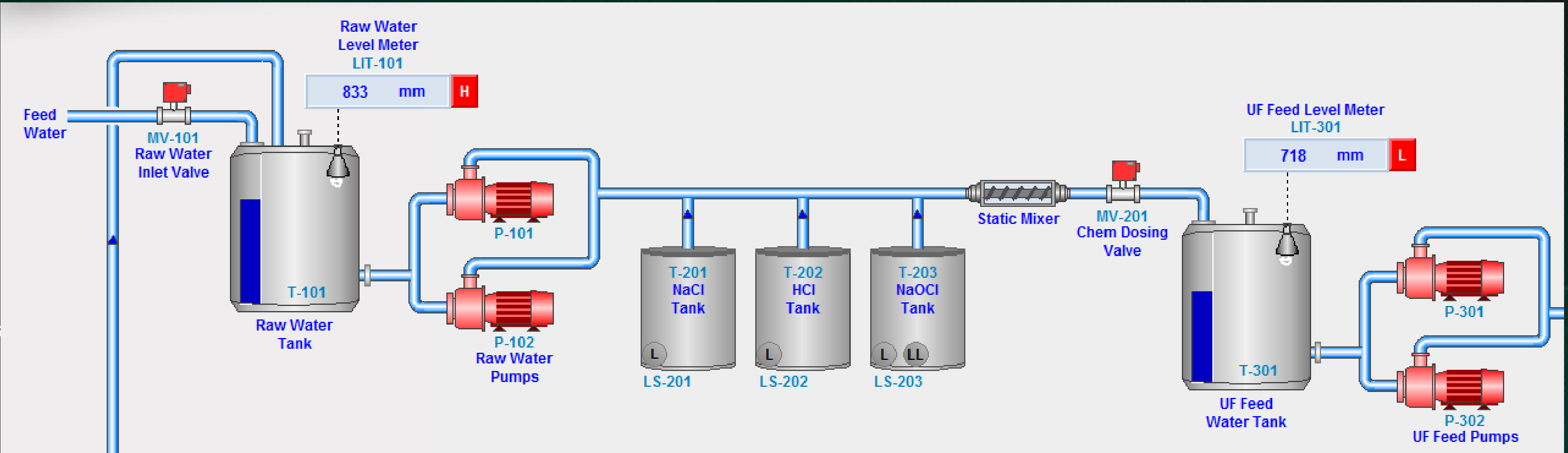
Operator	Description	Example
Valid	Set state measurement to valid input	Before: P101 = 1 (On) After: P101 = 0 (Off)
Invalid	Set state measurement to invalid input	Before: P101 = 0 (Off) After: P101 = -5 (Invalid)

L1 Attack Demo

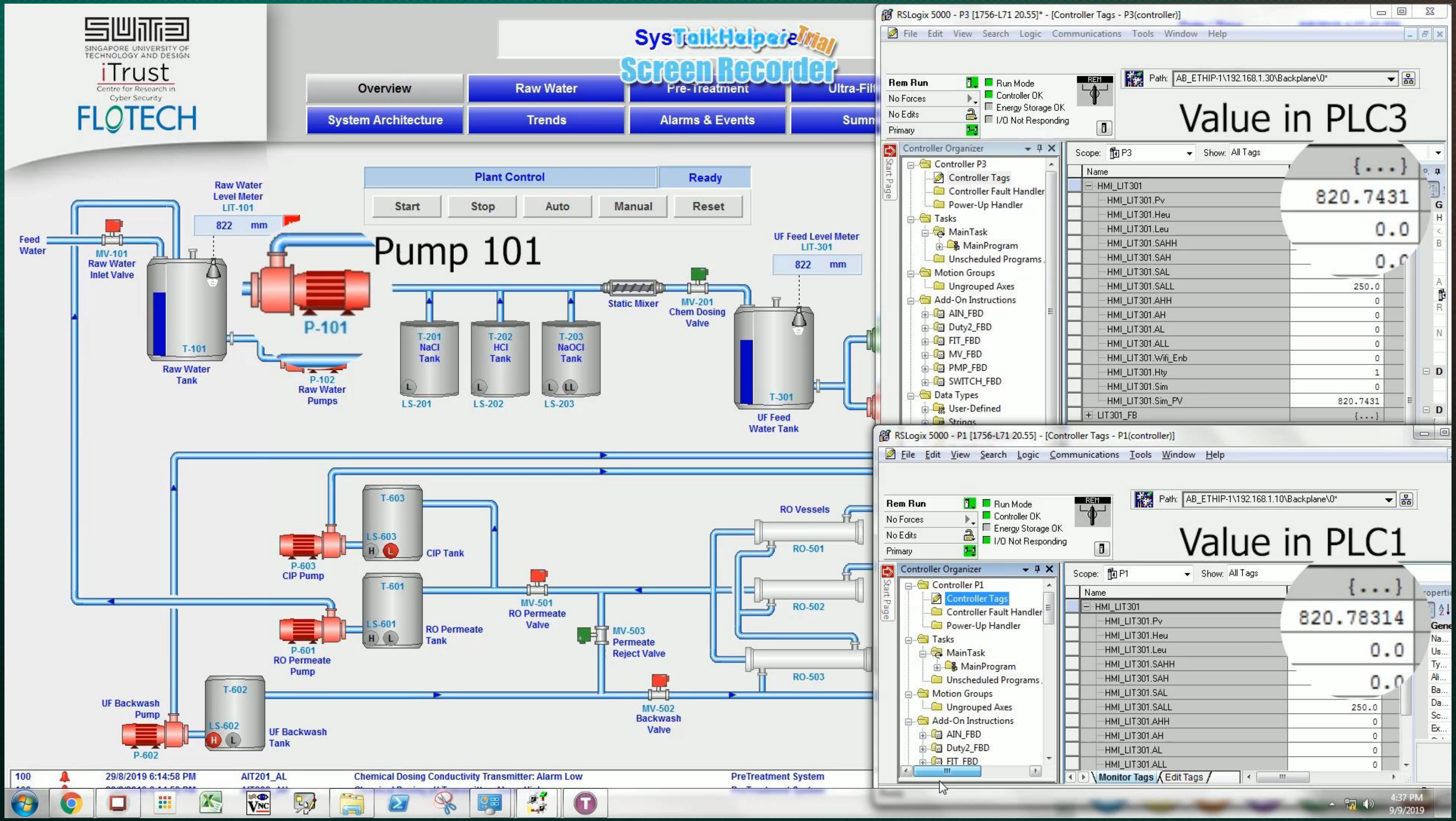
Stage 1 strategy is to have P101 and P102 be interlocked with LIT301

- Low Setpoint: 800mm ⇒ P101/P102 START
- High Setpoint: 1000mm ⇒ P101/P102 STOP

SSPMS Attack: Mutating of LIT301 value to LOW from PLC3 to PLC1



Kaspers



Kaspersky Industrial Cybersecurity Conference 2019

L0 Attack Demo

Stage 1 strategy is to have MV101 be activated by LIT101

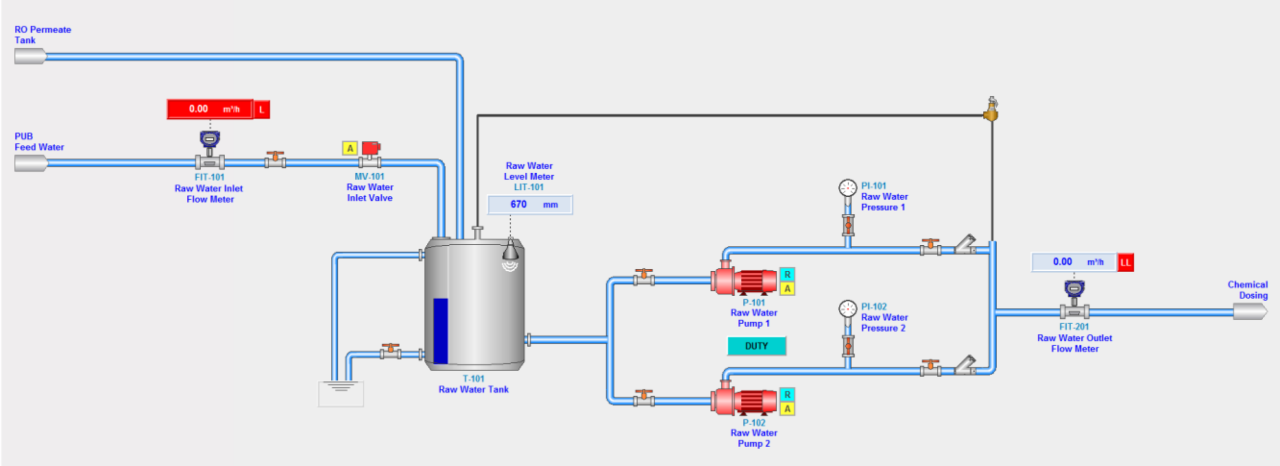
a) Low Low Setpoint: 250mm & P101/P102 STOP AND MV101 OPEN

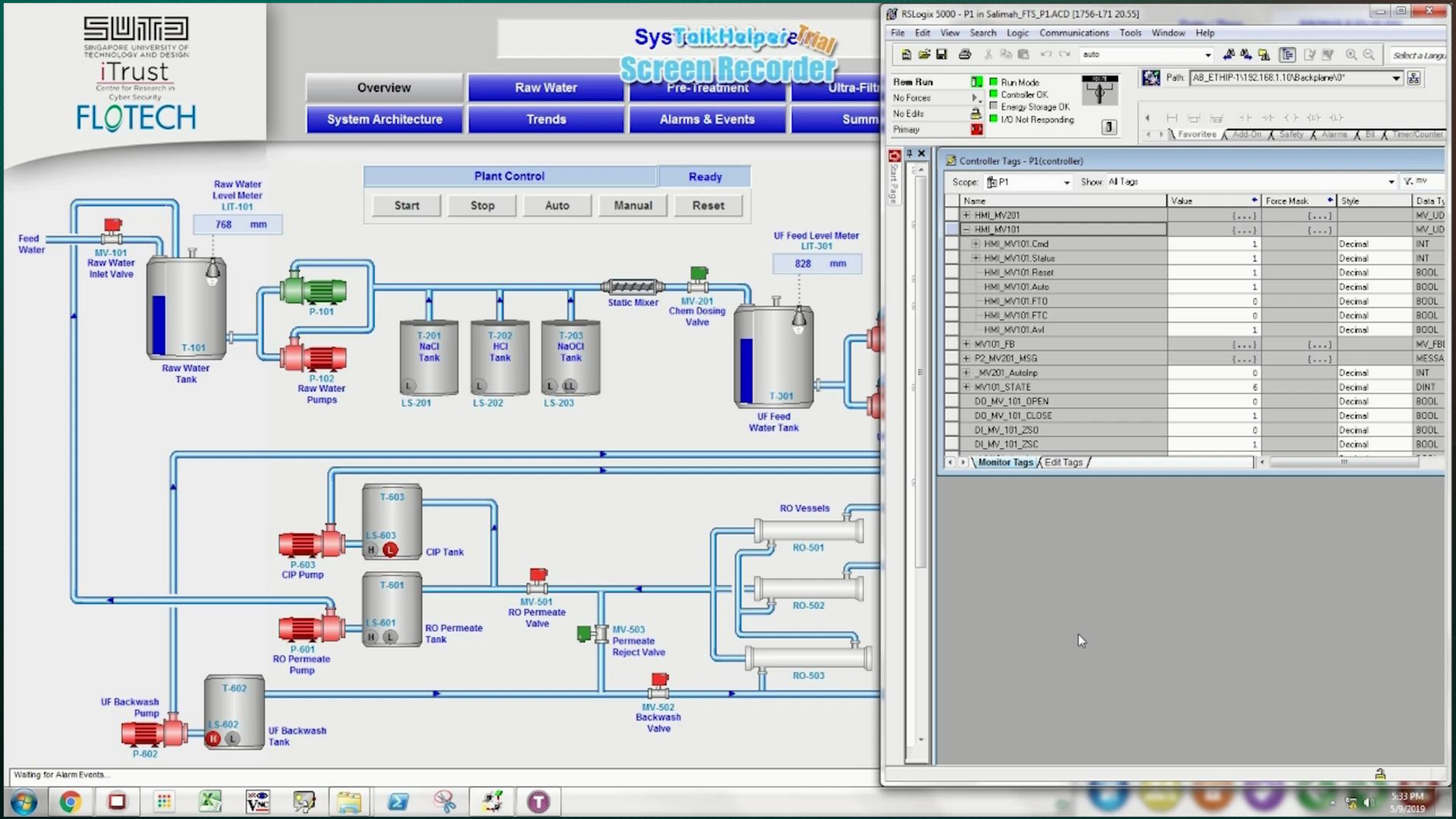
b) Low Setpoint: 500mm MV101 OPEN

c) High Setpoint: 800mm MV101 CLOSE

d) High High Setpoint: 1200mm Alarm

SSSMP Attack: Mutating P101 & MV101 status to PLC1 and command to actuators





Kaspersky Industrial Cybersecurity Conference 2019

Findings

1. Out of range values and commands
2. Corelated Invariants across PLCs
3. False positives

Current Work

1. Automated generation of attacks
2. Creating a test suite for ADMs to be tested against and given a benchmark

Specials thanks to

Sridhar Adepu

Gayathri Sugumar

Nils Ole Tippenhauer

Aditya P. Mathur

Questions?

Francisco Furtado

francisco_dos@sutd.edu.sg

Salimah Liyakkathali

liyakkathali@sutd.edu.sg

Kaspersky Industrial Cybersecurity Conference 2019

September 18-20, 2019, Sochi, Russia

Thank you!

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

iTrust
Centre for Research in Cyber Security