iTrust
Centre for Research in Cyber Security

Briefing to IDS Teams – 16 June 2023

Supported by

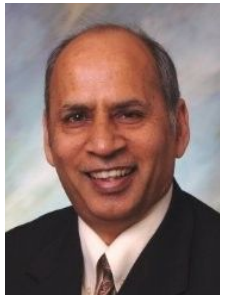
CSA SINGAPORE

National Cybersecurity R&D Laboratory

Ivan Christian
ivan_christian@sutd.edu.sg

CISS 2023 Organising Team

Event Directing


Prof. Aditya MATHUR


Prof. Jianying ZHOU


Col. TAN Shengyang

Judges


ME6 William TEO

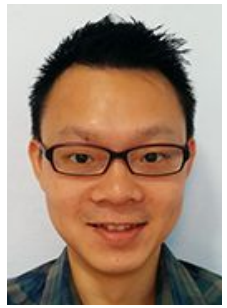

Delaney NG


Matthias YEO


CHONG Rong Hwa

Organising Secretariat


ME4 Benedict TAN


Mark GOH

CISS 2023 Finals Organising Team

Green Team


Francisco FURTADO


Jonathan TAY


Andrew TAY


R Aanand

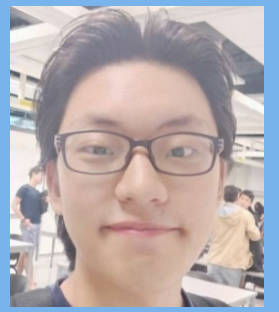
IDS Analysis Team


Ivan CHRISTIAN


Dr. Gauthama RAMAN


Andy TAY


Naga SIVA


ZHOU Wentao

Objectives of CISS 2023

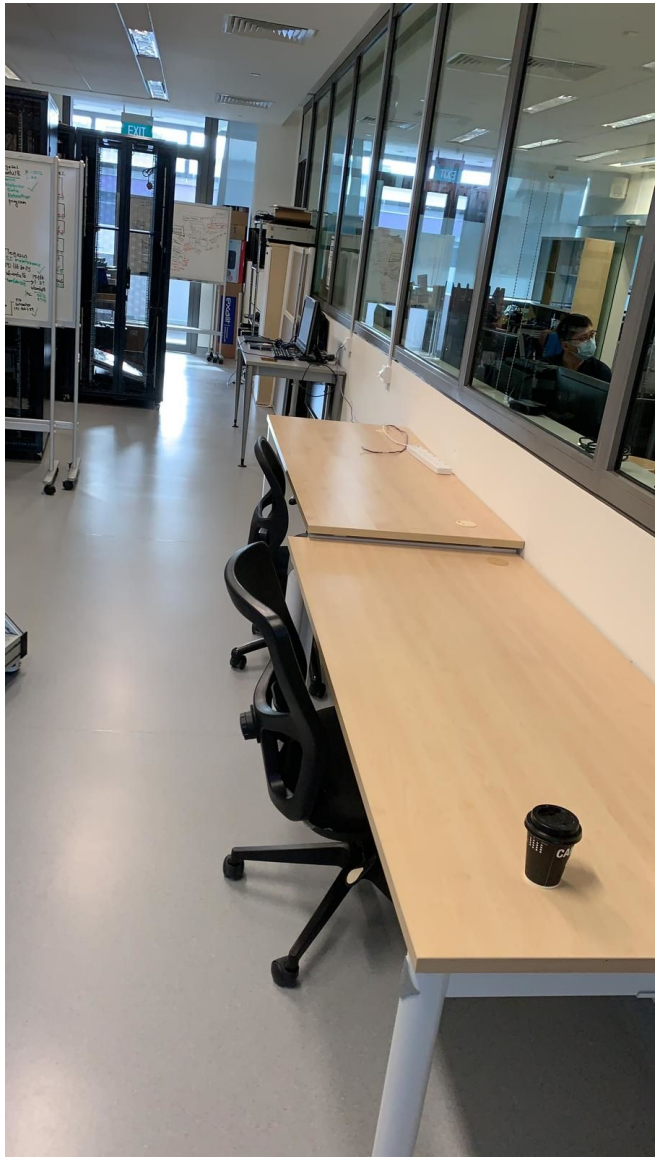
- **Validate and Assess Technologies**
  - Validate and assess the effectiveness of technologies developed by researchers & commercial entities with iTrust
- **Develop capabilities**
  - Develop capabilities for defending critical infrastructure (CI) / cyber-physical systems (CPS) under cyber-attacks
- **Understand TTPs**
  - Understand composite Tactics, Techniques and Procedures (TTPs) for enhanced Operation Security

CISS 2023 IDS Team Timeline

16 Jun	IDS Teams Briefing
19 Jun - 18 Jul	IDS Team Systems Installation
19 - 21 Jul	Active Network Scanning
24 - 28 Jul	Baselining Sessions
18 Aug	Opening ceremony
18, 21 - 24 Aug	Exercise Execution (CISS Finals)
28 Aug	IDS Evaluation by iTrust

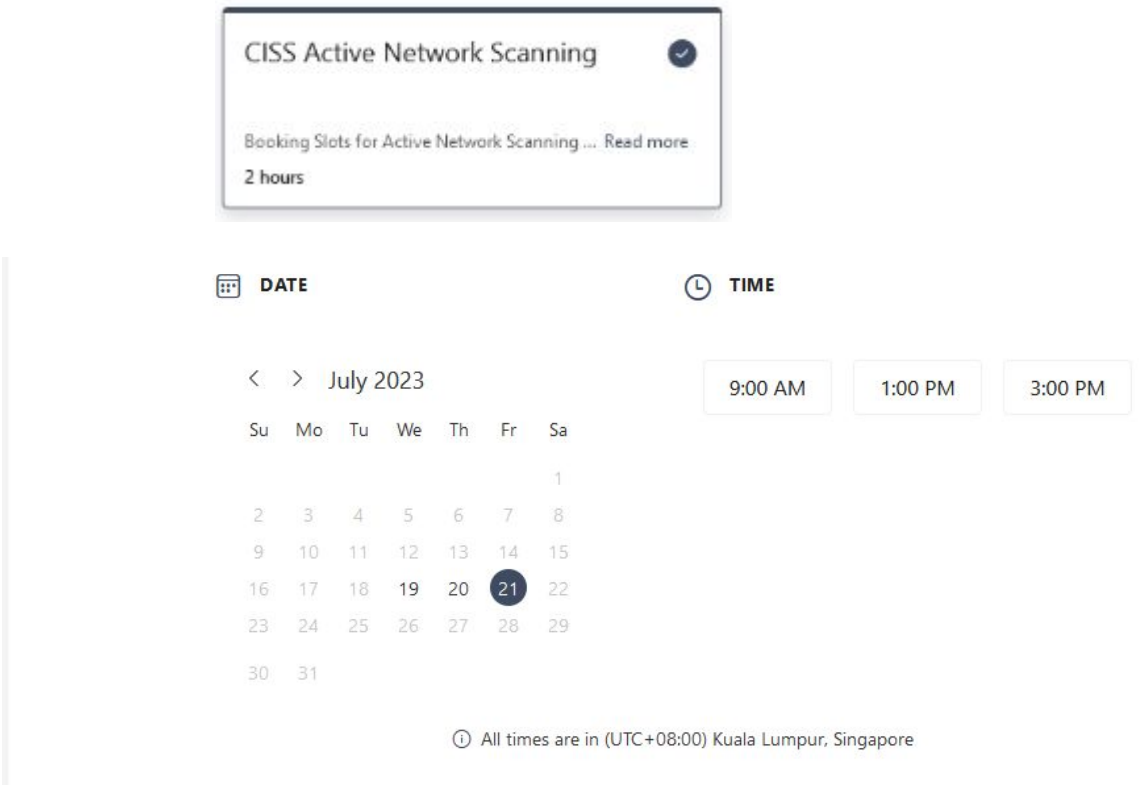
IDS Installation Details

- **Book at most two days to set up your systems at iTrust**
  - 19 June 2023 - 18 July 2023 (excluding holidays)
  - 0900 to 1800
  - Booking Link
- **Deliver systems to iTrust SWaT Lab**
  - Address:
    Building 2, Level 7, Room 14,
    8 Somapah Road,
    Singapore 487372
  - POC: Boon Kiat (81579108)
- **We will provide**
  - Power socket
  - Deduplicated traffic from all testbeds via Ethernet.
  - 1 x RJ45 port from the aggregator
  - Up to 700 Mbps throughput
- **Bring your own**
  - power strips
  - cables
  - SIM device for remote accessible



Active Network Scanning Details

- **Book one session**
  - 19 - 21 July 2023
  - 0900 - 1100, 1300 - 1500, 1500 - 1700
  - Booking Link
- **We will provide**
  - access to the network
  - dedicated slot per vendor
- **Bring your own tools**

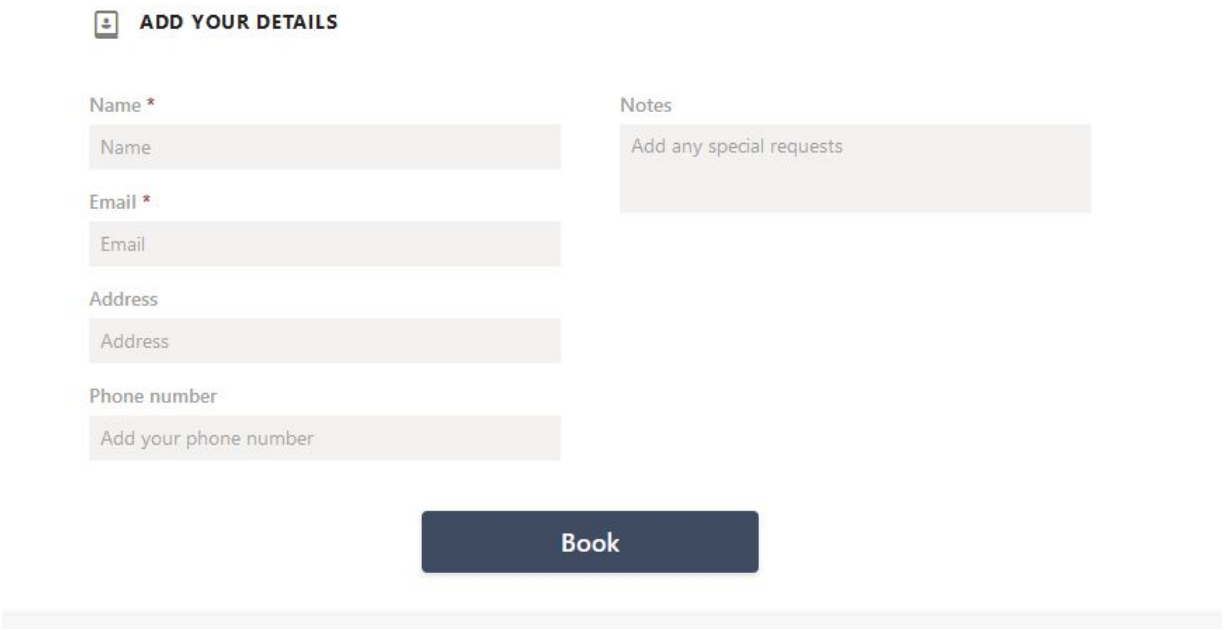


Baselining Sessions Details

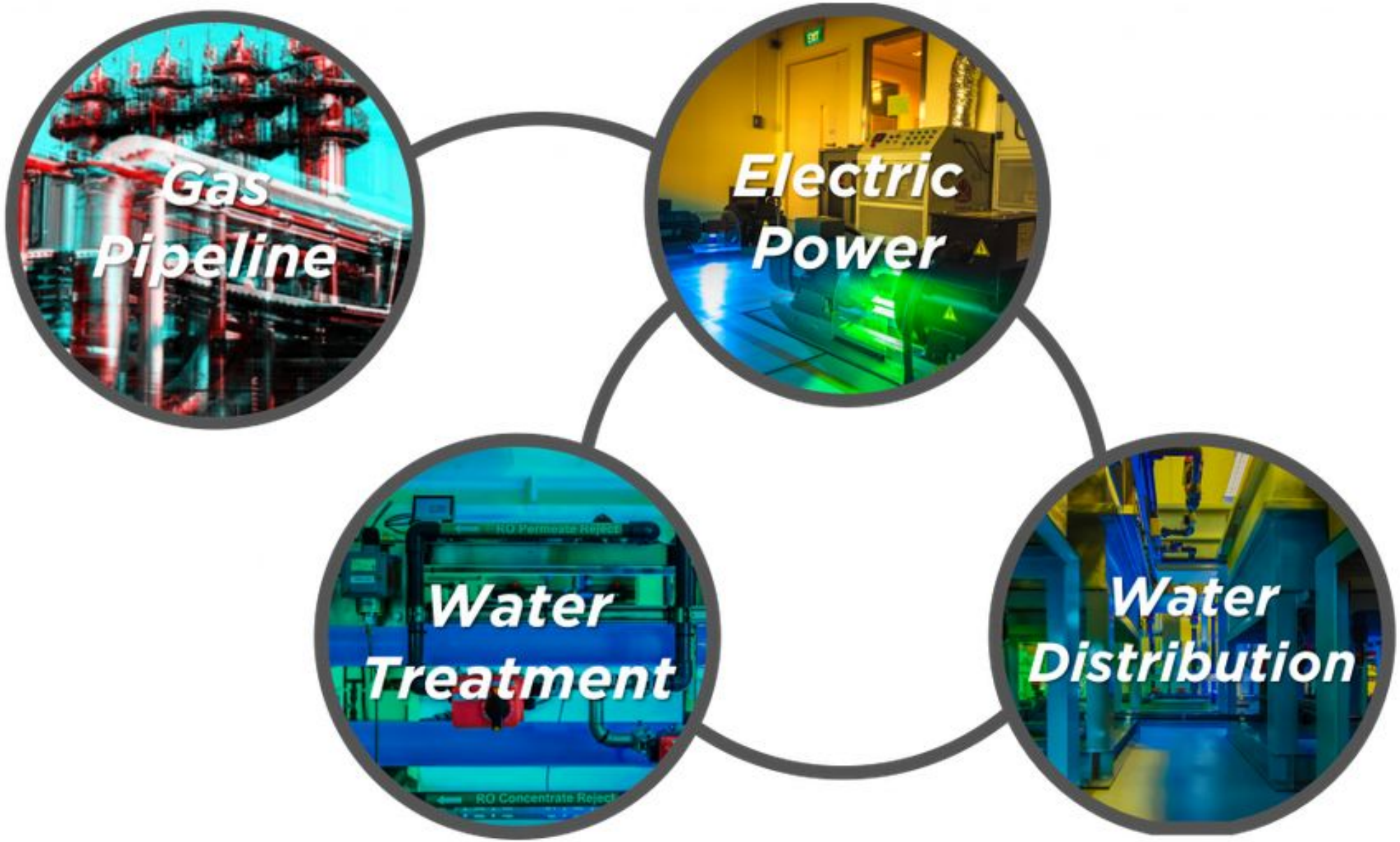
- **Period**
  - 24 - 28 July
  - 1000 - 1700
- **Configuration**
  - Concurrent session across all vendors
  - Testbeds and Digital Twin will running in normal mode
- **Actions taken by the operator made known**
- **No active scanning during this period**
- **No further devices be added after 28 July**

Requests

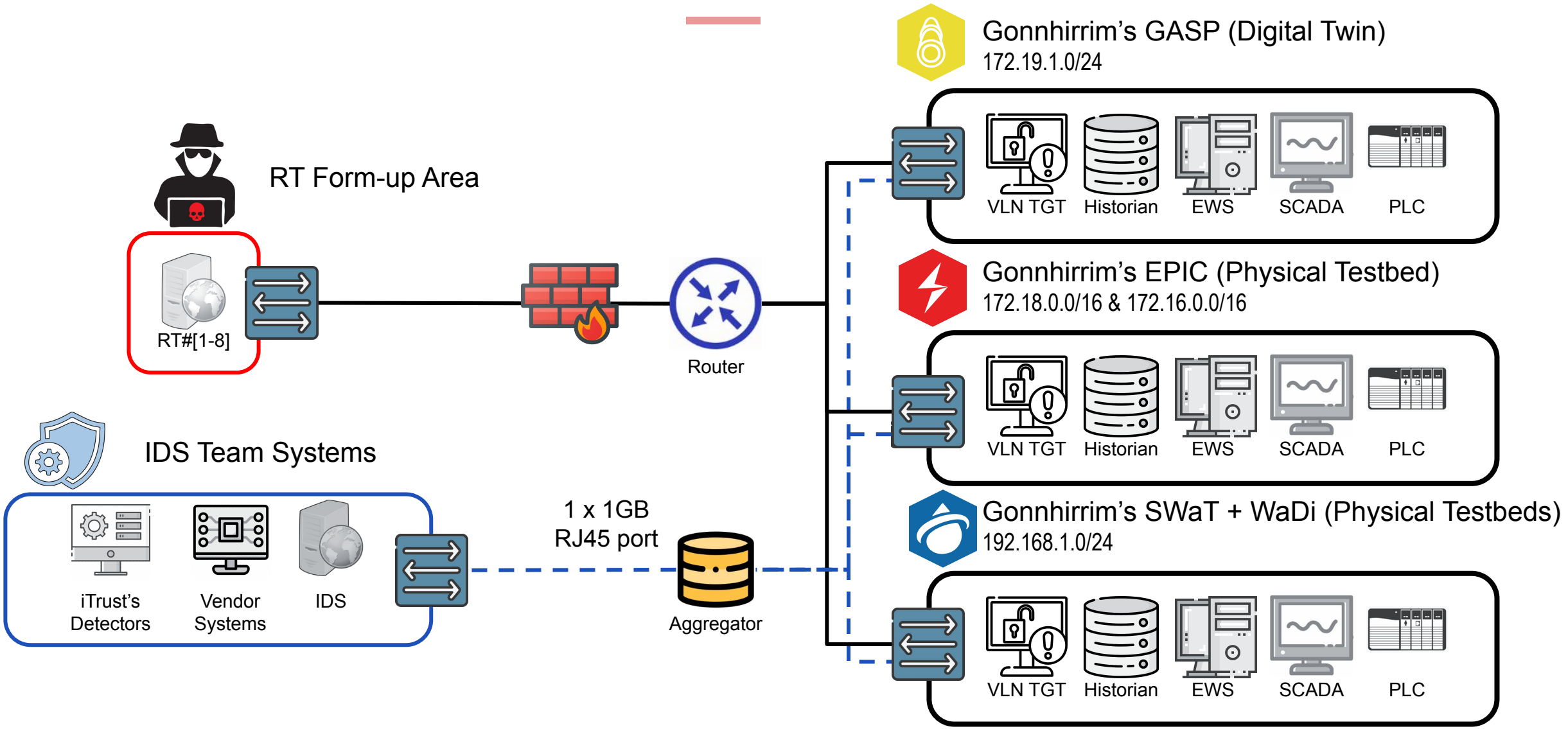
- **Any other requests, please do through the booking link**
  - E.g. 2 x RJ45 ports, request for historian data
  - We will do our best to accommodate the request
- Please also indicate which vendor you are affiliated with as part of your name
  - E.g. Ivan Christian (iTrust) → In the name field.



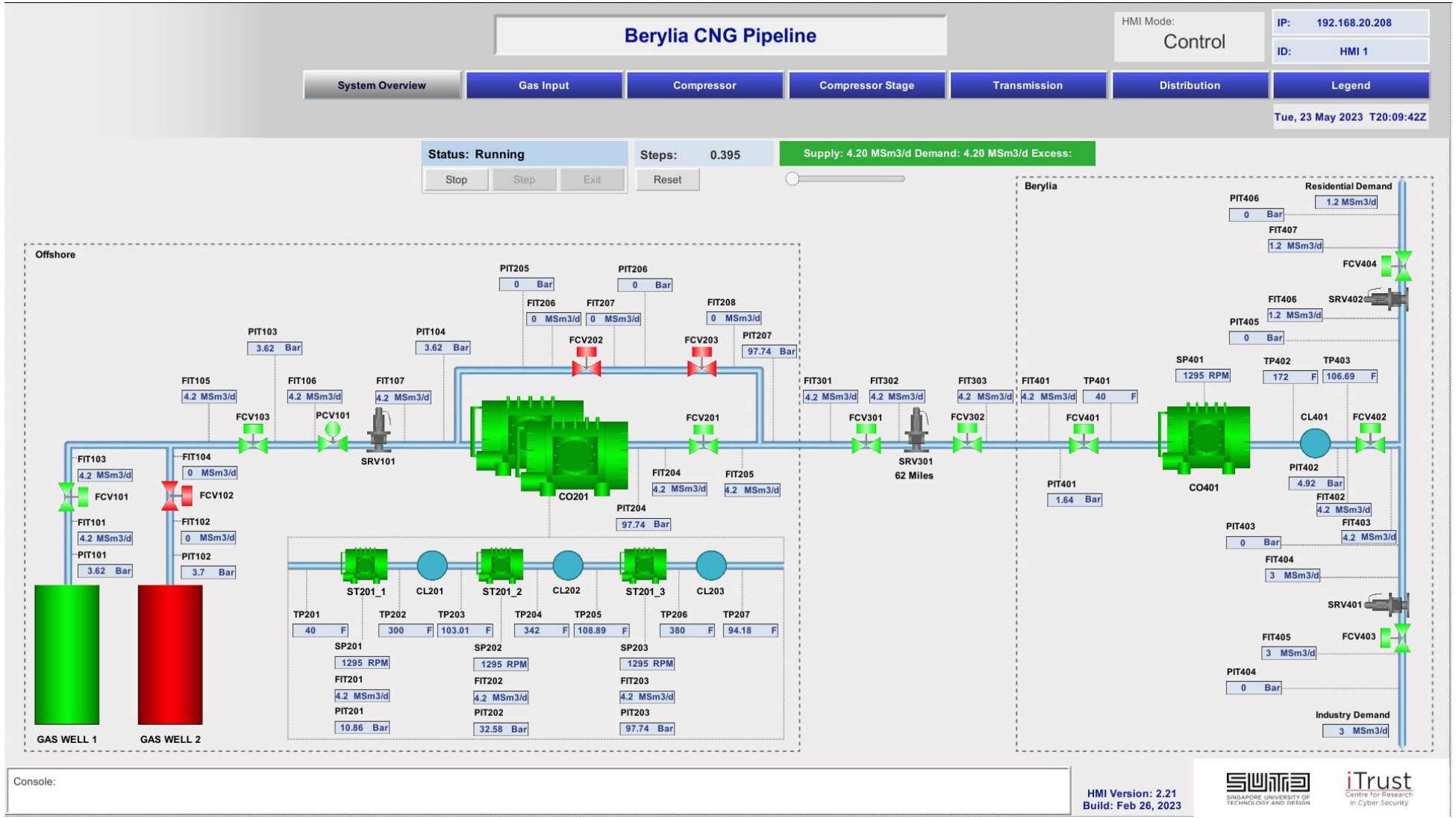
Setup for CISS 2023 Execution


Gas Pipeline
Electric Power
Water Treatment
Water Distribution

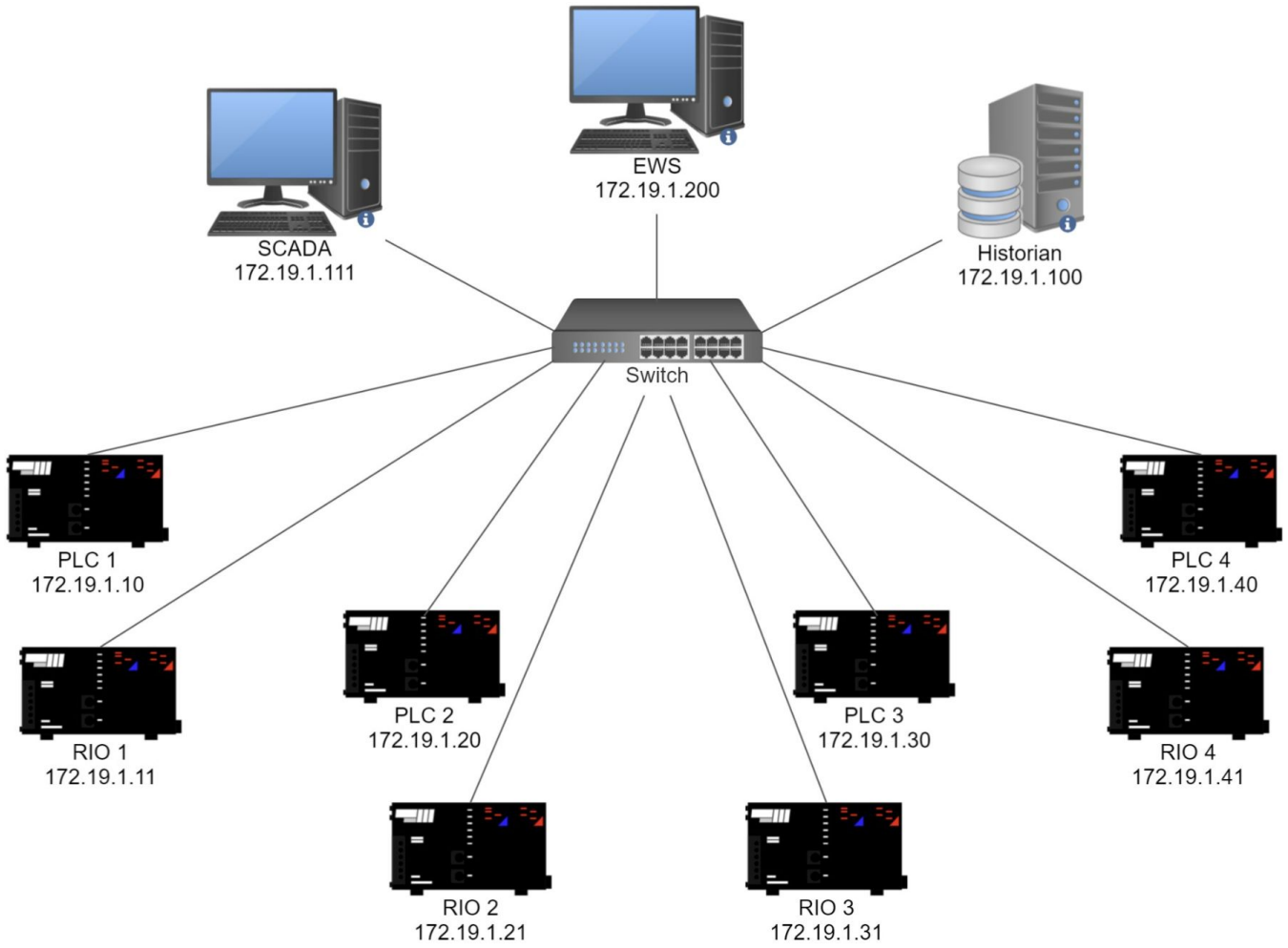
CISS Finals Network Architecture



GAS Pipeline HMI



GAS Pipeline Network



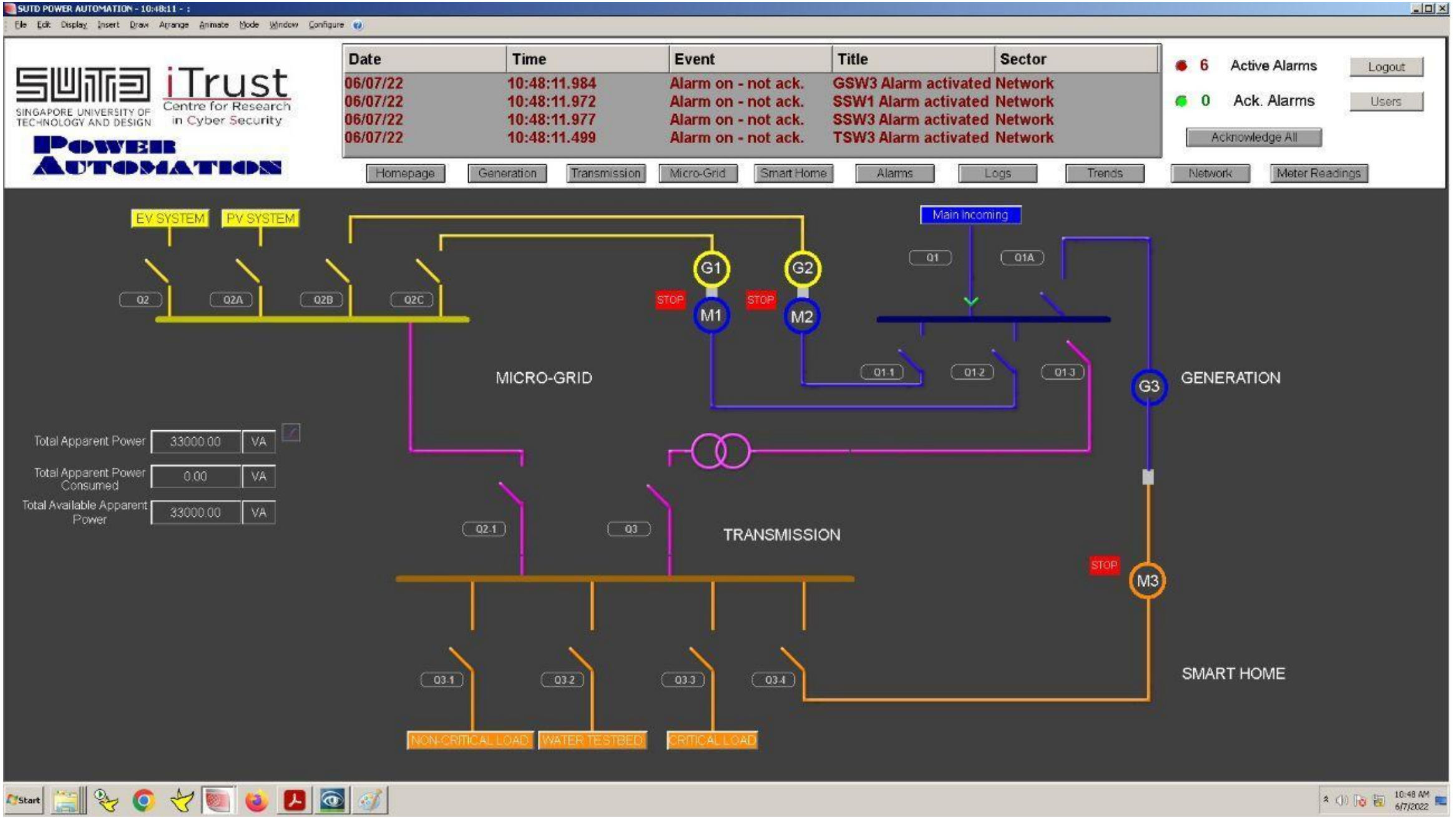
PLCs: Python

Subnet:

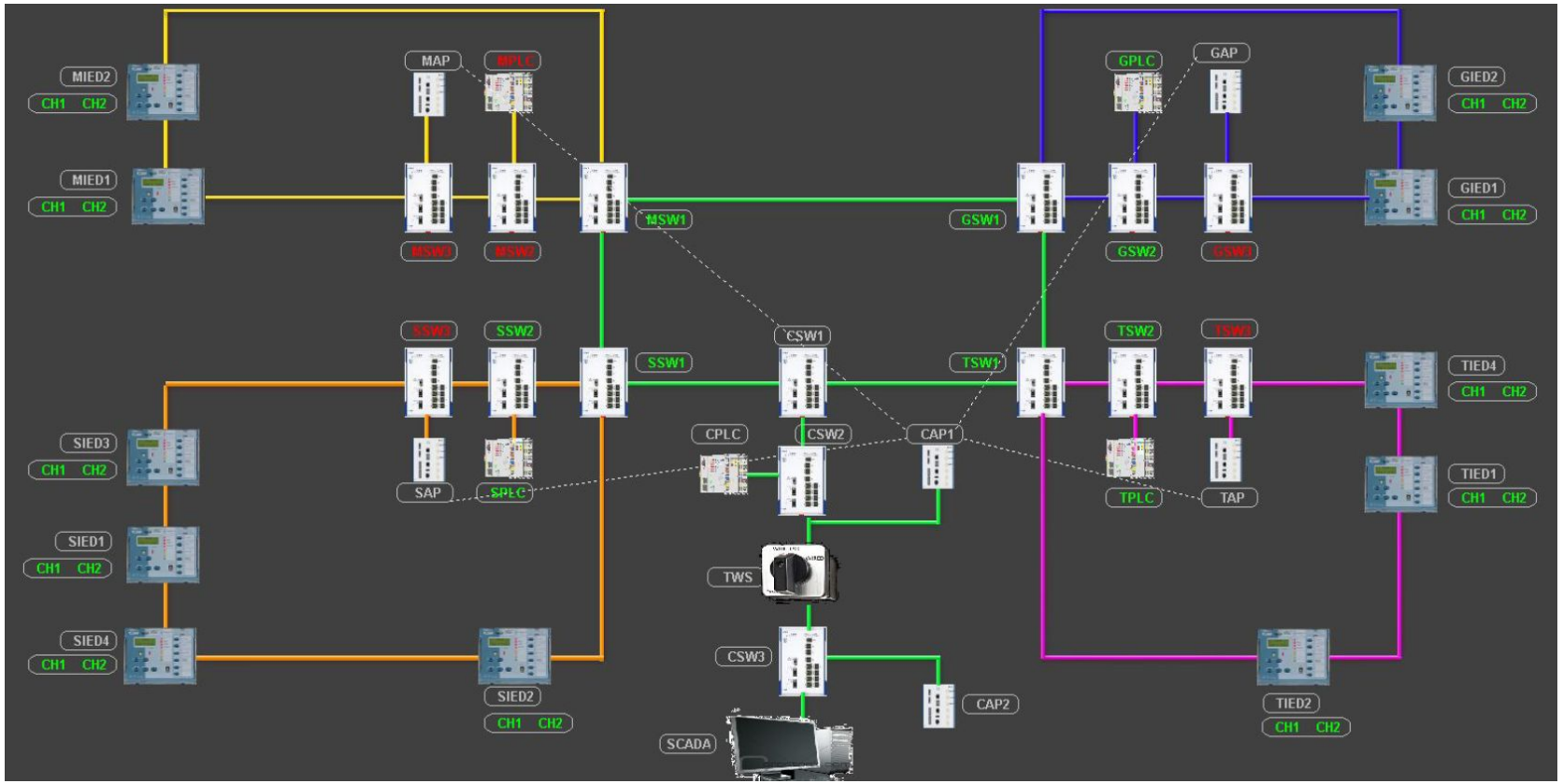
1. 172.19.1.0/24

Protocol:

1. OPCUA
2. ZMQ


SUTD POWER AUTOMATION - 10:48:11 - :
File Edit Display Insert Draw Arrange Animate Mode Window Configure
SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN
iTrust
Centre for Research in Cyber Security
POWER AUTOMATION
Date Time Event Title Sector
06/07/22 10:48:11.984 Alarm on - not ack. GSW3 Alarm activated Network
06/07/22 10:48:11.972 Alarm on - not ack. SSW1 Alarm activated Network
06/07/22 10:48:11.977 Alarm on - not ack. SSW3 Alarm activated Network
06/07/22 10:48:11.499 Alarm on - not ack. TSW3 Alarm activated Network
6 Active Alarms
0 Ack. Alarms
Logout
Users
Acknowledge All
Homepage Generation Transmission Micro-Grid Smart Home Alarms Logs Trends Network Meter Readings
EV SYSTEM
PV SYSTEM
Main Incoming
Q1
Q1A
Q2
Q2A
Q2B
Q2C
G1
G2
STOP
STOP
M1
M2
MICRO-GRID
Q1-1
Q1-2
Q1-3
G3
GENERATION
Total Apparent Power 33000.00 VA
Total Apparent Power Consumed 0.00 VA
Total Available Apparent Power 33000.00 VA
Q2-1
Q3
TRANSMISSION
STOP
M3
Q3-1
Q3-2
Q3-3
Q3-4
SMART HOME
NON-CRITICAL LOAD
WATER TESTBED
CRITICAL LOAD
Start
10:48 AM
6/7/2022

Electric Grid Network



PLCs: WAGO

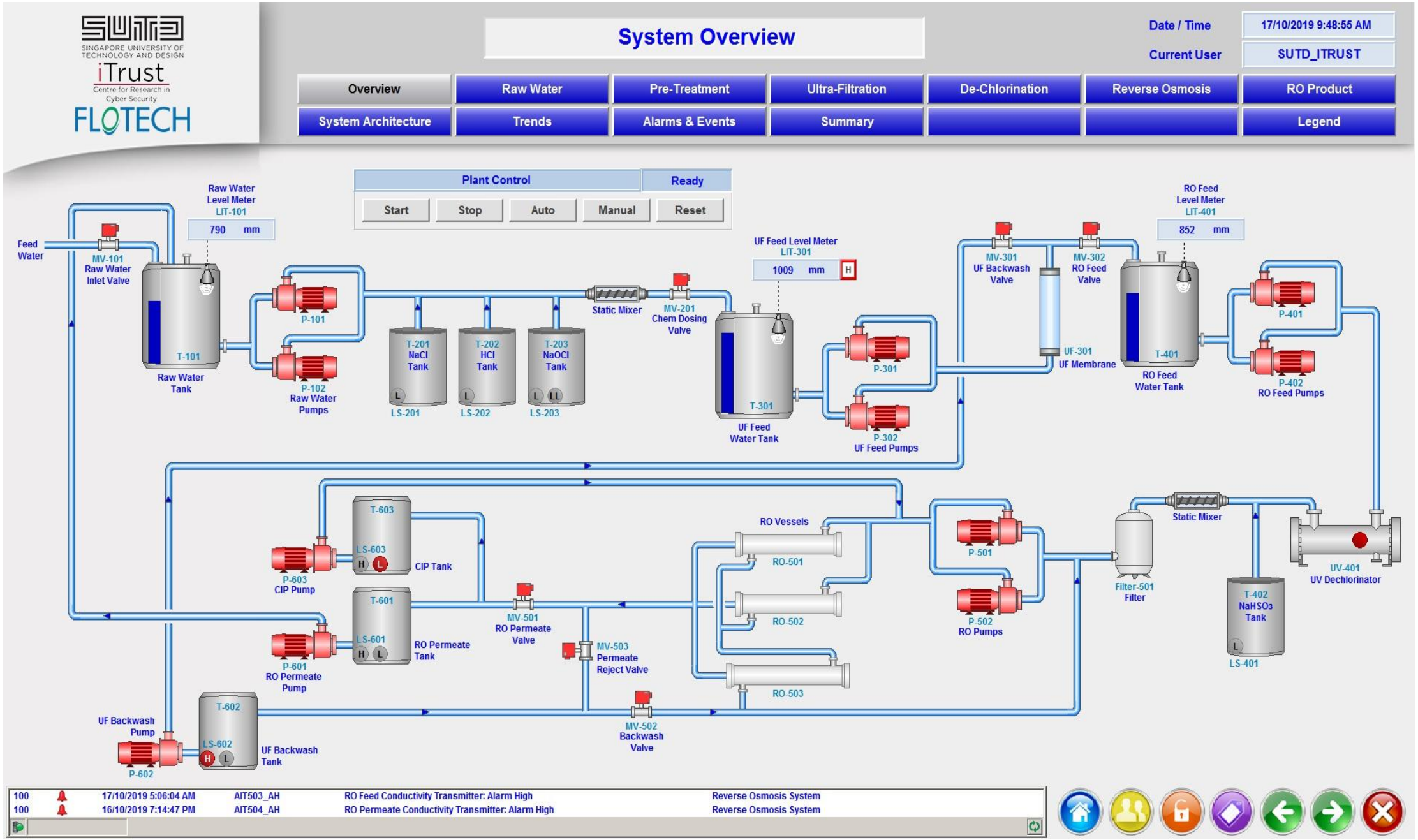
Subnet:

1. 172.18.0.0/16
2. 172.16.0.0/16

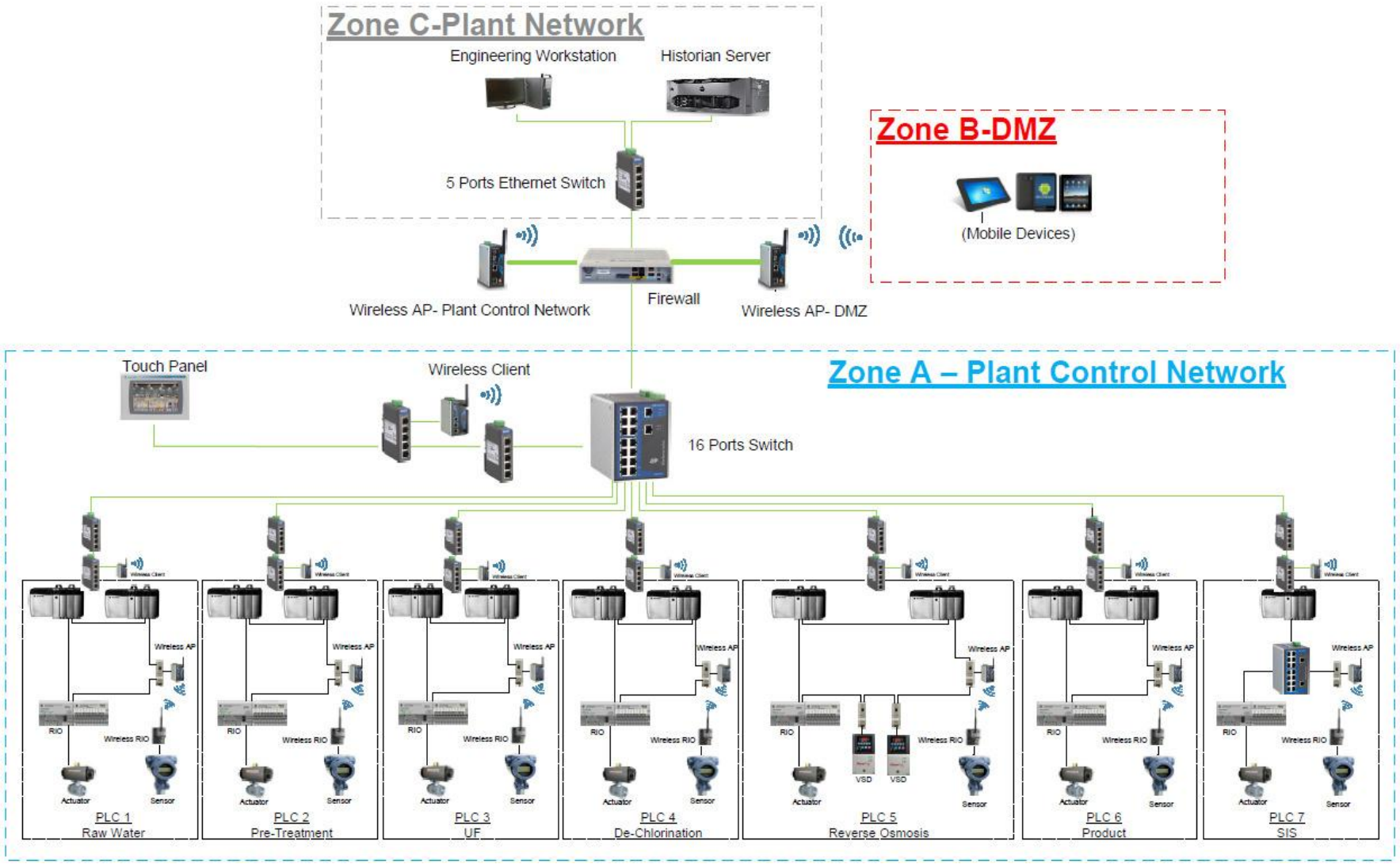
Protocols:

1. IEC 61850
   a. MMS
   b. GOOSE

a. Modbus TCP

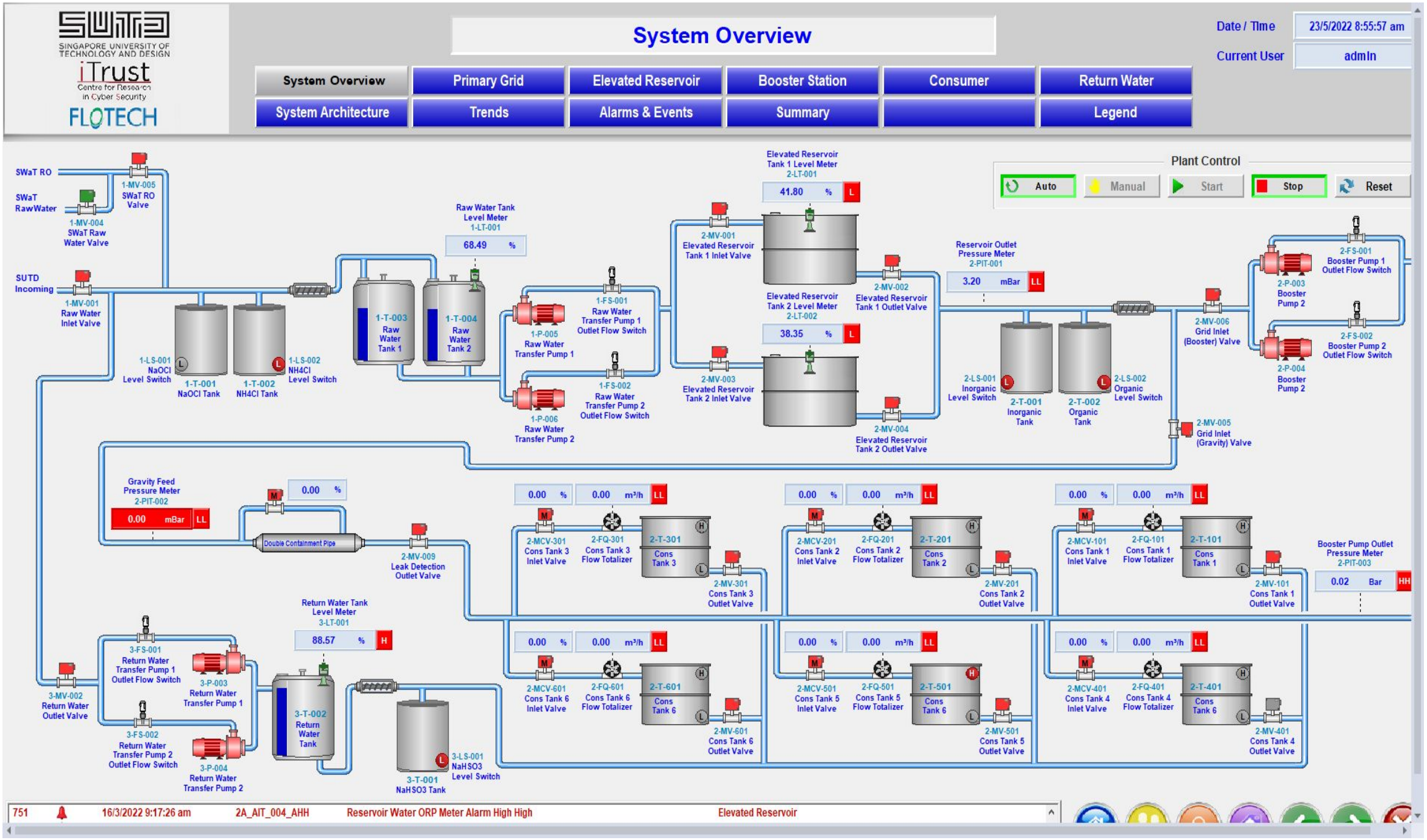

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN
iTrust
Centre for Research in Cyber Security
FLOTECH
System Overview
Date / Time
17/10/2019 9:48:55 AM
Current User
SUTD_ITRUST
Overview
Raw Water
Pre-Treatment
Ultra-Filtration
De-Chlorination
Reverse Osmosis
RO Product
System Architecture
Trends
Alarms & Events
Summary
Legend
Plant Control
Ready
Start
Stop
Auto
Manual
Reset
Feed Water
MV-101 Raw Water Inlet Valve
Raw Water Level Meter LIT-101
790 mm
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
1009 mm
H
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
852 mm
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
UV-401 UV Dechlorinator
T-402 NaHSO3 Tank
LS-401
UF Backwash Pump
T-602
LS-602
UF Backwash Tank
P-602
MV-502 Backwash Valve
100 17/10/2019 5:06:04 AM AIT503_AH RO Feed Conductivity Transmitter: Alarm High Reverse Osmosis System
100 16/10/2019 7:14:47 PM AIT504_AH RO Permeate Conductivity Transmitter: Alarm High Reverse Osmosis System

Water Treatment Network Diagram

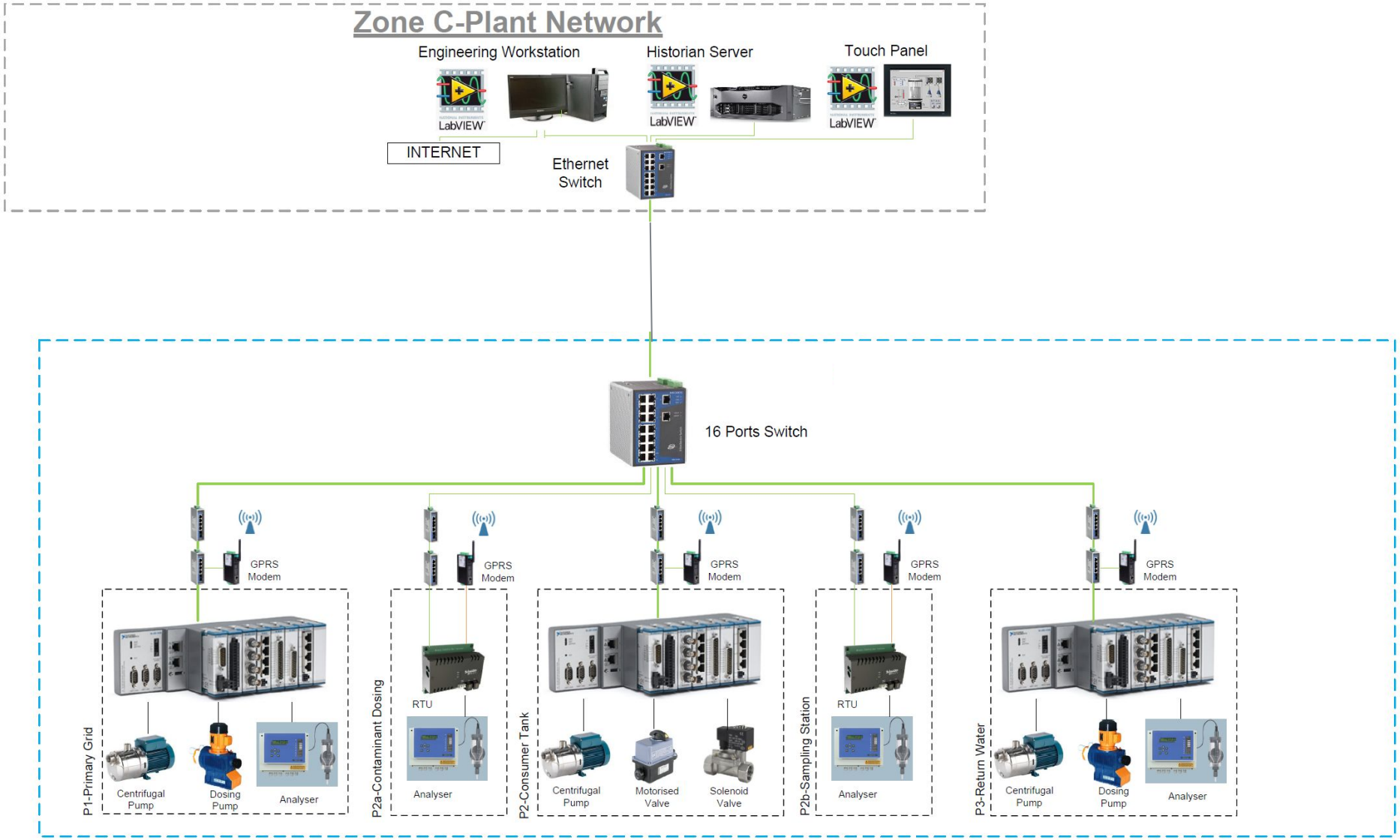


PLC: Allen-Bradley
Subnet: 192.168.1.0/24
Protocol:

1. EtherNet/IP (ENIP)


SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN
iTrust
Centre for Research in Cyber Security
FLOTECH
System Overview
Date / Time
23/5/2022 8:55:57 am
Current User
admin
System Overview
Primary Grid
Elevated Reservoir
Booster Station
Consumer
Return Water
System Architecture
Trends
Alarms & Events
Summary
Legend
Plant Control
Auto
Manual
Start
Stop
Reset
SWaT RO
SWaT RawWater
1-MV-004 SWaT Raw Water Valve
1-MV-005 SWaT RO Valve
SUTD Incoming
1-MV-001 Raw Water Inlet Valve
1-LS-001 NaOCl Level Switch
1-T-001 NaOCl Tank
1-T-002 NH4Cl Tank
1-LS-002 NH4Cl Level Switch
Raw Water Tank Level Meter 1-LT-001
68.49 %
1-T-003 Raw Water Tank 1
1-T-004 Raw Water Tank 2
1-P-005 Raw Water Transfer Pump 1
1-FS-001 Raw Water Transfer Pump 1 Outlet Flow Switch
1-P-006 Raw Water Transfer Pump 2
1-FS-002 Raw Water Transfer Pump 2 Outlet Flow Switch
Elevated Reservoir Tank 1 Level Meter 2-LT-001
41.80 %
Elevated Reservoir Tank 2 Level Meter 2-LT-002
38.35 %
2-MV-001 Elevated Reservoir Tank 1 Inlet Valve
2-MV-002 Elevated Reservoir Tank 1 Outlet Valve
2-MV-003 Elevated Reservoir Tank 2 Inlet Valve
2-MV-004 Elevated Reservoir Tank 2 Outlet Valve
Reservoir Outlet Pressure Meter 2-PIT-001
3.20 mBar LL
2-LS-001 Inorganic Level Switch
2-T-001 Inorganic Tank
2-T-002 Organic Tank
2-LS-002 Organic Level Switch
2-MV-006 Grid Inlet (Booster) Valve
2-MV-005 Grid Inlet (Gravity) Valve
2-P-003 Booster Pump 2
2-P-004 Booster Pump 2
2-FS-001 Booster Pump 1 Outlet Flow Switch
2-FS-002 Booster Pump 2 Outlet Flow Switch
Gravity Feed Pressure Meter 2-PIT-002
0.00 mBar LL
Double Containment Pipe
2-MV-009 Leak Detection Outlet Valve
2-MCV-301 Cons Tank 3 Inlet Valve
2-FQ-301 Cons Tank 3 Flow Totalizer
2-T-301 Cons Tank 3
2-MV-301 Cons Tank 3 Outlet Valve
2-MCV-201 Cons Tank 2 Inlet Valve
2-FQ-201 Cons Tank 2 Flow Totalizer
2-T-201 Cons Tank 2
2-MV-201 Cons Tank 2 Outlet Valve
2-MCV-101 Cons Tank 1 Inlet Valve
2-FQ-101 Cons Tank 1 Flow Totalizer
2-T-101 Cons Tank 1
2-MV-101 Cons Tank 1 Outlet Valve
Booster Pump Outlet Pressure Meter 2-PIT-003
0.02 Bar HH
2-MCV-601 Cons Tank 6 Inlet Valve
2-FQ-601 Cons Tank 6 Flow Totalizer
2-T-601 Cons Tank 6
2-MV-601 Cons Tank 6 Outlet Valve
2-MCV-501 Cons Tank 5 Inlet Valve
2-FQ-501 Cons Tank 5 Flow Totalizer
2-T-501 Cons Tank 6
2-MV-501 Cons Tank 5 Outlet Valve
2-MCV-401 Cons Tank 4 Inlet Valve
2-FQ-401 Cons Tank 4 Flow Totalizer
2-T-401 Cons Tank 6
2-MV-401 Cons Tank 4 Outlet Valve
Return Water Tank Level Meter 3-LT-001
88.57 % H
3-MV-002 Return Water Outlet Valve
3-FS-001 Return Water Transfer Pump 1 Outlet Flow Switch
3-P-003 Return Water Transfer Pump 1
3-FS-002 Return Water Transfer Pump 2 Outlet Flow Switch
3-P-004 Return Water Transfer Pump 2
3-T-002 Return Water Tank
3-T-001 NaHSO3 Tank
3-LS-001 NaHSO3 Level Switch
751
16/3/2022 9:17:26 am
2A_AIT_004_AHH
Reservoir Water ORP Meter Alarm High High
Elevated Reservoir

Water Distribution Network



PLC: Allen-Bradley
Subnet: 192.168.1.0/24
Protocols:

1. EtherNet/IP (ENIP)
2. Modbus TCP

Alert Logging Procedure and Timeline

28 August 2023

Alert Logging via Syslog

- **Alert logging will be from 0900 to 1800**
  - 18, 21- 24 Aug, for your own collection and analysis
  - 28 Aug, IDS evaluation by iTrust
- **Your systems will be turned on by iTrust at 8.30am**
- **Please shutdown your servers at the end of the day**
- **Configure system to produce syslogs for Graylog extractor**
- **During Installation, ensure that Graylog can receive your syslogs**

Monitoring Rules

- **Should monitor**
  - 192.168.1.0/24
  - 172.18.0.0/16
  - 172.16.0.0/16
  - 172.19.1.0/24
- **Need not monitor**
  - Hypervisors
  - 10.0.0.0/8
  - 169.254.0.0/16

IDS Performance Analysis

18 August - 24 August 2023 (Red Team Execution)

28 August 2023 (Evaluation)

Evaluation Session

- **Each of the IDS will be evaluated against a set of benchmark Attacks**

- **The following are the types of possible attacks launched during the exercise and evaluation:**

- **IT Attack**
  - These attacks purely affect communications in the network
- **OT Attack**
  - These attacks purely affect the processes of the system
- **IT-OT Attack**
  - These attacks come as a combination that affect the communications and the processes

Performance Metrics

Score	Identification of Components	Readability	Accuracy	Responsiveness	Intrusivity
4					
3					
2					
1					
0					

Framework Rubric					
Score	**Identification of Components**	**Readability**	**Accurcacy of the solution**	**Responsiveness of Solution**	**Intrusivity of the Solution**
4	Specific Component is identified, Specific Stage Identified, Component failure type identified clearly, Reason for failure has also been identified. Example: An alarm on Stage 1 : P101 has been raised. P101 has failed to open due to an attack on LIT101.	Flesch-Kincaid Readability score of 70.0 - 100.0 (US 7th Graders and below can easily understand)	Model Detects 90.0 % - 100% of the attacks (TP). Model also detects 0.0 %- 10 % False Alarm.	Alarm is generated within 0 s - 60 s of the anomaly	Solution does not disrupts with plant operations
	Specific Component is identified, Specific Stage Identified, Component				

Component Identification

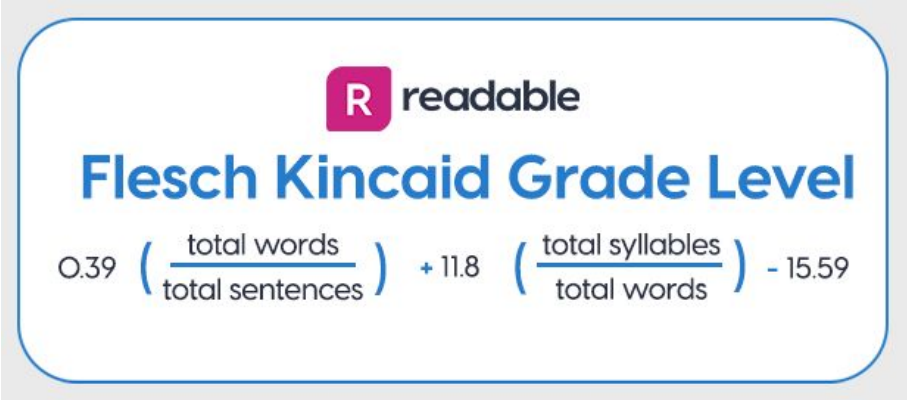
- **4 Points**
  - Failed Stage Identified (1 point)
  - Component Identified (1 point)
  - Failure type (1 point)
  - **Reason for Failure (1 point)**
- **3 Points**
  - Failed Stage Identified (1 point)
  - Component Identified (1 point)
  - **Failure type (1 point)**
- **2 Points**
  - Failed Stage Identified (1 point)
  - **Component Identified (1 point)**
- **1 Point**
  - **Failed Stage Identified (1 point)**
- **0 Point**
  - Nothing identified

Readability

To measure the clarity of the alert for a detector, it needs to be human readable and can return meaningful information to the operators or anyone viewing the alert. Not everyone is trained in the art of reading alerts through network information or process specific jargons.
Using Flesch-Kincaid formula, we can calculate the score.

Readability Measurement:

- Flesch-Kincaid Score 70.0 - 100.0 (4 points)
- Flesch-Kincaid Score 50.0 - 69.9 (3 points)
- Flesch-Kincaid Score 30.0 - 49.9 (2 points)
- Flesch-Kincaid Score 10.0 - 29.9 (1 points)
- Flesch-Kincaid Score 0.0 - 9.9 (0 points)



https://readable.com/readability/flesch-reading-ease-flesch-kincaid-grade-level/

Accuracy

Accuracy Measurement is done based on whether the solution can precisely detect the attacks done on the system and does not generate False alarms.

Accuracy Performance Measurement:

- 90.0 - 100.0% Accuracy and 0.0 - 10.0 % False Alarm Rate (4 points)
- 70.0 - 89.9% Accuracy and 10.1 - 30.0 % False Alarm Rate (3 points)
- 50.0 - 69.9% Accuracy and 30.1 - 50.0 % False Alarm Rate (2 points)
- 30.0 - 49.9% Accuracy and 50.1 - 70.0 % False Alarm Rate (1 points)
- 0.0 - 29.9% Accuracy and 70.1 - 100.0 % False Alarm Rate (0 points)

Responsiveness

Detectors are supposed to alert the operators promptly to prevent permanent damage to the system. It is agreed that generally the sooner the operators are alerted the better.

Responsiveness Measurement:

- Within the minute (4 points)
- Within the hour (3 points)
- Within 4 hours (2 points)
- More than 4 hours (1 points)
- No even detected (0 points)

Intrusivity

A measure of a detector would also be on how intrusive the it would be when detecting any anomalies in the system. If the detector breaks the system then it would lead to a pretty bad situation, therefore we need to make sure that the solution does not break the system.

How this category will be calculated would be a ratio of the system downtime due to detector and total system uptime.

Intrusivity Measurement:

- Never breaks the system. (4 points)
- Disrupts the system 1- 20% of the time (3 points)
- Disrupts 21 - 50% of the time (2 points)
- Disrupts 51 - 99% of the time (1 points)
- Always breaks the system (0 points)

IDS Evaluation

iTrust will be sending out the list of attacks done during the evaluation session by **30 August 2023.**

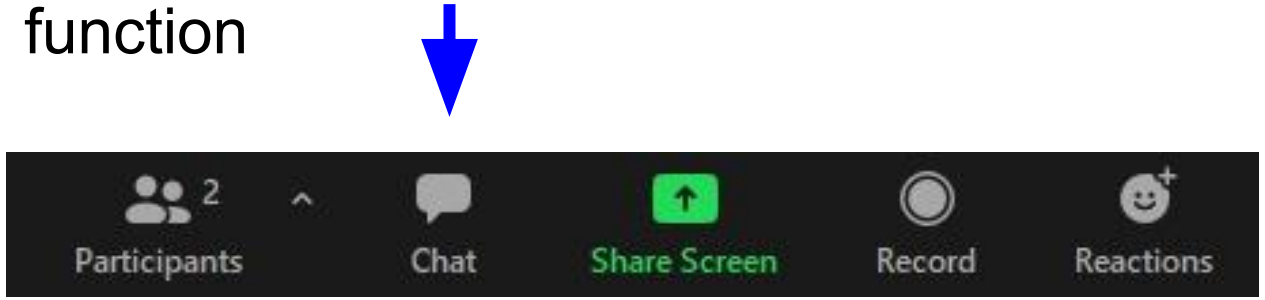
The report generated by the solutions are to be sent over back to iTrust by **15 September 2023.**

The performance of the solutions will then be evaluated using the Performance Metric and a report will be generated and sent over on a later date.

Q&A

Asking questions via Zoom:

Step 1: Use chat function



Step 2: Type in the word “question” and wait for your turn