iTrust
Centre for Research in Cyber Security

Briefing to IDS Teams
16 August 2024

Supported by

CSA SINGAPORE

National Cybersecurity R&D Laboratory

AGENDA

- IDS Timeline
- Administration Procedures
- CISS Setup
- Network Architecture
- IDS Performance analysis
- Q&A

IDS TIMELINE (REVISED)

Online briefing:	16 Aug 2024 (10:30 AM)
Onsite installation period:	19 – 30 Aug 2024
Active network scanning period:	2 - 12 Sep 2024
Baselining session:	13 - 18 Sep 2024
Evaluation session:	19 - 20 Sep 2024

ONSITE INSTALLATION PERIOD

Book max 2 days to set up your systems at iTrust

- 19 - 30 Aug 2024 (excluding weekend and 3rd Sep)
- 09:00 to 18:00
- Booking Link (https://tinyurl.com/ciss24ids)

Deliver systems to SWaT (from 19 August)

- Building 2, Level 7, Room 14,
  8 Somapah Road,
  Singapore 487372
- POC: Andrew (9745 0741)

ONSITE INSTALLATION PERIOD

We will provide

- Power socket
- Network 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 PERIOD

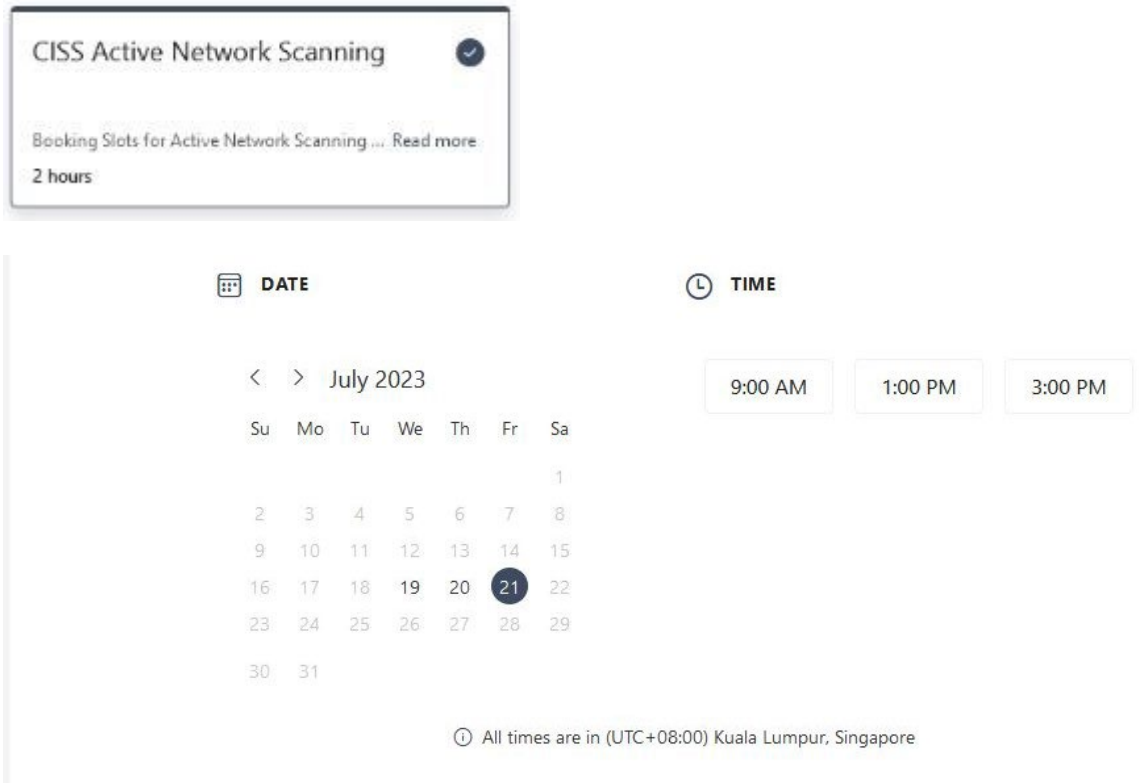
Book one session

- 2 - 12 Sep 2024 (Onsite)
- 0900 - 1100, 1300 - 1500, 1500 - 1700
- Booking Link (https://tinyurl.com/ciss24ids)

We will provide

- Access to the network
- dedicated slot per vendor

Bring your own tools



BASELINING SESSIONS DETAILS

Period

- 13 - 18 Sep 2024
- 10:00 – 17:00 hrs

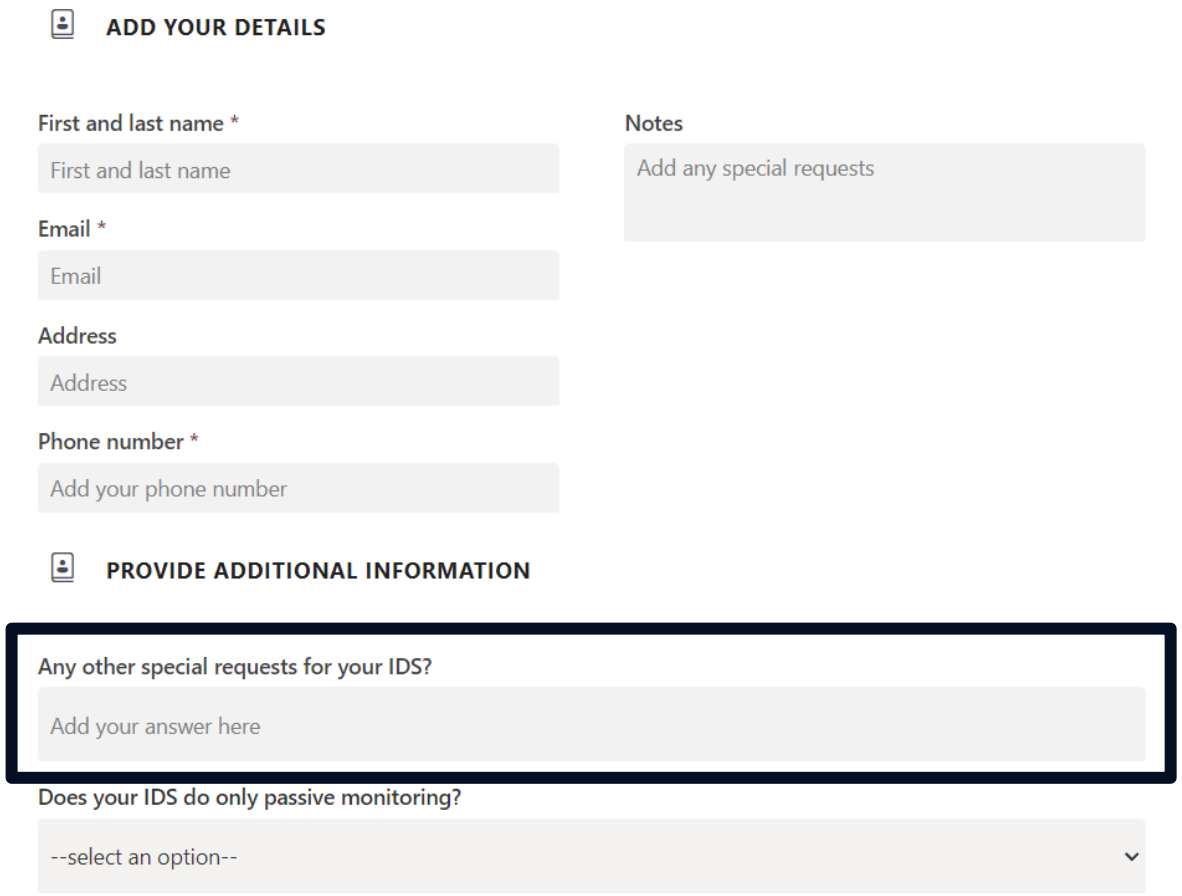
Configuration

- Concurrent session across all vendors
- Testbeds will running in normal mode

Please Note

- Actions taken by the operator made known
- No active scanning during this period
- No further devices be added after 10 Sep

REQUESTS

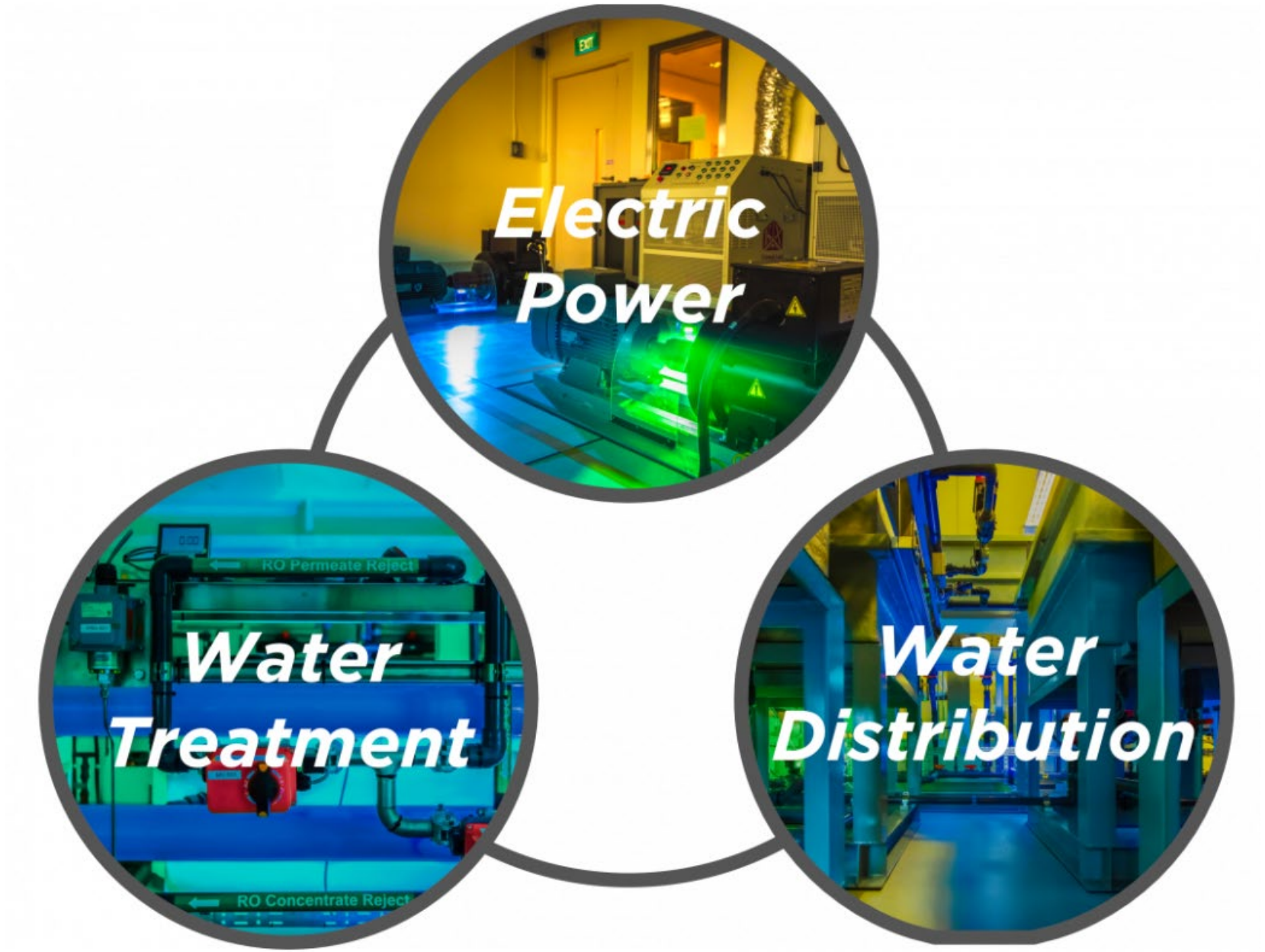


Any other requests, please do through the booking link

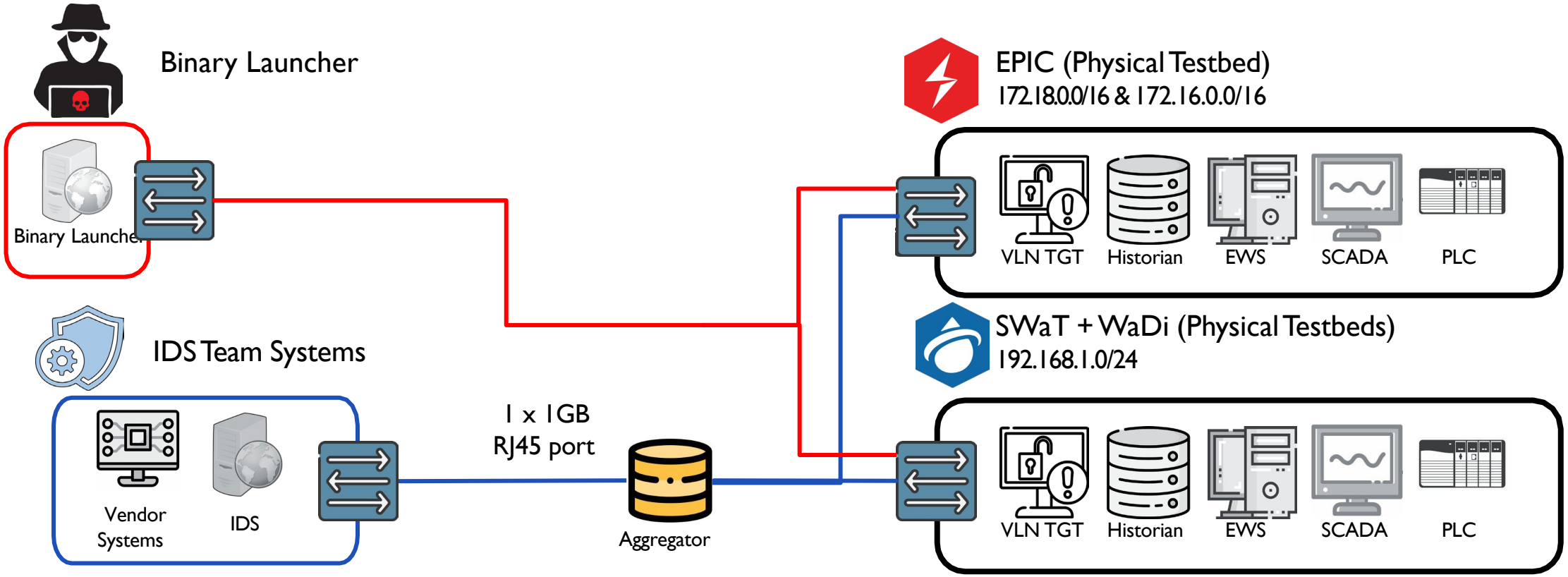
- E.g. 2 x RJ45 ports, request for historian data
- We will do our best to accommodate the request
- Please also indicate which vendor you are affiliated with as part of your name
- E.g. Ivan Christian (iTrust) → In the name field.

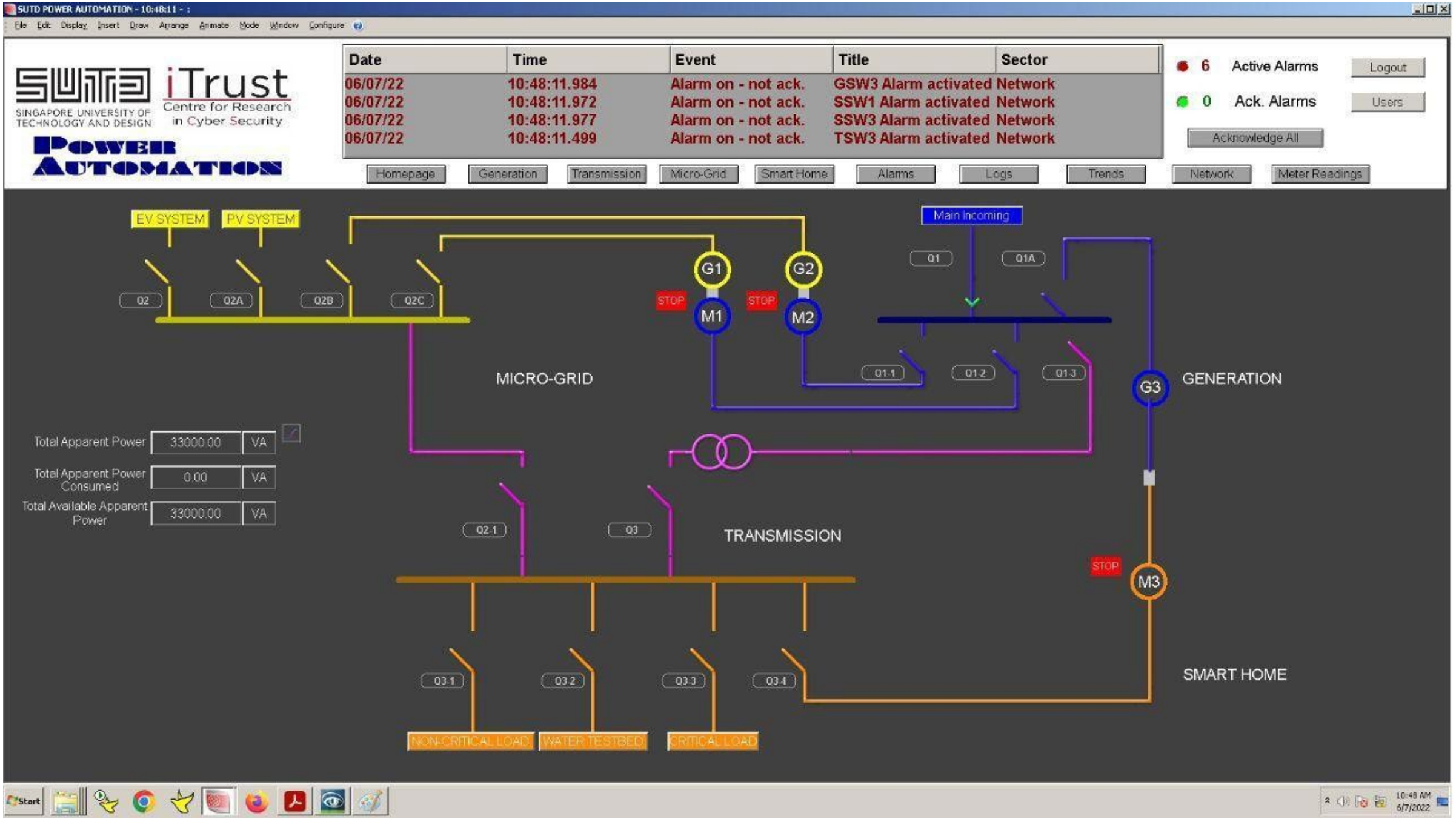
SETUP FOR CISS 2024 EXECUTION

THE EIGHTH INTERNATIONAL CRITICAL INFRASTRUCTURE SECURITY SHOWDOWN

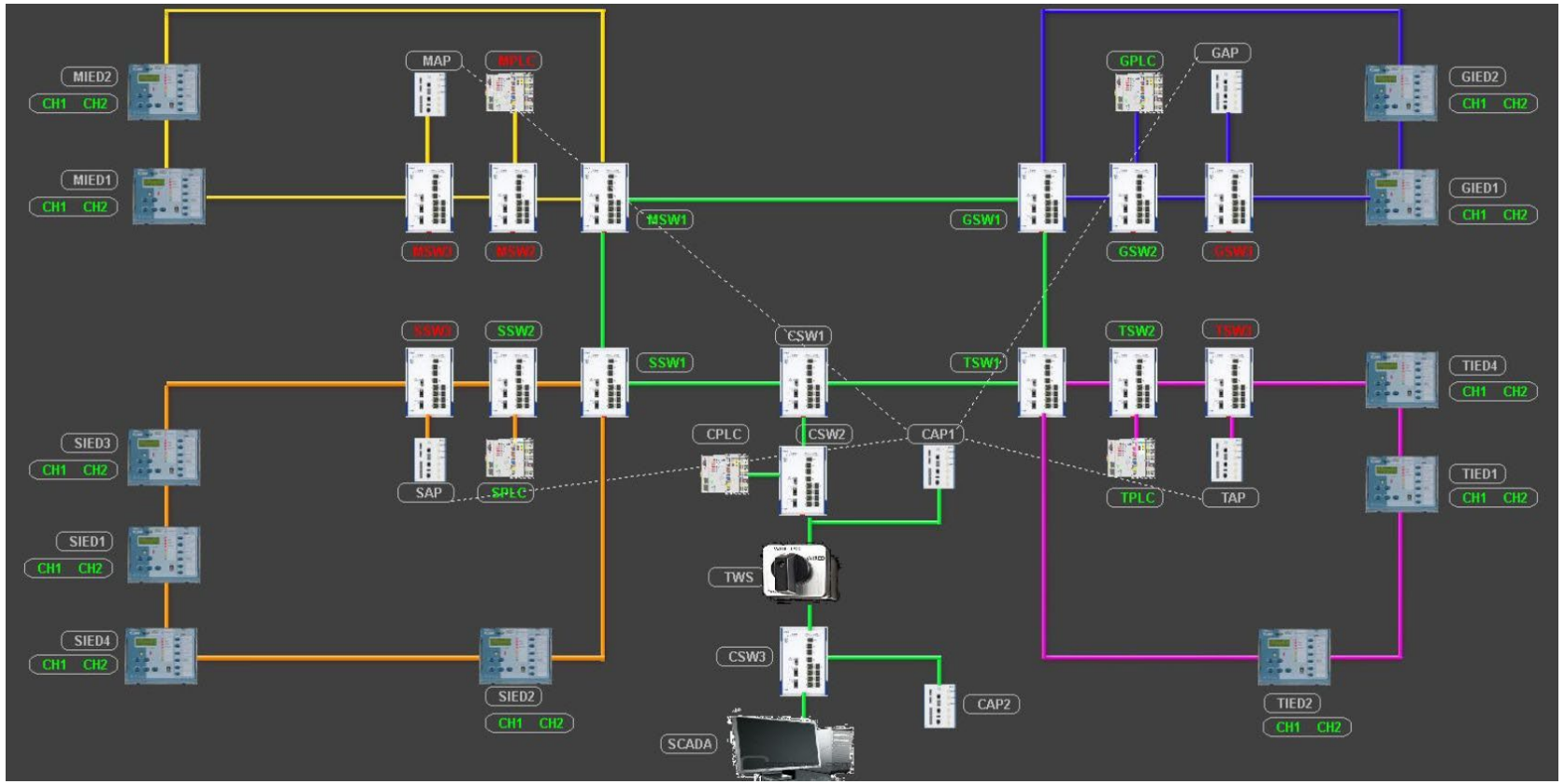

Electric Power
RO Permeate Reject
Water Treatment
RO Concentrate Reject
Water Distribution

CISS NETWORK ARCHITECTURE




SUTD POWER AUTOMATION - 10:48:11 - :
File Edit Display Insert Draw Arrange Animate Mode Window Configure
SUTD
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
Q1-1
Q1-2
Q1-3
MICRO-GRID
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



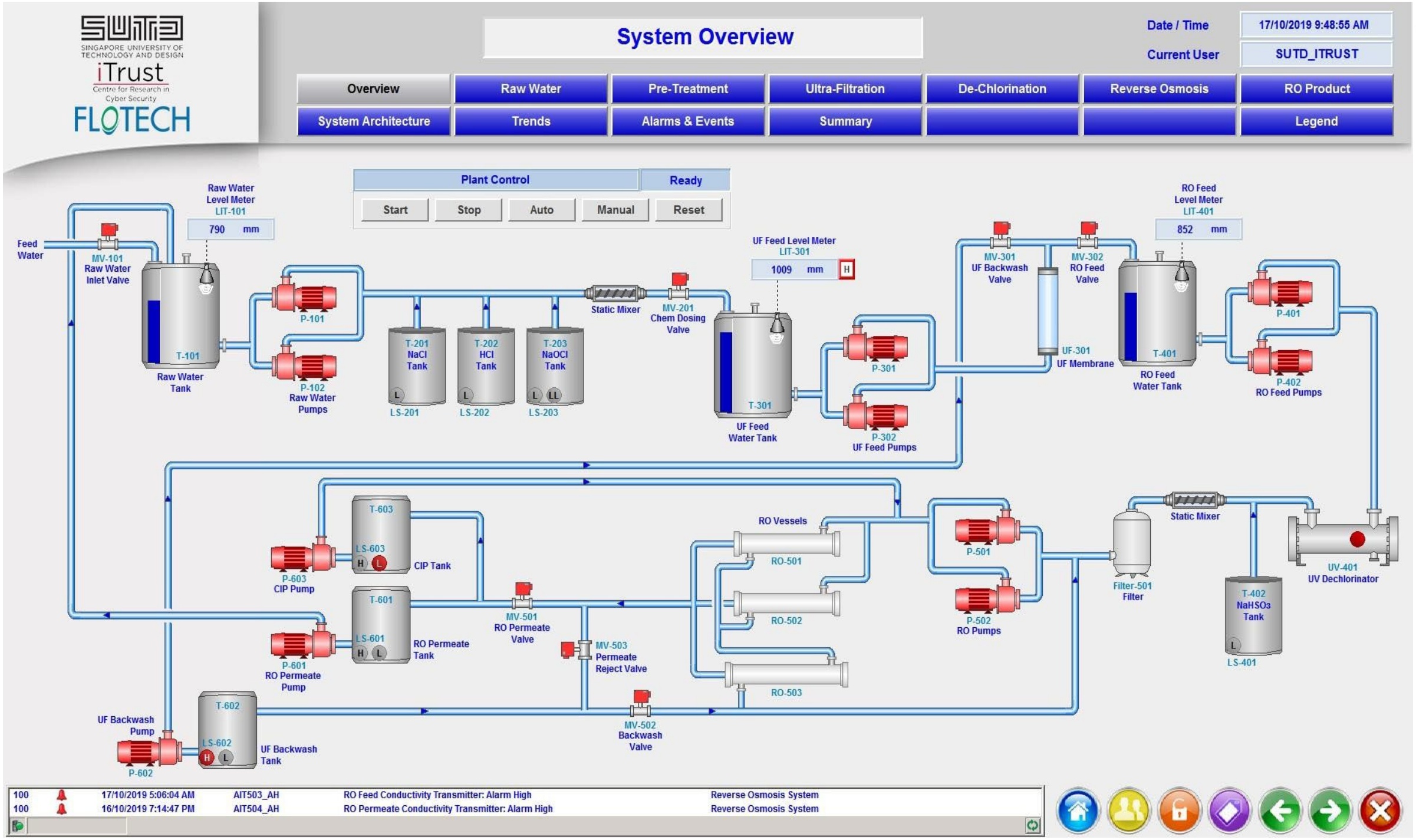
PLCs: WAGO

Subnet:

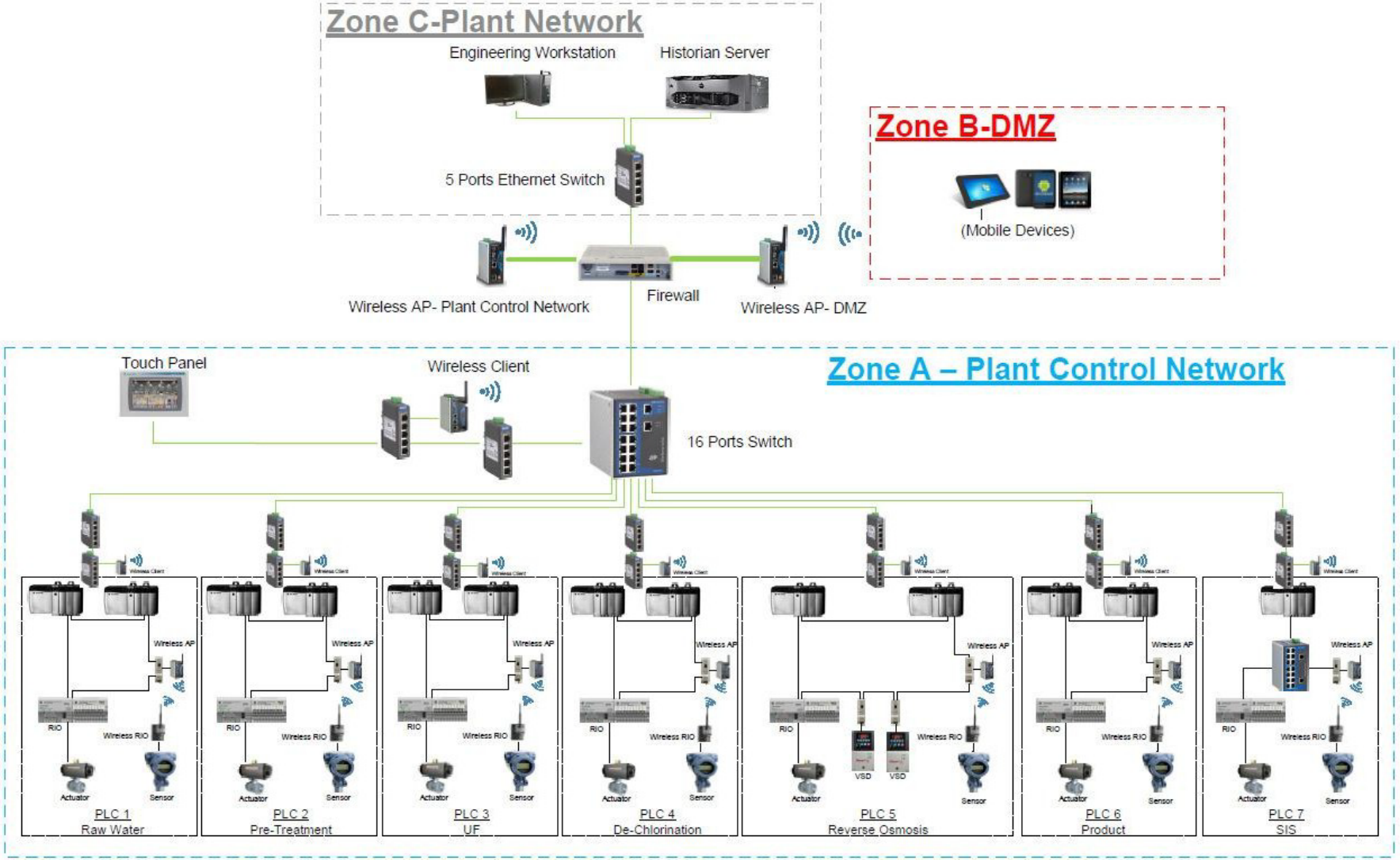
1. 172.18.0.0/16
2. 172.16.0.0/16

Protocols:

1. IEC 61850
   a. MMS
   b. GOOSE
2. Modbus TCP

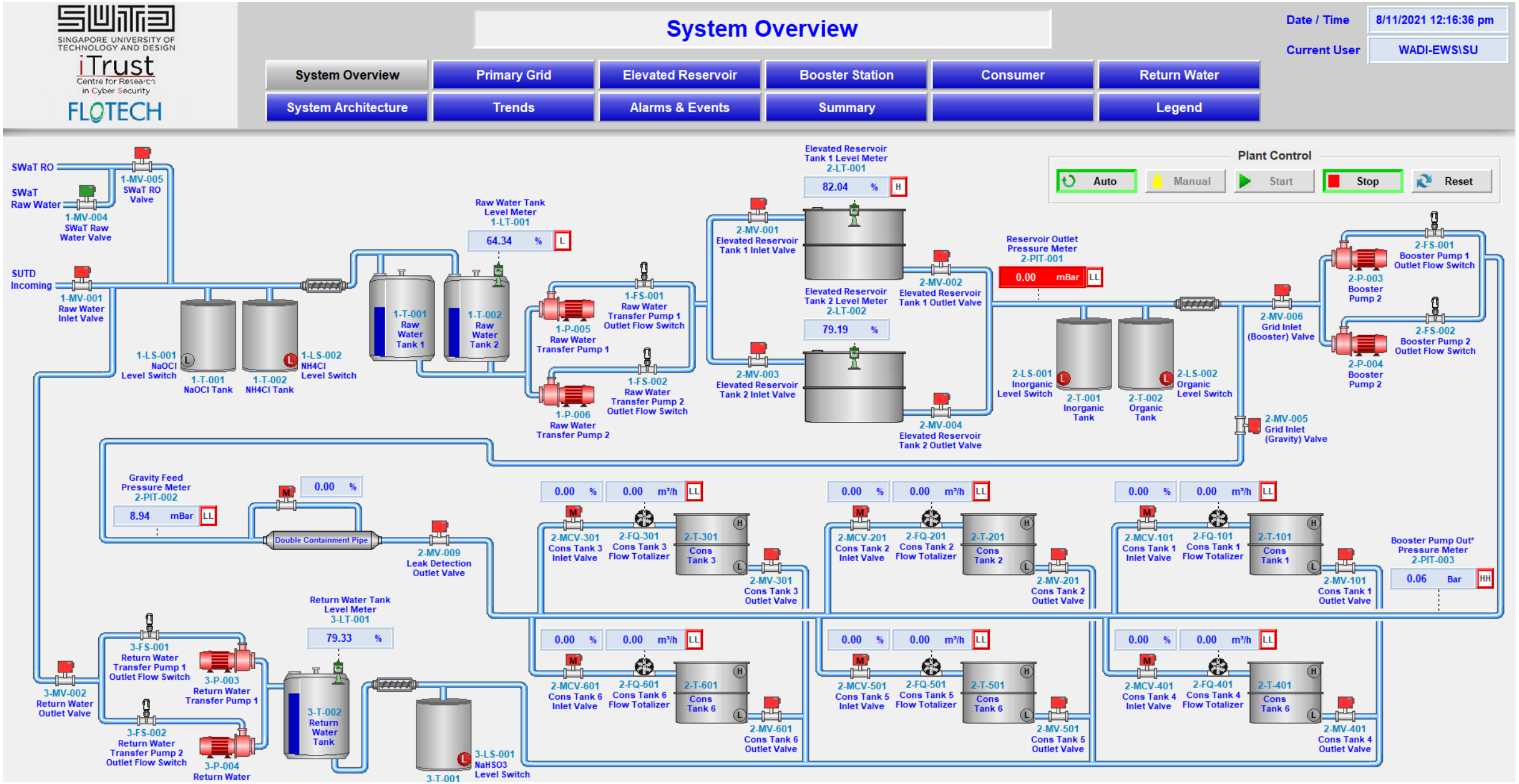

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN
iTrust
Centre for Research in Cyber Security
FLOTECH
System Overview
Date / Time
17/10/2019 9:48:55 AM
Current User
SUTD_ITRUST
Overview
Raw Water
Pre-Treatment
Ultra-Filtration
De-Chlorination
Reverse Osmosis
RO Product
System Architecture
Trends
Alarms & Events
Summary
Legend
Plant Control
Ready
Start
Stop
Auto
Manual
Reset
Raw Water Level Meter LIT-101
790 mm
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
1009 mm
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
T-602
LS-602
UF Backwash Tank
UF Backwash Pump
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

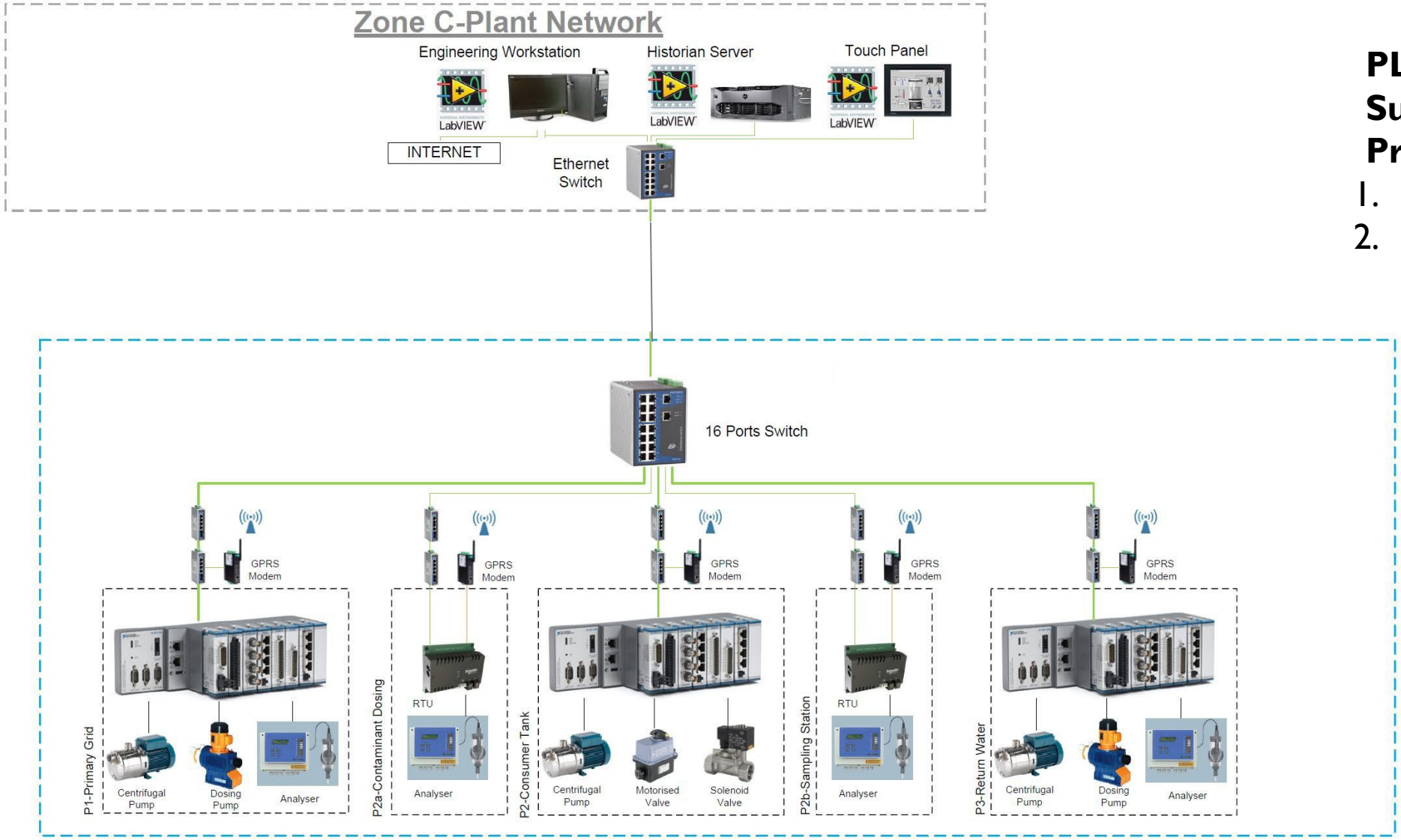


PLC: Allen-Bradley
Subnet: 192.168.1.0/24
Protocol:

1. EtherNet/IP (ENIP)


SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN
iTrust
Centre for Research in Cyber Security
FLOTECH
System Overview
Date / Time
8/11/2021 12:16:36 pm
Current User
WADI-EWS\SU
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 Raw Water
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
64.34 %
1-T-001 Raw Water Tank 1
1-T-002 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
82.04 %
Elevated Reservoir Tank 2 Level Meter 2-LT-002
79.19 %
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
0.00 mBar
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-P-003 Booster Pump 2
2-FS-001 Booster Pump 1 Outlet Flow Switch
2-P-004 Booster Pump 2
2-FS-002 Booster Pump 2 Outlet Flow Switch
2-MV-005 Grid Inlet (Gravity) Valve
Gravity Feed Pressure Meter 2-PIT-002
8.94 mBar
0.00 %
Double Containment Pipe
2-MV-009 Leak Detection Outlet Valve
0.00 % 0.00 m³/h
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 Out* Pressure Meter 2-PIT-003
0.06 Bar
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
79.33 %
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
3-T-002 Return Water Tank
3-T-001
3-LS-001 NaHSO3 Level Switch

Water Distribution Network



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

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

MONITORING GUIDELINES

Should monitor

- 192.168.1.0/24
- 172.18.0.0/16
- 172.16.0.0/16

Need not monitor

- Hypervisors
- 10.0.0.0/8
- 169.254.0.0/16

REPORTING OF INCIDENTS

Each IDS will get a Live excel spreadsheet

- Fields as below
- Custom fields allowed
- Update as alerts are found
- Spreadsheets will be open till end of 20 Sep

No	Period Start Time	Period End Time	Source IP/Port	Destination IP/Port	Protocol	Severity Level	OT Variable	OT Value	Impact Assessment	Description
e.g.	d-mmm-yy hh:mm:ss	d-mmm-yy hh:mm:ss	IP/Port	IP/Port	TCP, UDP, ICMP, etc.	critical, high, medium, low	-	-	Discovery (Network Enumeration)	-
e.g. 1	15-Aug-24 15:00:00	15-Aug-24 15:00:30	192.168.200.123	192.168.200.234 (HMI)	ICMP	Medium	-	-	Discovery (Network Enumeration)	-
e.g. 2	15-Aug-24 16:00:00	15-Aug-24 16:30:30	192.168.200.123/52112	192.168.200.56/44818	ENIP	High	Valve_1	Open	Damage to property	-

IDS PERFORMANCE ANALYSIS

19 - 27 Sep 2024 (Red Team Execution)

19 - 20 Sep 2024 (Evaluation)

IDS PERFORMANCE ANALYSIS

- Each of the IDS will be evaluated against a set of red team attacks
- OT Attacks that purely affect the processes of the system will be launched during the evaluation
- Reports will be given to the committee live during the execution of the attacks
- Performance will be analysed based on the DRACE metrics
- Evaluation Dates
  - 19 to 20 Sep 2024

Performance Metrics

Score	Components	Readability	Accuracy	Responsiveness	Disruptivity
4	- Identified components attacked. - Identified Source and Destination IP Addresses - Failure type - Reason for Failure	Flesch-Kincaid Score 70.0 - 100.0	- 90.0 - 100.0% Accuracy and 0.0 - 10.0 % False Alarm Rate	- Responds within 5 seconds	- 0% plant downtime
3	- Identified components attacked. - Identified Source and Destination IP Addresses - Failure type	Flesch-Kincaid Score 50.0 - 69.9	- 70.0 - 89.9% Accuracy and 10.1 - 30.0 % False Alarm Rate	- Responds within 30 seconds	- 1-20% plant downtime
2	- Identified all components attacked. - Identified Source and Destination IP Addresses	Flesch-Kincaid Score 30.0 - 49.9	- 30.0 - 49.9% Accuracy and 50.1 - 70.0 % False Alarm Rate	- Responds within 5 minutes	- 21 –50% plant downtime
1	- Identified all components attacked.	Flesch-Kincaid Score 10.0 - 29.9	- 10.0 - 29.9% Accuracy and 70.1 - 90.0 % False Alarm Rate	- Responds within 60 minutes	- 51 – 99% plant downtime
0	- Nothing identified	Flesch-Kincaid Score 0.0 - 9.9	- 0.0 - 9.9% Accuracy and 90.1 - 100.0 % False Alarm Rate	- No response	- 100% plant downtime

COMPONENT IDENTIFICATION

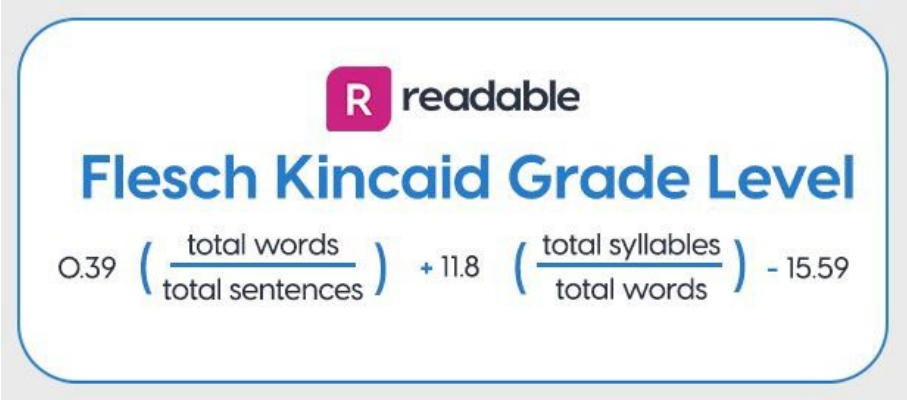
- 4 Points
  - Source and Destination Indicator Identified (1 point)
  - Component Identified (1 point)
  - Failure type (1 point)
  - Reason for Failure (1 point)
- 3 Points
  - Source and Destination Indicator Identified (1 point)
  - Component Identified (1 point)
  - Failure type (1 point)
- 2 Points
  - Source and Destination Indicator Identified (1 point)
  - Component Identified (1 point)
- 1 Point
  - **Source and Destination Indicator** 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)
  - 30.0 - 49.9% Accuracy and 50.1 - 70.0 % False Alarm Rate (2 points)
  - 10.0 - 29.9% Accuracy and 70.1 - 90.0 % False Alarm Rate (1 points)
  - 0.0 - 9.9% Accuracy and 90.1 - 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 5 seconds (4 points)
- Within 30 seconds (3 points)
- Within 5 minutes (2 points)
- Within 60 minutes (1 points)
- Not detected (0 points)

DISRUPTIVITY

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.

Disruptivity 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)

Q&A

THANK YOU