ST Engineering

CSA SINGAPORE | SG Passion Made Possible

OTCEP
2023
OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

22 – 23 AUGUST 2023

Threat Analysis for OT/ICS Environment

Agenda

- Background of Operational Technology (OT)
- Challenges in Defending the OT systems
- Possible Approaches on Enhanced OT Cyber Defence
- Use Case
- Conclusion
- Q&A

Background of Operational Technology (OT)

- The unique characteristics of OT and why OT is so different from the other in multiple dimensions

Operational Requirement Differences

Operational Technology (OT)

Control and safety systems and industrial process assets

Productivity, Safety & Reliability

OT

Machinery
Equipment and Assets
Monitoring Systems
Control Systems

Requirement → Control and Safety System, and Industrial Process Assets

INFORMATION TECHNOLOGY (IT)

Business and enterprise systems that store, process and deliver information

Confidentiality, Availability & Integrity

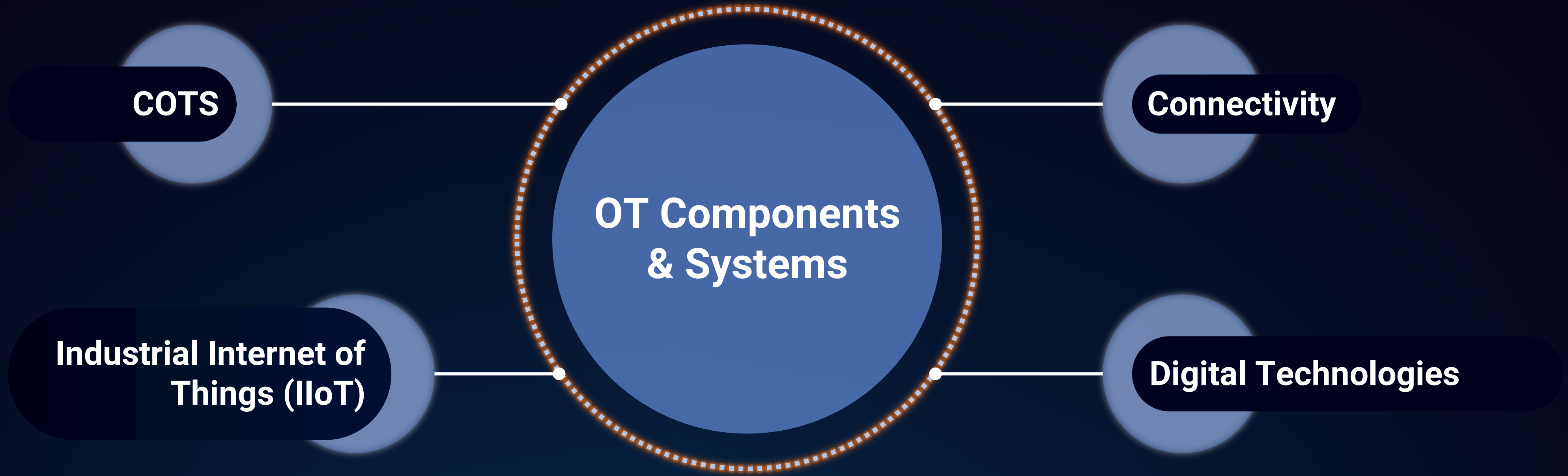
IT

Storage Systems
Computing Technology
Business Applications
Data Analysis

Requirement → Store, Process and Deliver Information

Connectivity with Productivity

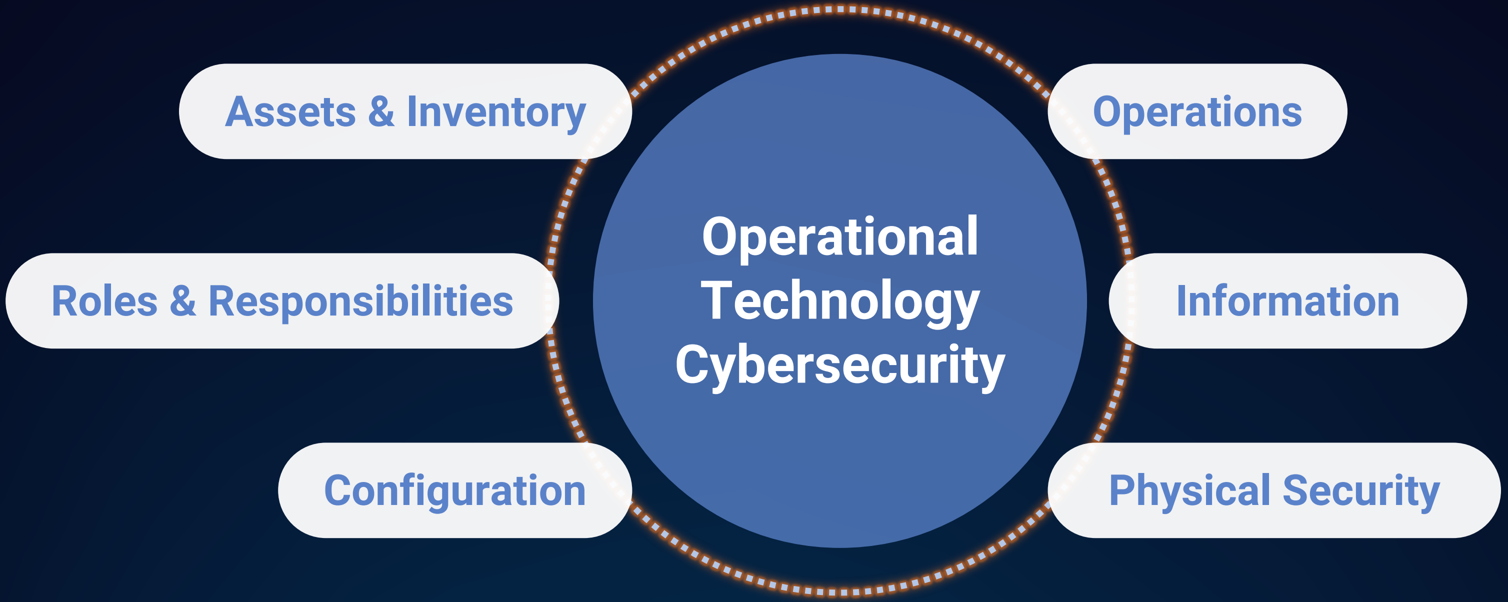
- Where OT elements were once not connected, today you must look hard to find those not on the global space.



Connections and digital technologies, including COTS (commercial-of-the-shelf) assets are gradually getting into the space of control devices and systems.

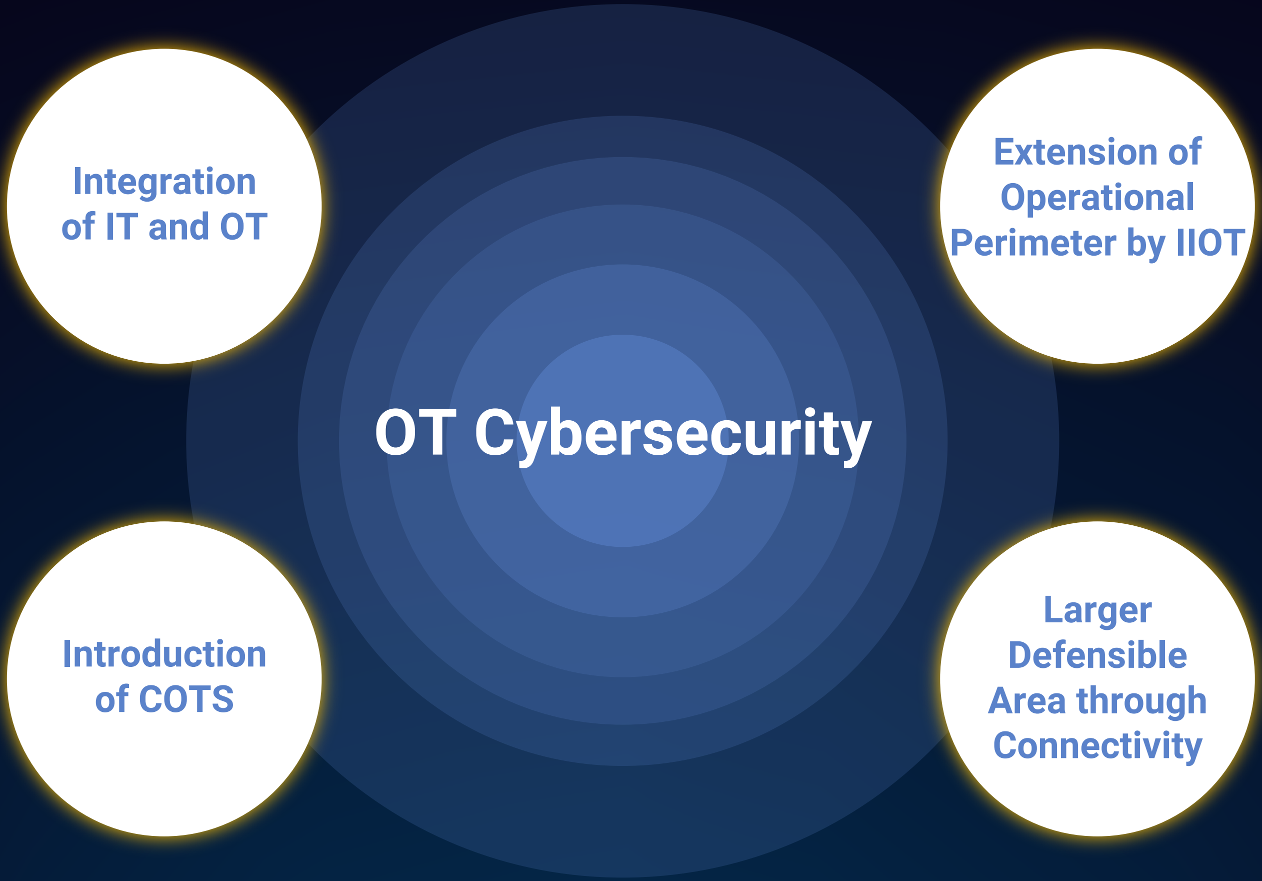
Entanglement between Integration and Segregation

- Challenges arising out from integration of IT and OT, on one hand, justifies for holistic cybersecurity management and, on the other hand, demands clear operational jurisdiction.
- IT was always the domain of the CIO. There are strict differences between IT and OT networks and among people working in these respective areas, from profiles, types of systems to work with, to tasks / priorities.



Complexity with Organic Merging Trend

- Compounding effects of OT, IT, IIOT, COTS and Connectivity in cybersecurity and operational arena



OT Cybersecurity

Integration of IT and OT

Extension of Operational Perimeter by IIOT

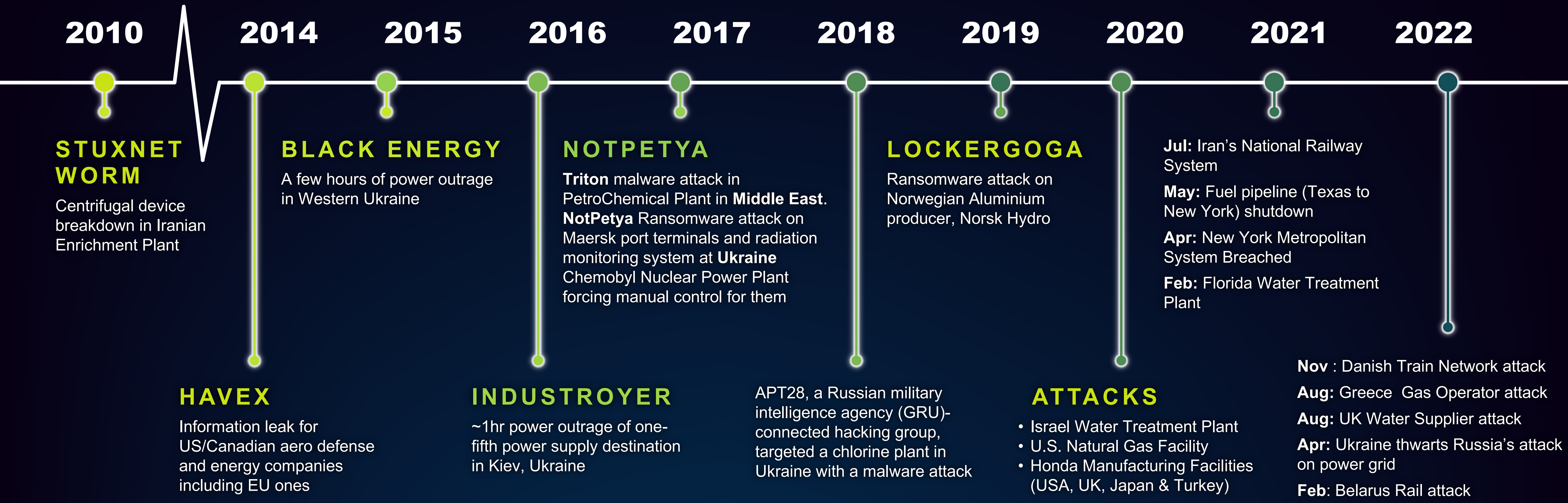
Introduction of COTS

Larger Defensible Area through Connectivity

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

Increasing Cyber Threats – Real & Imminent

- OT System



2010

STUXNET WORM

Centrifugal device breakdown in Iranian Enrichment Plant

2014

HAVEX

Information leak for US/Canadian aero defense and energy companies including EU ones

2015

BLACK ENERGY

A few hours of power outrage in Western Ukraine

2016

INDUSTROYER

~1hr power outrage of one-fifth power supply destination in Kiev, Ukraine

2017

NOTPETYA

Triton malware attack in PetroChemical Plant in **Middle East**. **NotPetya** Ransomware attack on Maersk port terminals and radiation monitoring system at **Ukraine** Chemobyl Nuclear Power Plant forcing manual control for them

2018

APT28, a Russian military intelligence agency (GRU)-connected hacking group, targeted a chlorine plant in Ukraine with a malware attack

2019

LOCKERGOGA

Ransomware attack on Norwegian Aluminium producer, Norsk Hydro

2020

ATTACKS

- Israel Water Treatment Plant
- U.S. Natural Gas Facility
- Honda Manufacturing Facilities (USA, UK, Japan & Turkey)

2021

Jul: Iran's National Railway System

May: Fuel pipeline (Texas to New York) shutdown

Apr: New York Metropolitan System Breached

Feb: Florida Water Treatment Plant

2022

Nov : Danish Train Network attack

Aug: Greece Gas Operator attack

Aug: UK Water Supplier attack

Apr: Ukraine thwarts Russia's attack on power grid

Feb: Belarus Rail attack

Threats Trend to Consider and Likely to Exacerbate

AI-Power Attacks

- **AI – powerful 2023 cybersecurity trend.**
- Cybercriminals **use AI to develop more sophisticated attacks**, e.g. AI-powered malware.

Supply Chain Attacks

- **Cybercriminals target 3rd party vendors and service providers to access customers' systems and data.**
- Increased network of suppliers and partners lowers cost of ownership but increases risk of supply chain attacks.
- It is difficult to detect implantations and manifestations higher up the supply chain.

Threats Trend to Consider and Likely to Exacerbate

Deepfakes and Disinformation

- Deepfakes or AI-generated synthetic media have made headlines for **potential to spread disinformation and deceive the public**.
- **Social engineering attacks to target humans** will be not easy to clearly and quickly identify as the content gets richer and more immersive and **attackers continue doing the harvesting**.

Threats Arising from Insider / Vendor / System Integrator

- **Insider threats will always be non-zero and a significant concern.**
- With prevalence of remote work, it is **challenging to detect and prevent insider threats**.
- Employees with access to sensitive information and systems might have been compromised, without knowing it upfront.

Threats Trend to Consider and Likely to Exacerbate

5G and IoT Security Challenges

- **2025 – approximately 25 billion IoT connections globally, increasing the threat of large-scale DDoS botnet attacks:**
  - Companies have many different kinds of IoT technologies being connected to their network and these devices also use a wide range of communications protocols, increasing the risks of threats.
  - These IoT devices also lack built-in and vigorous security measures.
- **Quick 5G technology adoption leads to convenience and efficiency in the increased number of IoT devices, while presenting a new frontier of cybercriminals:**
  - The Internet of Things (IoT) will be even more significant in daily operations.
  - With the combination of COTS, 5G, Industrial IoT and OT, the entire spectrum of point of entry for attackers has just exploded, especially with benefits of lower cost of wireless adoption and deployment scores.

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

APJ Projection by Mandiant 2023

Elevated Threat Levels and Disruptions to Semiconductor Manufacturers in Asia Pacific

- Critical manufacturing sector, e.g. semiconductor industry, is frequently targeted by ransomware.
- Semiconductor producers more likely to pay ransoms to prevent monetary losses from production downtime or large-scale work stoppages.

Asia Pacific Countries Could See More Retaliatory Attacks by Pro-Russia Hacktivist Groups

- Due to multiple Asia Pacific countries sanctions on Russia.
- Recent targeting of organisations represents a significant escalation and expansion in targeting.
- Asia Pacific-based organisations should prepare themselves for such attacks.

Reference: https://d110erj175o600.cloudfront.net/wp-content/uploads/2022/11/02144954/Mandiant-2023-Forecast-Report.pdf

Challenges in Defending the OT System and Network

Defending an OT system and networks requires different understanding and background compared to the traditional IT.

- What are these challenges?
- What kind of attention are warranted from our business stakeholders?

Some Pain Points in OT Environment

- VAPT are manual, tedious and based on Interview
- Unable to map out threats to assets effectively
- Information gap between ICS (OT) and Cybersecurity staff
- Threat intel from various sectors and domains not relevant to sector & region
- Determining and aligning business processes
- Adhering to IEC62443 Standards and Compliance
- Adhering to CSA CCoP 2.0 Compliance

Challenges in Defending the OT Systems and Network

Complication and Propagation Effects from Unsecure and Outdated OT Devices, Systems and Networks

- **Legacy software and systems** with insufficient security protection.
- **Unpatched or out-of-date systems** can be worsened by end-of-life and end-of-support conditions.
- **Operational system that could not be patched** might become a time bomb.

Underestimation of Synergistic Power of Over-Arching Visibility with Respect to Depth and Breadth of Scope

- Multiple cybersecurity products **working in isolation**.
- **Limited visibility** in terms of health and entities from the network which can be aggravated by large geographical area.

Challenges in Defending the OT Systems and Network

Essential Combination and Reinforcement of Administrative, Physical and Technical Controls for an Effective Outcome to Business

- **Careful reorganisation and remodelling** for a seamless exchange of control and information between OT and IT systems is required but lacking
- **Inappropriate business case**, justifying for OT security with emphasis on ROI

Prolific Nature of Malicious Behaviours

- **More malwares in different forms and nature** due to widespread usage of shared codes and tools.
- **Non-ICS malware such as ransomware and cryptoware add more pressure** to the defences.
- **Well-liked and common ground culture of default credentials and account**, including hard-coded passwords, and **adoption of sub-par OEM products** aided in the elevation of the situation.

Possible Approaches on Enhanced OT Cyber Defence

What are threats that businesses are facing and how businesses could potentially resolve them appropriately?

Targeting Different Types of OT Threat Alert

Threat #1

Arising from misconfiguration and assets placement

Threat #2

Arising from modelling / machine learning anomalies

Threat #3

Arising from engineering faults / SCADA indicators

Threat #4

Arising from behavioural analytics anomalies

OT Security Solution Strategy

Level 0

Signal Monitoring

Level 1~4

Process Monitoring

Anomalies and Alerts

Process, logs and Behaviour Analysis

Process Digital Twin

Breach & Attack Simulation

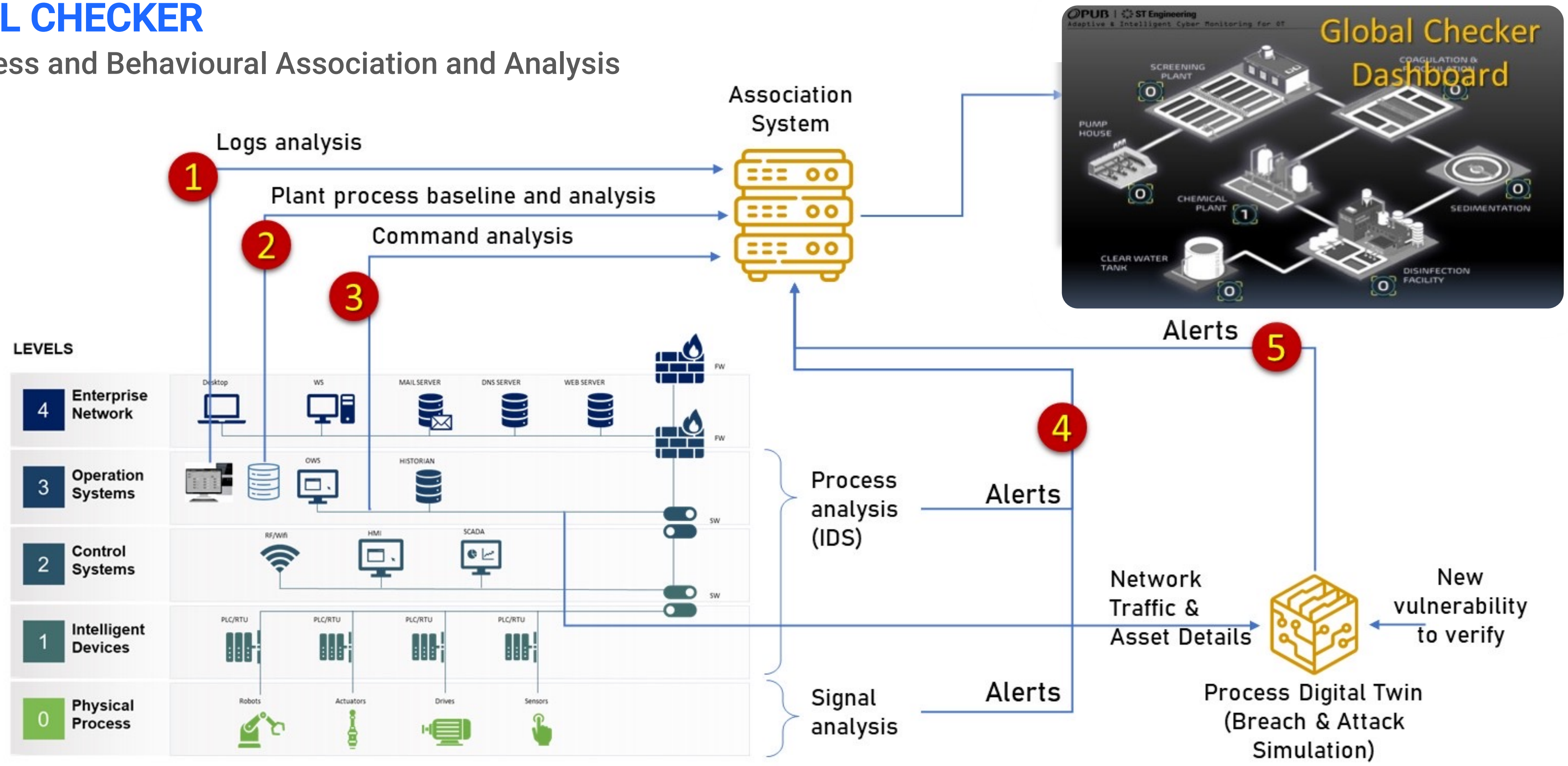
Global Checker

ICS Process and Behavioural Association and Analysis

ICS Process and Behavioral Association / Correlation and Analysis

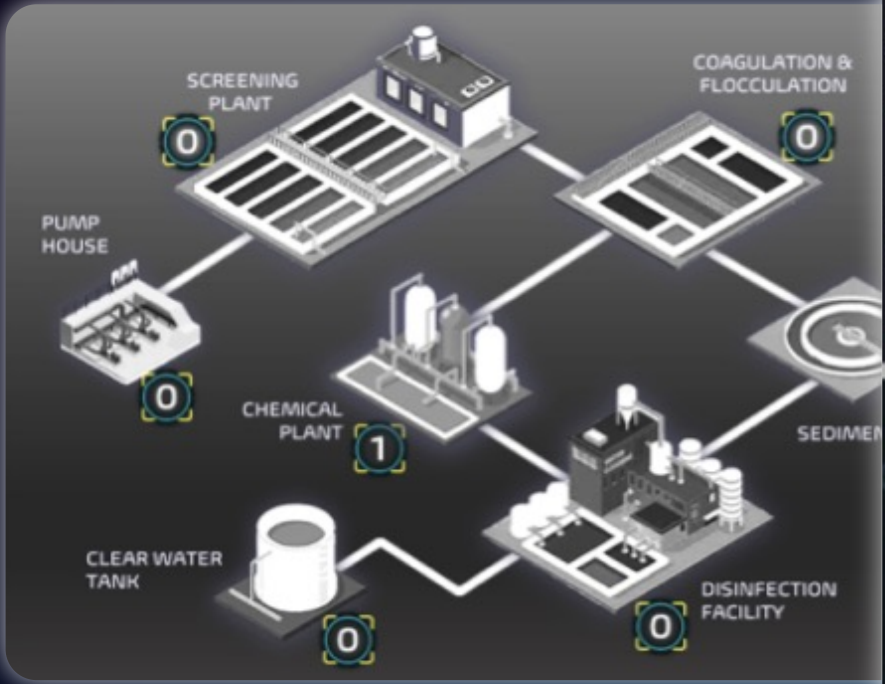
GLOBAL CHECKER

ICS Process and Behavioural Association and Analysis

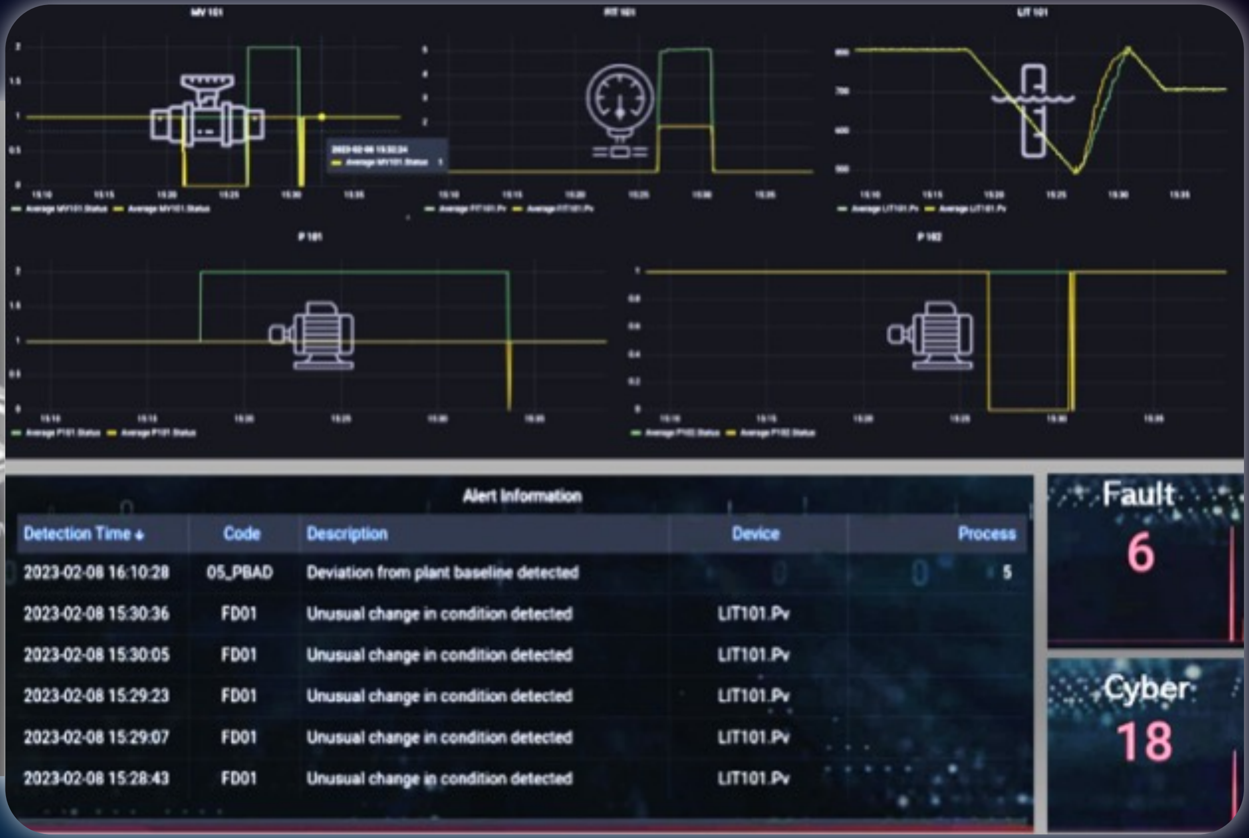


ICS Process and Behavioral Association / Correlation and Analysis

DASHBOARD
(Overall Process)



DASHBOARD
(Sensor & Actuator)

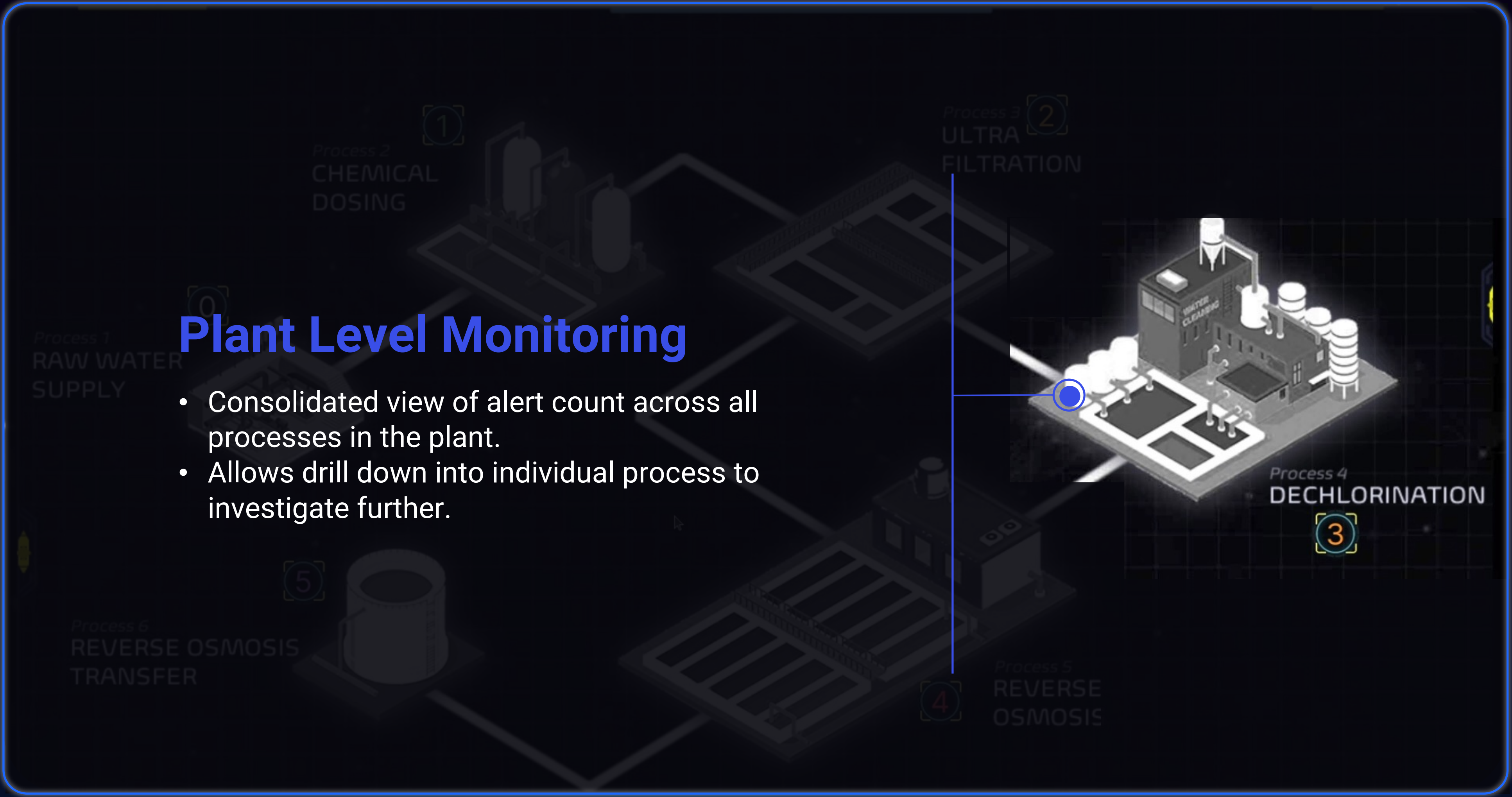


Alert Information

Detection Time ↓	Code	Description	Device	Process
2023-02-08 16:10:28	05_PBAD	Deviation from plant baseline detected		5
2023-02-08 15:30:36	FD01	Unusual change in condition detected	LIT101.Pv	
2023-02-08 15:30:05	FD01	Unusual change in condition detected	LIT101.Pv	
2023-02-08 15:29:23	FD01	Unusual change in condition detected	LIT101.Pv	
2023-02-08 15:29:07	FD01	Unusual change in condition detected	LIT101.Pv	
2023-02-08 15:28:43	FD01	Unusual change in condition detected	LIT101.Pv	

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

Plant Monitoring (Overview)

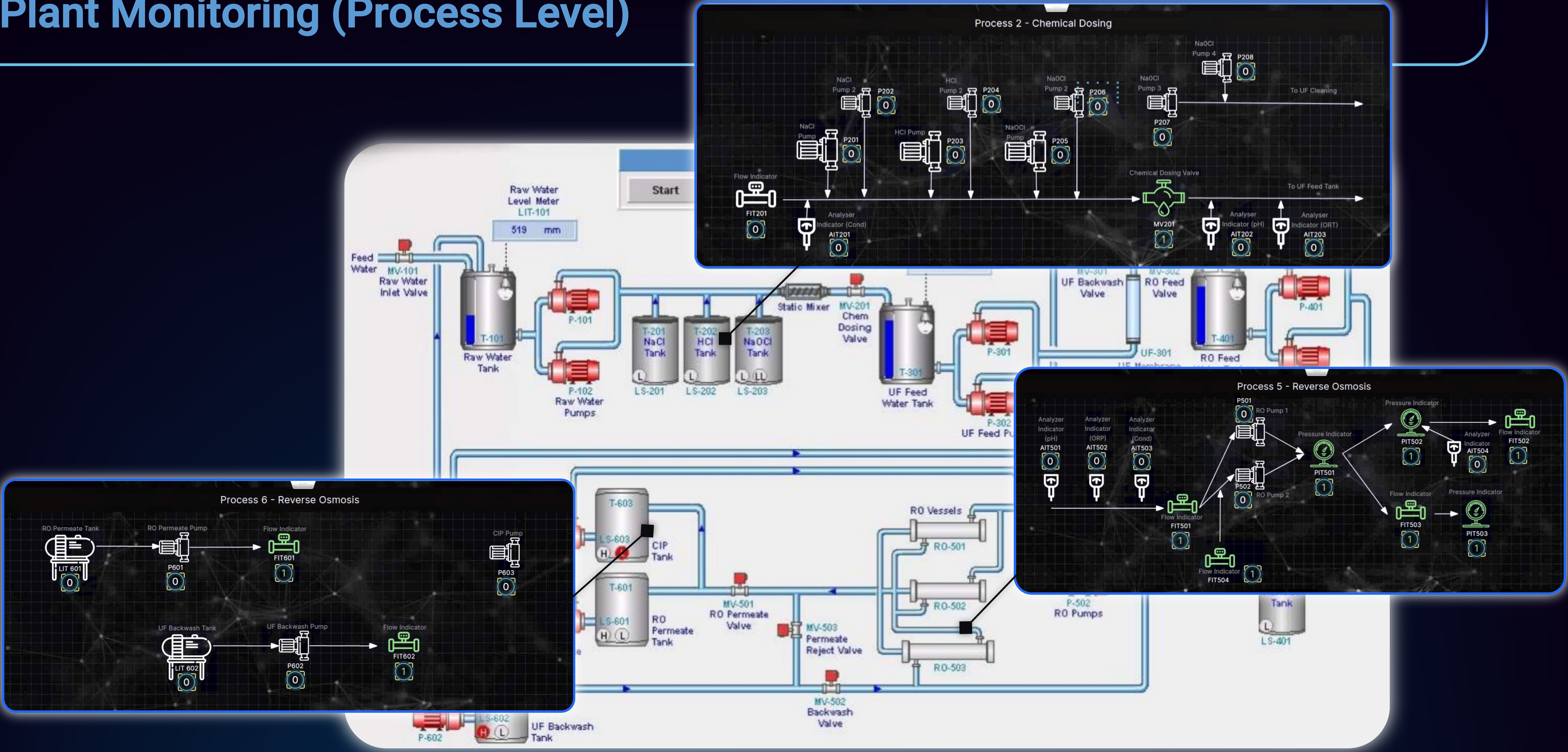


Plant Level Monitoring

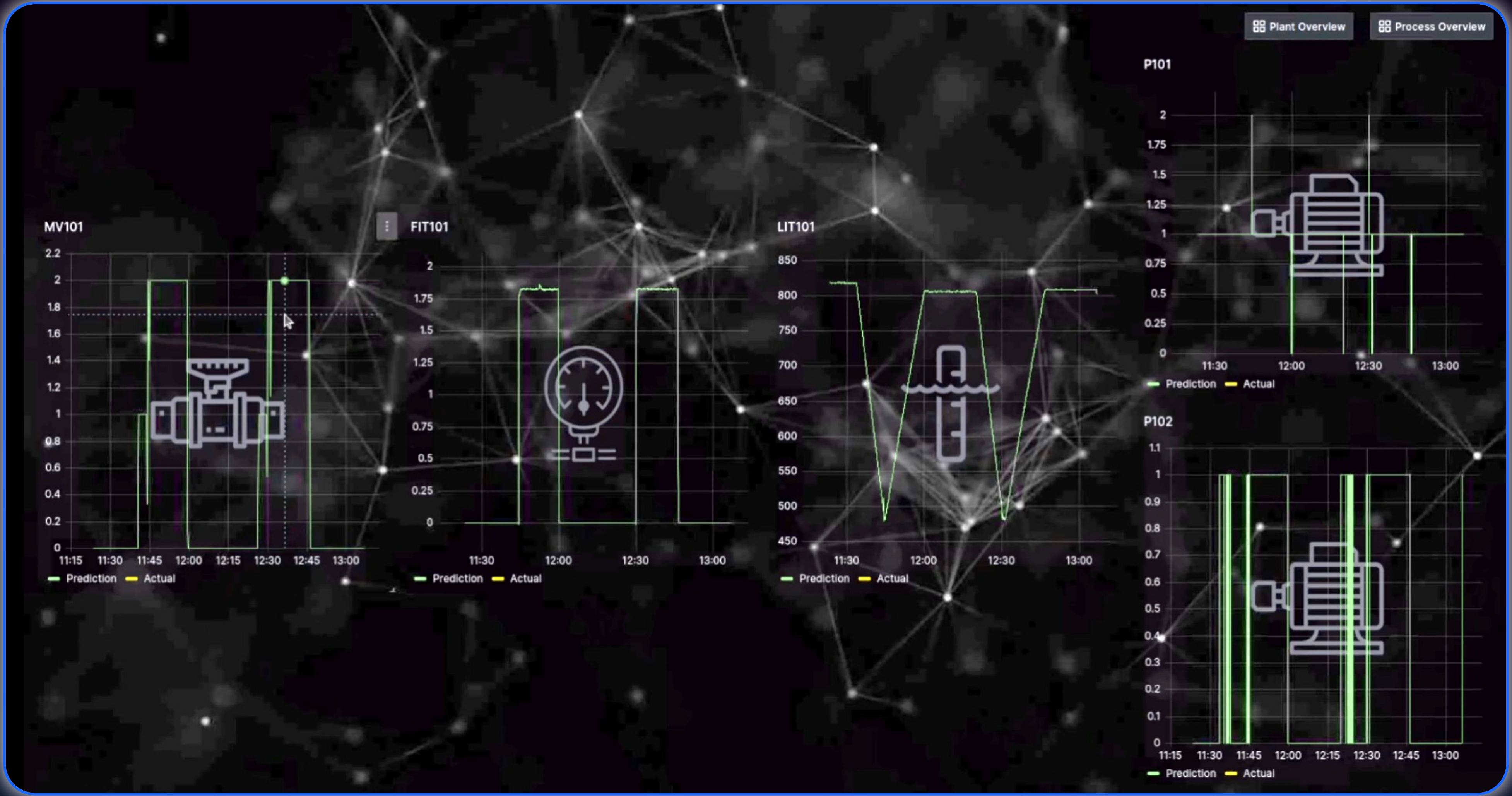
- Consolidated view of alert count across all processes in the plant.
- Allows drill down into individual process to investigate further.

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

Plant Monitoring (Process Level)



Sensor Monitoring

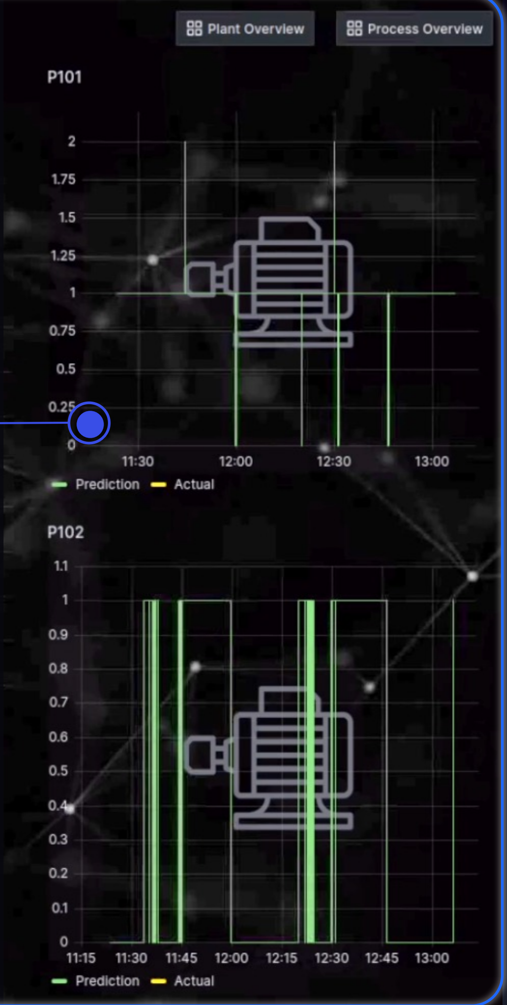


OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

Sensor Monitoring

Sensor Level Monitoring

- Provides real-time and historical view of sensor telemetry.
- It visualises readings predicted by the models as well as the actual, allowing operator to quickly identify any deviation.



Attack Simulation based on Digital Twin

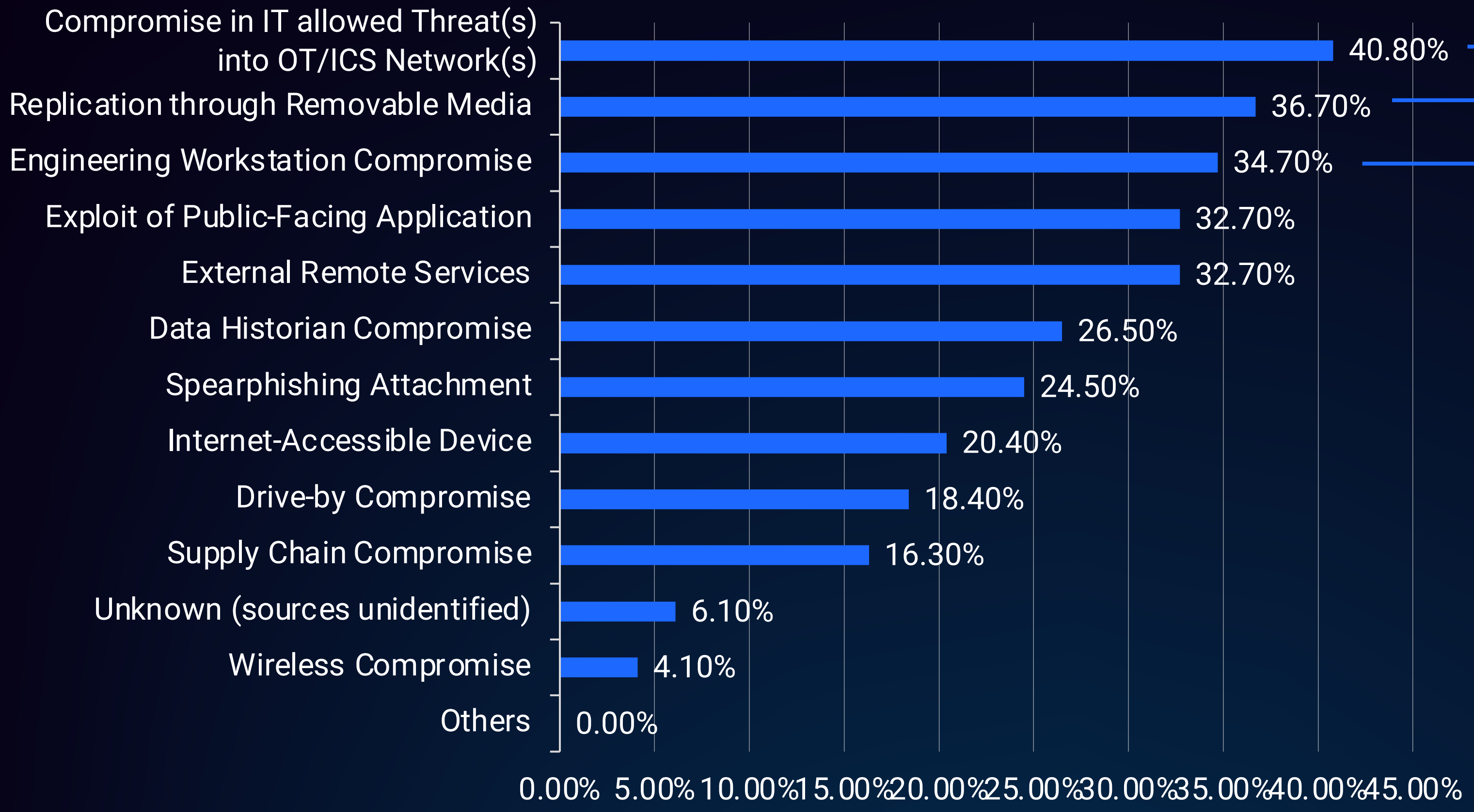
OTCEP
2023
OPERATIONAL TECHNOLOGY
CYBERSECURITY EXPERT PANEL FORUM 2023

Use Case

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

Point of Entry

Attack Vectors involved in OT / Control systems



1 **Compromise in IT,** allowing threats into the ICS / OT control networks

2 Risk of threats through **removable media** (USBs, external hard drives, etc.)

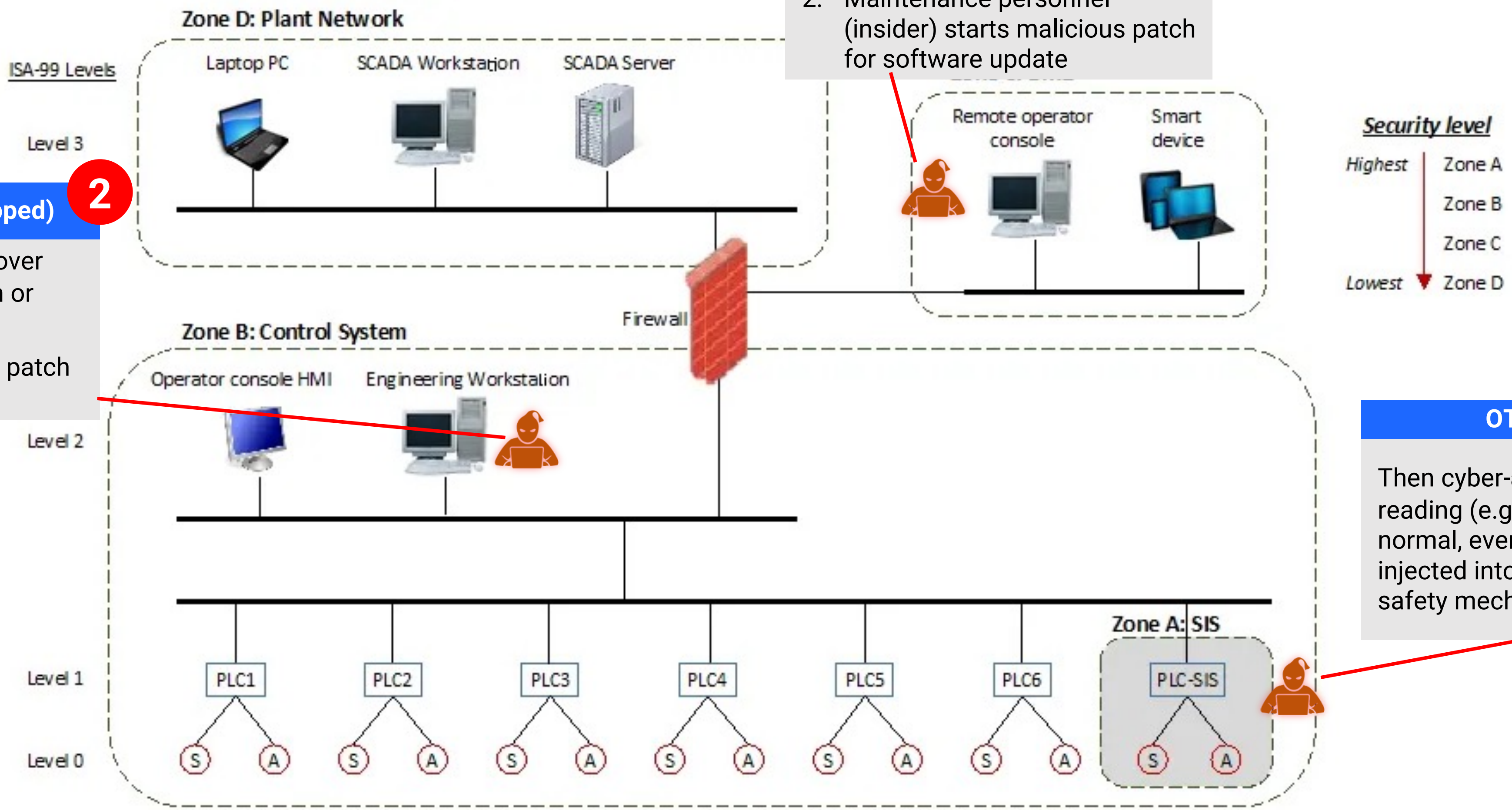
3 **Engineering workstations** used to program or change logic controllers

ATTRIBUTION

1. Malicious intent
2. Human error
3. Account compromise (phishing emails, leaked passwords, etc.)

Source: https://www.nozominetworks.com/downloads/US/SANS-Survey-2022-OT-ICS-Cybersecurity-Nozomi-Networks.pdf

OT Cyber-Attack scenarios



1

IT Environment

1. Remote attacker takes over engineering workstation or
2. Maintenance personnel (insider) starts malicious patch for software update

2

OT Environment (Air Gapped)

1. Remote attacker takes over engineering workstation or
2. Maintenance personnel (insider) start malicious patch for software update

3

OT Environment

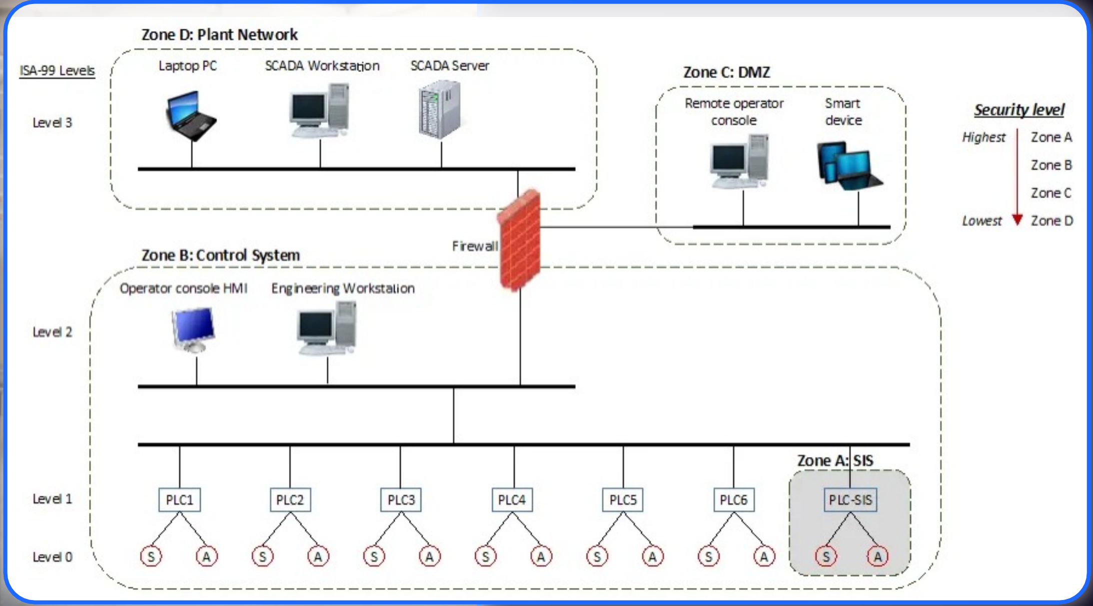
Then cyber-attacker spoof sensors reading (e.g. chemical) to be normal, even when chemicals are injected into the water. (Bypass safety mechanisms)

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

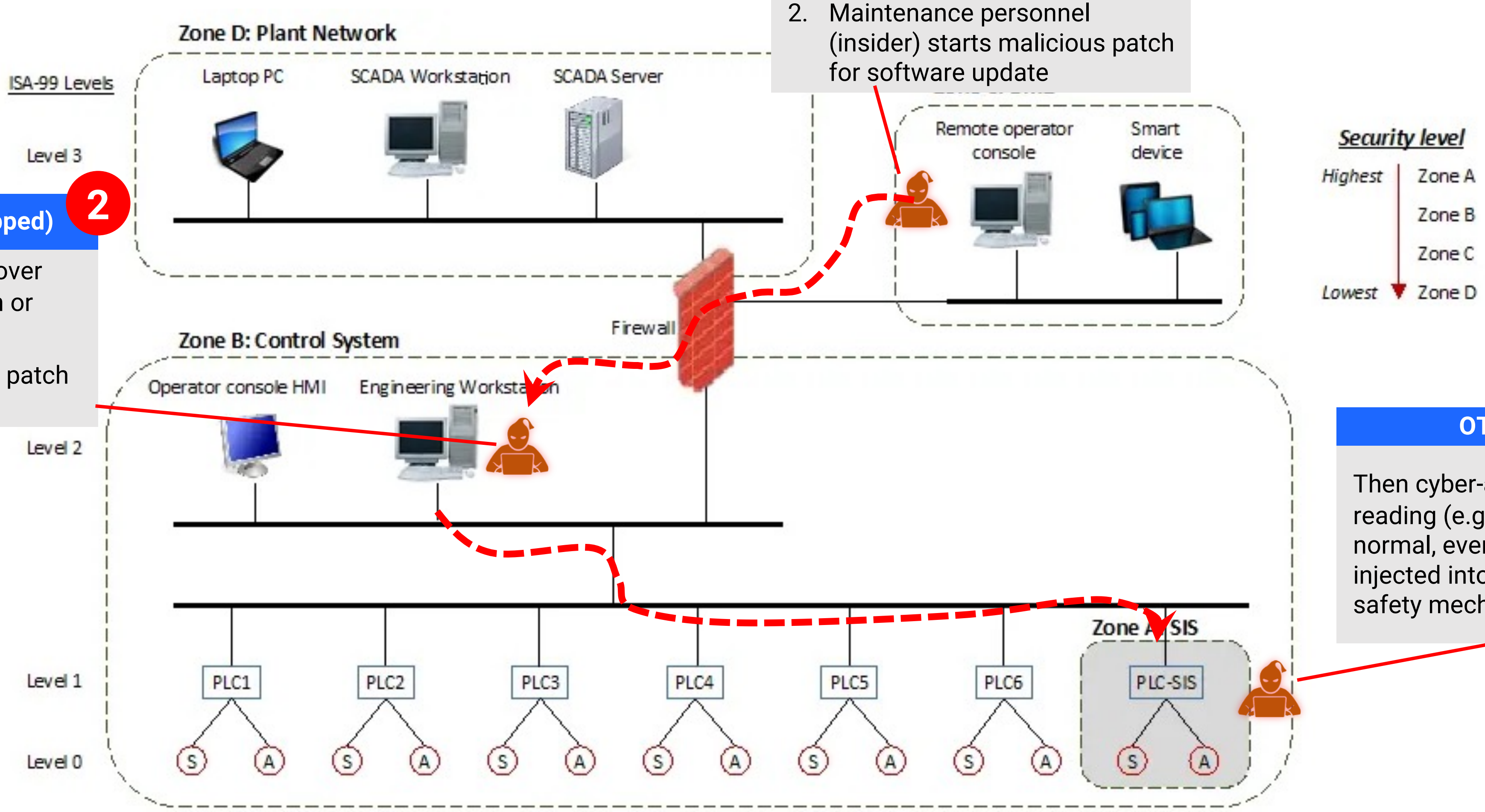
OT Cyber-Attack scenarios

Funded by the Singapore Government

5-gallons/min and 6-stages operational water treatment testbed located at SUTD



OT Cyber-Attack scenarios



IT Environment 1

1. Remote attacker takes over engineering workstation or
2. Maintenance personnel (insider) starts malicious patch for software update

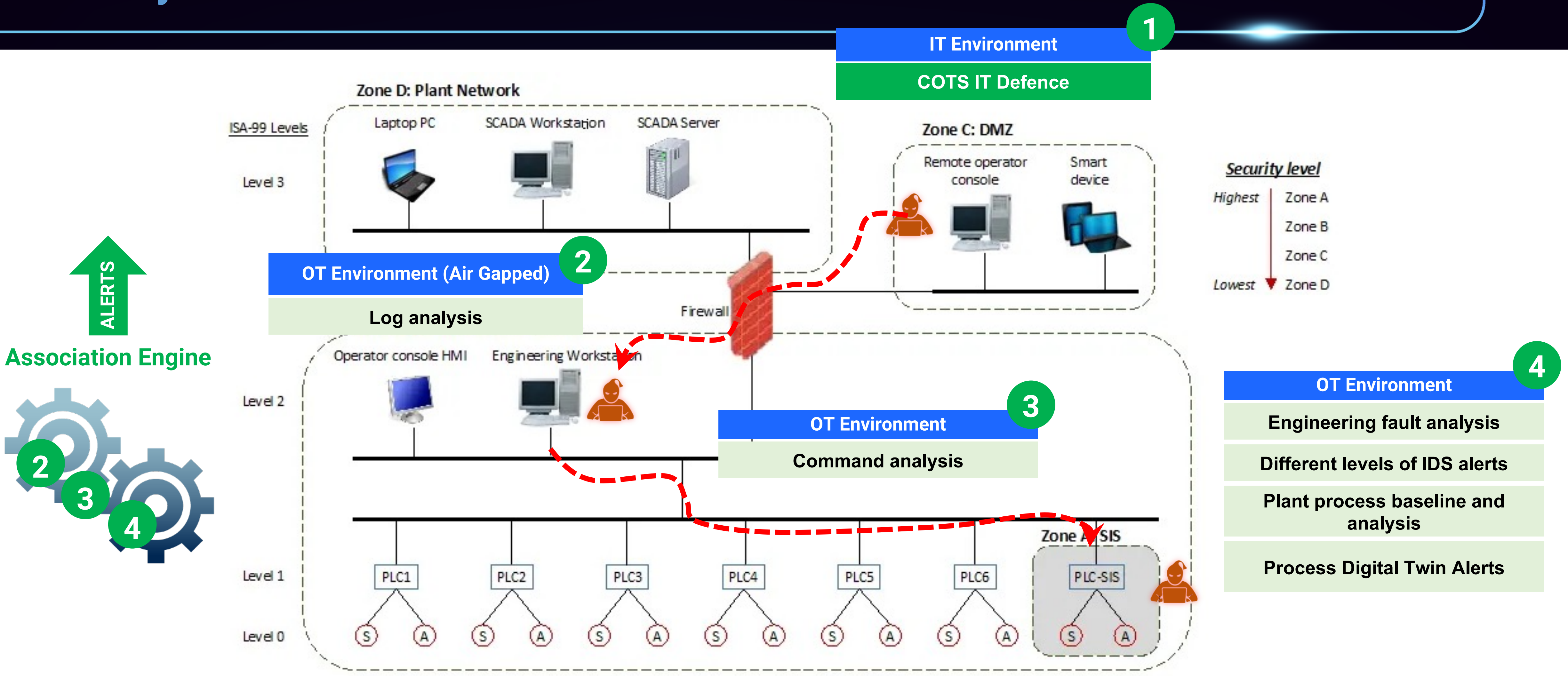
OT Environment (Air Gapped) 2

1. Remote attacker takes over engineering workstation or
2. Maintenance personnel (insider) start malicious patch for software update

OT Environment 3

Then cyber-attacker spoof sensors reading (e.g. chemical) to be normal, even when chemicals are injected into the water. (Bypass safety mechanisms)

OT Cyber-Attack scenarios



1 IT Environment

COTS IT Defence

2 OT Environment (Air Gapped)

Log analysis

3 OT Environment

Command analysis

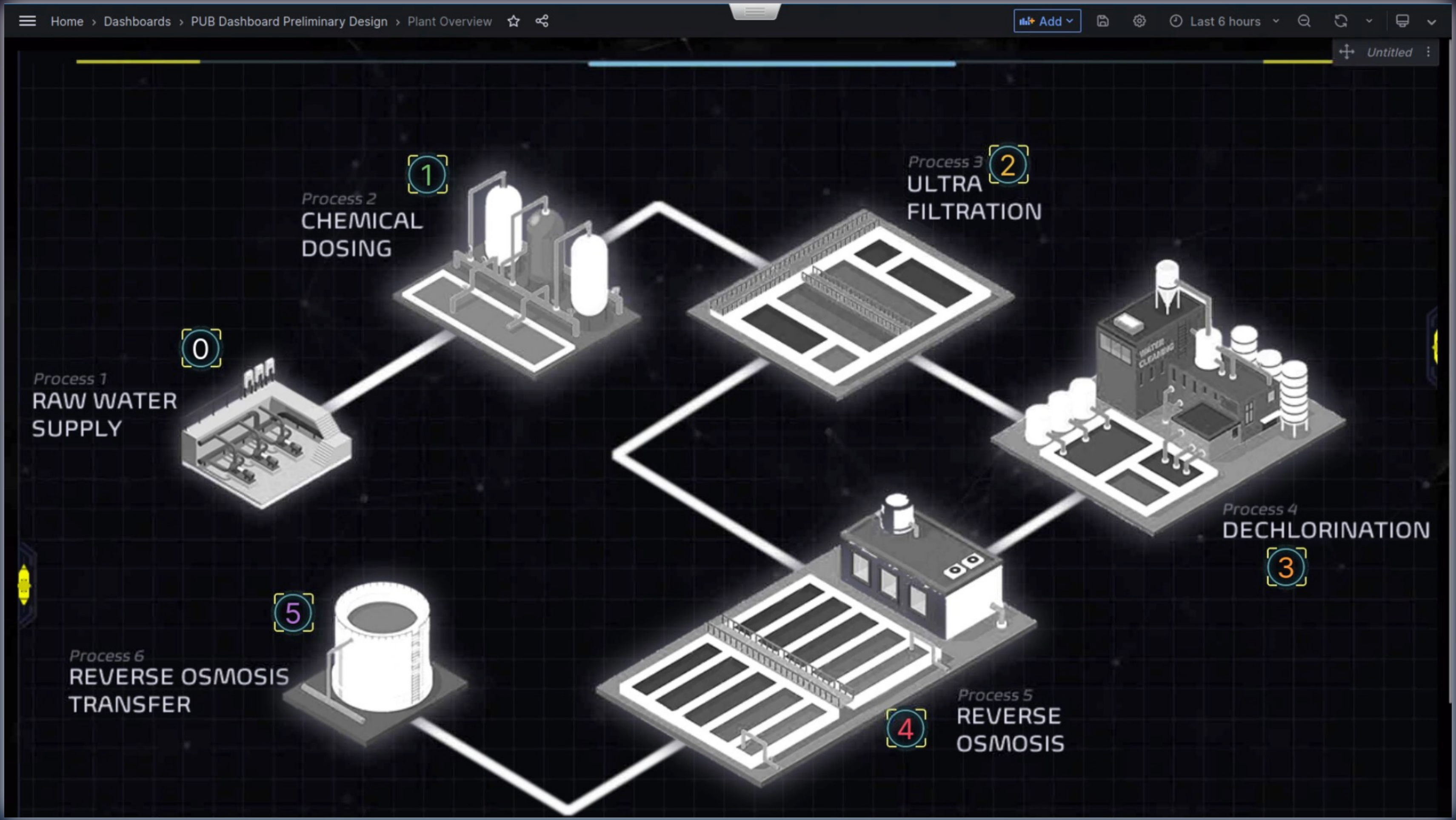
4 OT Environment

- Engineering fault analysis
- Different levels of IDS alerts
- Plant process baseline and analysis
- Process Digital Twin Alerts

Association Engine

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

Dashboard for OT Cyber Attack scenarios



Conclusion

Increased Complexity in Defending OT Networks against Cyber-Attacks

- Due to digitalisation of OT Networks which also increases operational efficiency.

Anomalies Detected Mainly due to Network Malfunction or Cybersecurity Incident

- Further investigation will be required in order to draw a conclusion.

Proactive Assessment and Identification of Live OT Network Required to Fix Vulnerabilities

- Can be achieved by leveraging on Digital Twin and Simulation.

OT NETWORK LIKELY TO BE THE NEXT BATTLE GROUND

- Due to IT security is becoming more matured.

ST Engineering

Thank You

Dr. LIM Woo Lip

CTO, Cyber
ST Engineering

✉ woolip.lim@stengg.com