解碼智慧變電站通訊：
從架構設計到工業資安防護實踐攻略

余浩宇 Tony Yu

Moxa亞太區市場事業處應用工程技術主任

April 2025

Agenda

- **Taiwan Power/Energy Market Overview**
  電力能源產業概況
- **Key Factors of Power Network Resilience**
  強韌電力通訊網路的關鍵
- **Communication Network Resilience for Power Substation**
  變電站系統通訊與安全
- **Bridge the Network Security Gap**
  電力通訊安全強化之道

電力能源

強韌電網計畫與能源轉型加速推動

- 持續投入**強韌電網**
  - 智慧電網升級，變電站自動化、饋線自動化持續佈建
  - 從實體線路到數位化，**網路可視化**管理軟體需求攀升
  - **資安風險**帶動安全的設備需求提升

- 能源轉型加速推動
  - 再生能源來源分散/環境嚴苛，**強固設備**需求攀升
  - 再生能源與儲能併網、**監控需求擴增**
  - 電動車開始衝量，EVI 佈建加速**減緩電網衝擊需求**浮現

Key Factors of Power Network Resilience
強韌電力通訊網路的三個關鍵

- 通訊可靠性 (Reliability)
  - 強固通訊設備與設備監控
  - 提升網路可靠度
- 資訊安全 (Cybersecurity)
  - 系統設計規劃
  - 資安產品、防護措施導入
- 可視化 (Visibility)
  - 網路管理軟體導入
  - IT資安系統整合

MOXA

Communication Network Resilience for Power Substation

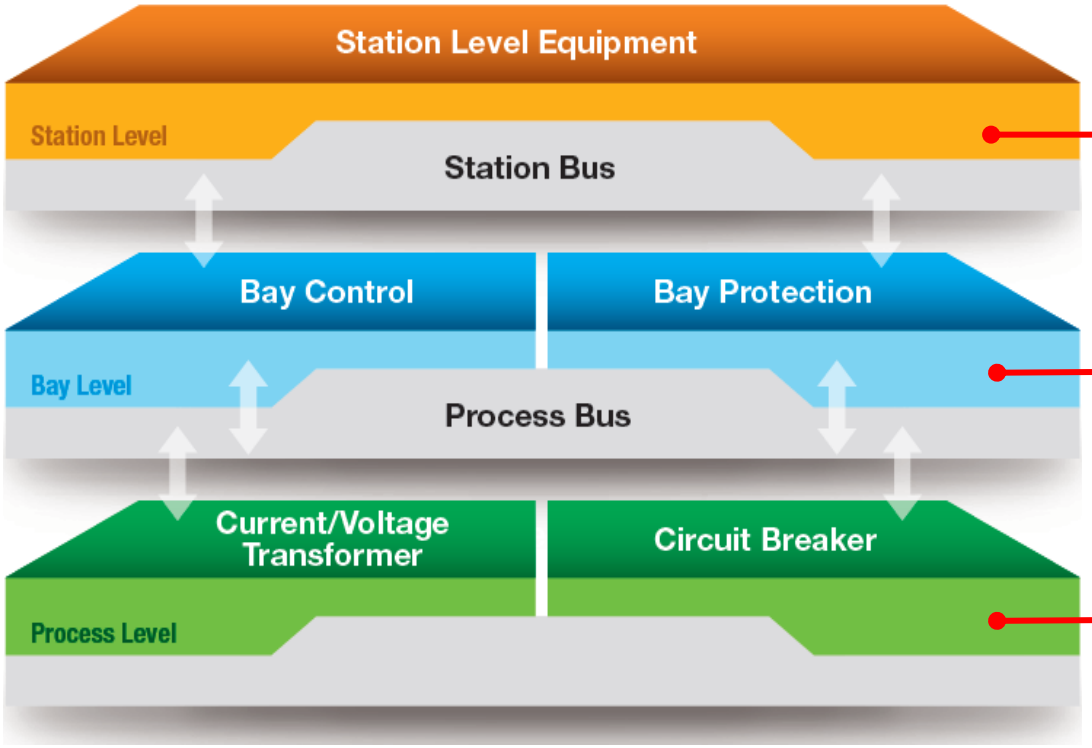
IEC 61850 Ed. 2.0

Communication networks and systems for power utility automation

General	-1	Introduction & overview
	-2	Glossary
Requirements	-3	General requirement
	-4	System & project management
	-5	Communication requirements for functions and device models
Configuration	-6	Configuration description language for communication in electrical substations related to IEDs
Data models	-7-1	Basic communication structure for substation and feeder equipment – Principles and models
	-7-2	Basic information and communication structure – Abstract communication service interface
	-7-3	Basic communication structure – Common data classes
	-7-4	Basic communication structure – Compatible logical node classes and data classes
Protocols	-8-1	Specific communication service mapping (SCSM) – Mappings to MMS and to ISO/IEC 8802-3
	-9-1	Specific communication service mapping (SCSM) – Sampled values over serial unidirectional multidrop point to point link
	-9-2	Specific communication service mapping (SCSM) – Sampled values over ISO/IEC 8802-3
	-9-3	Precision time protocol profile for power utility automation
Testing	-10	Conformance testing

IEC 61850 Substation Architecture

3 Levels & 2 Communication Buses

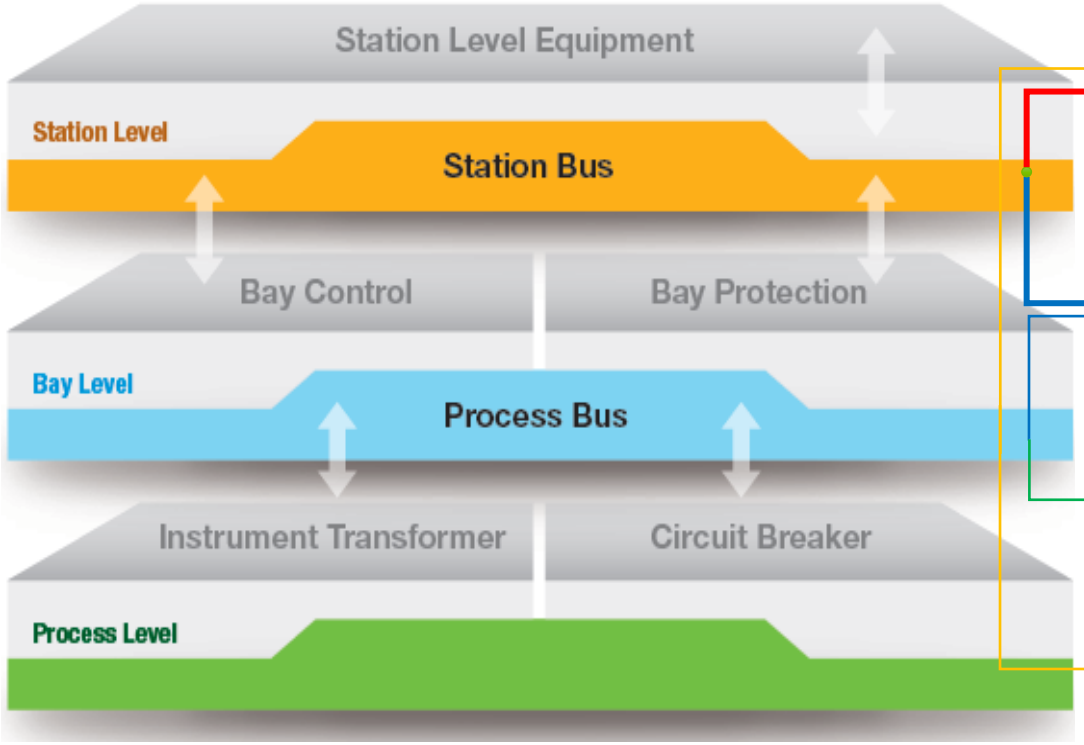


Power SCADA
Management & Monitoring

IED
Protection & Control

Merging Unit or Control Unit
Data acquisition and
Circuit breaking

IEC 61850 Communication Protocol



MMS:
Status monitoring and management

GOOSE:
Status update and send control command

SMV:
power line current and voltage value report

PTP:
Time synchronization to properly detect error sequence

MMS: Manufacturing Messaging Specification
GOOSE: Generic Object Oriented Substation Event
SMV: Sampled Values
PTP: Precision Time Protocol

Timing Requirement in Substation Networks

Communicating Partners	Service	Application Recovery Tolerated Delay	Required Communication Recovery Time
SCADA to IED, Client-server	IEC 61850-8-1	800ms	400ms
IED to IED interlocking	IEC 61850-8-1	12ms (with Tmin set to 4ms)	4ms
IED to IED, reserve blocking	IEC 61850-8-1	12ms (with Tmin set to 4ms)	4ms
Protection trip excluding Bus Bar protection	IEC 61850-8-1	8ms	4ms
Bus Bar protection	IEC 61850-9-2 on station bus	< 1ms	Bumpless (0ms)
Sampled Values (SMV)	IEC 61850-9-2 on process bus	Less then two consecutive samples	Bumpless (0ms)

Station bus

Process bus

Ref. IEC 61850-5

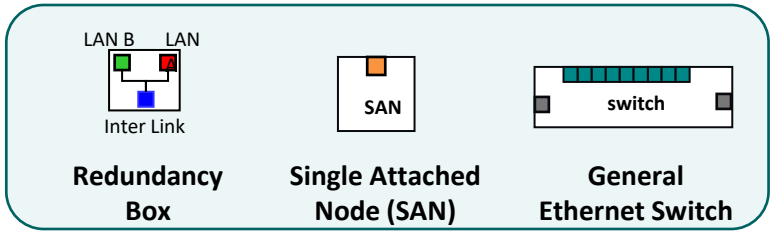
IEC 62439 Standard Redundancy in Industrial Ethernet

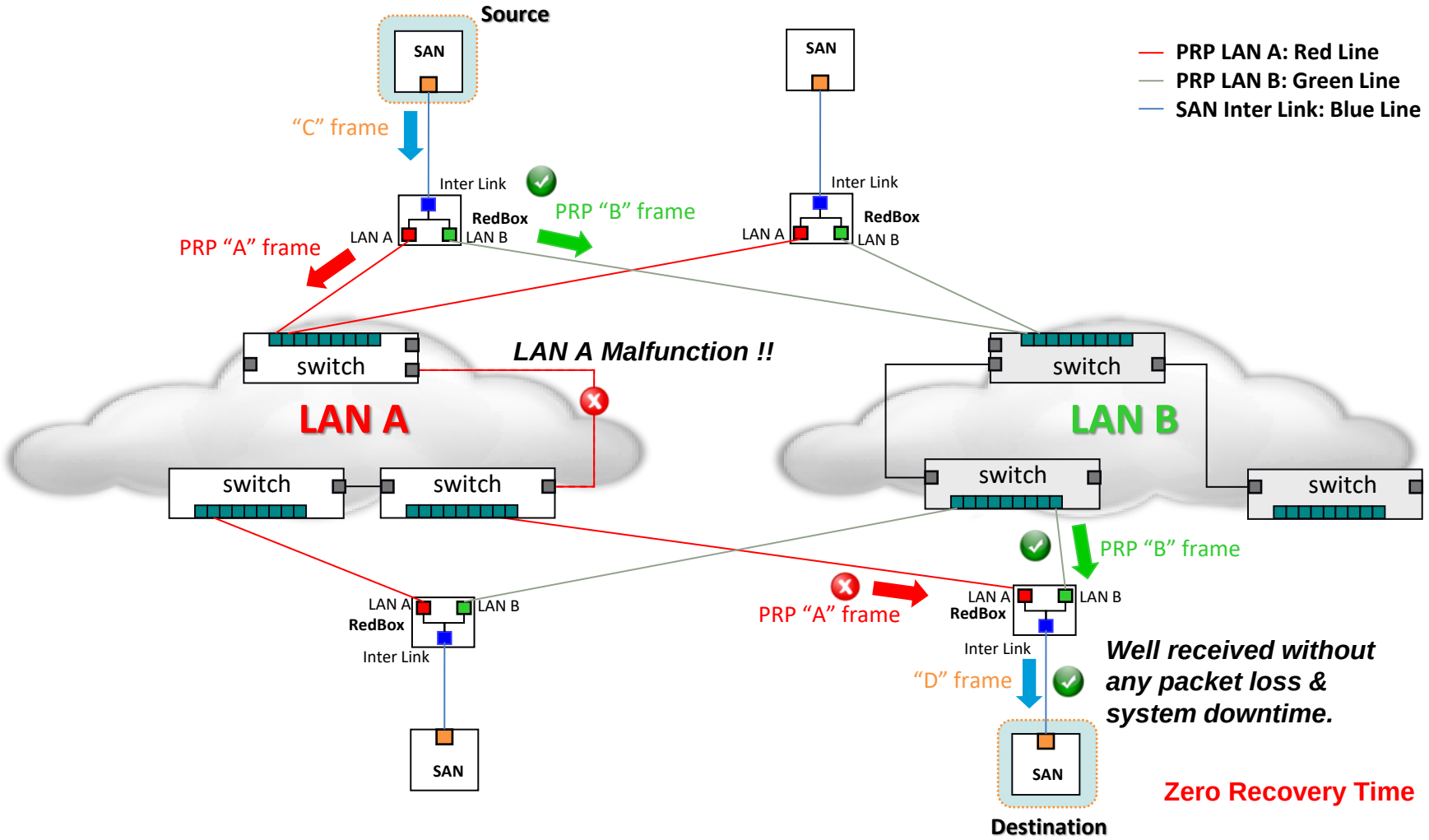
IEC 62439-1	defines the terms specifies how to calculate the reliability and availability specifies how to calculate the recovery time of **RSTP** (IEEE 802.2d)
IEC 62439-2	**MRP** (Media Redundancy Protocol), the Profinet ring protocol
IEC 62439-3	Two seamless protocols (**no recovery time**) **PRP** (Parallel Redundancy Protocol) **HSR** (High-availability, Seamless Redundancy)
IEC 62439-4	**CRP** (coupled redundancy protocol)
IEC 62439-5	**BRP**, similar to CRP
IEC 62439-6	**DRP** (Distributed Redundancy Protocol), similar to MRP and including a clock synchronization
IEC 62439-7	**RRP** (in preparation) another ring redundancy protocol

只有PRP與HSR支援零秒備援

PRP Operation

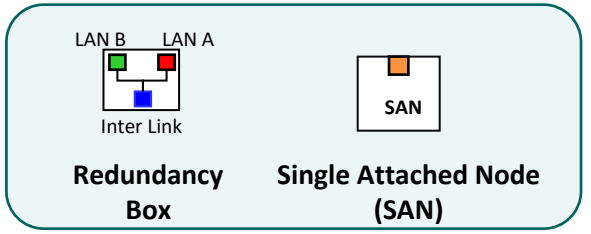
To transmit or receive two independent active paths to/from different LANs simultaneously in a zero-recovery time network

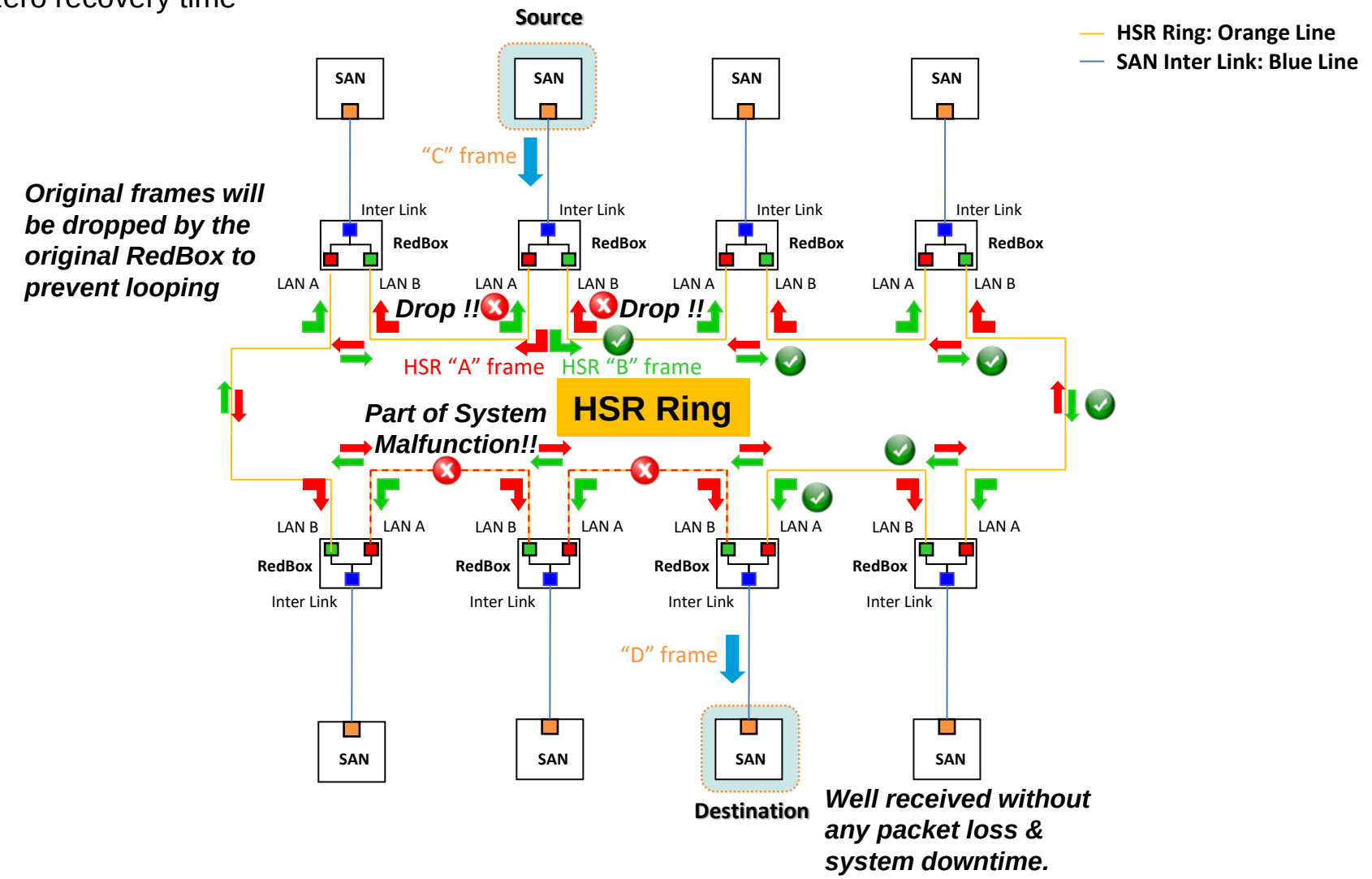




HSR Operation

Every frame is duplicated and then transmitted in both directions of the HSR ring to deliver zero recovery time





Power Substation Cybersecurity Challenges & Requirements

- **Challenge**
  - Asset management (資產管理)
  - Application recovery tolerated delay (通訊延遲要求)
- **Requirement**
  - Visualize communication status
  - Detect & response cyberattacks

Global Cybersecurity Initiatives Geared Towards Critical Infrastructure

- NERC Reliability Standard
- NIST Cybersecurity Framework (CSF) 2.0

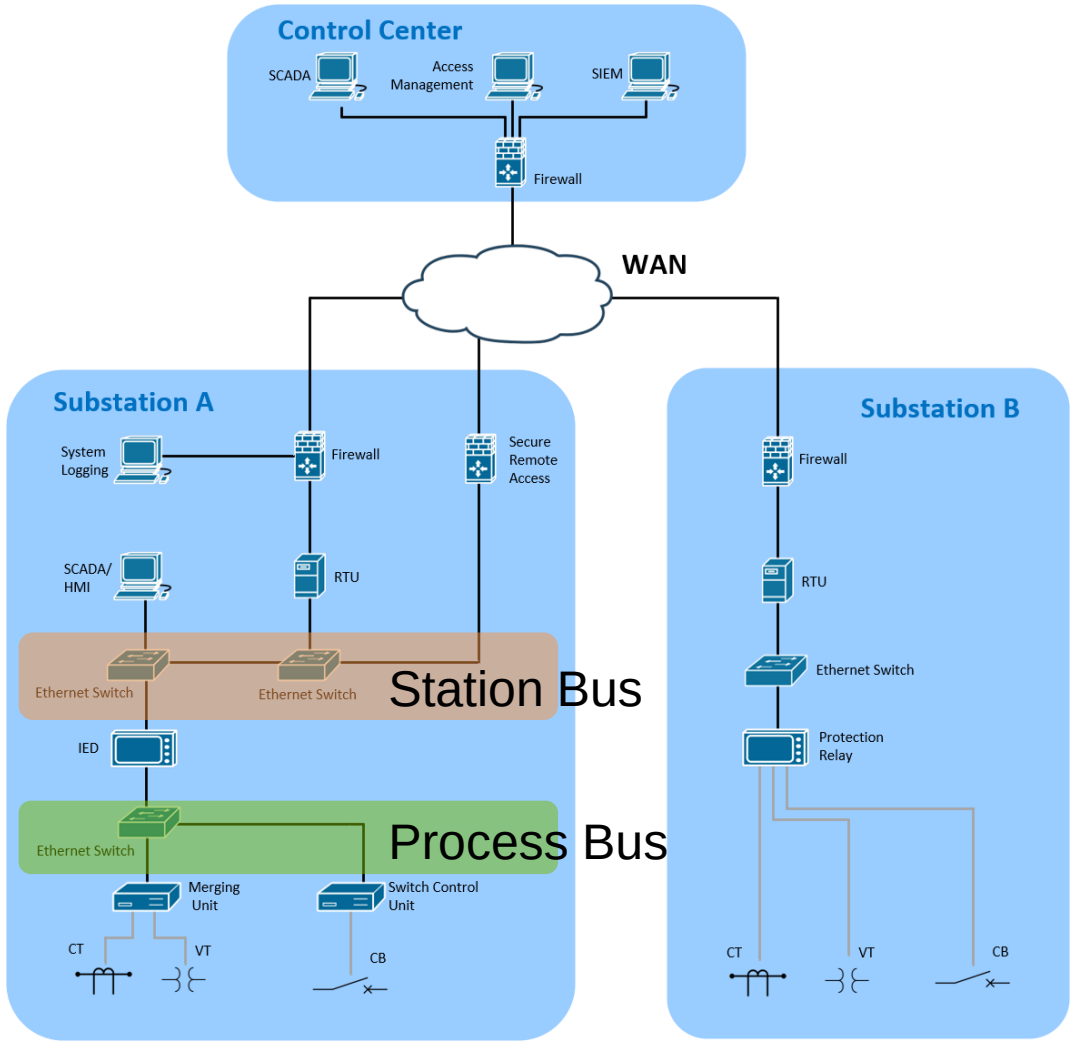
- NIS2 Directive
- CRA
- IEC 62351

- Cybersecurity Management Guidelines Ver. 3.0
- Guideline for Establishing Safety Principles for Ensuring Cybersecurity of Critical Infrastructure

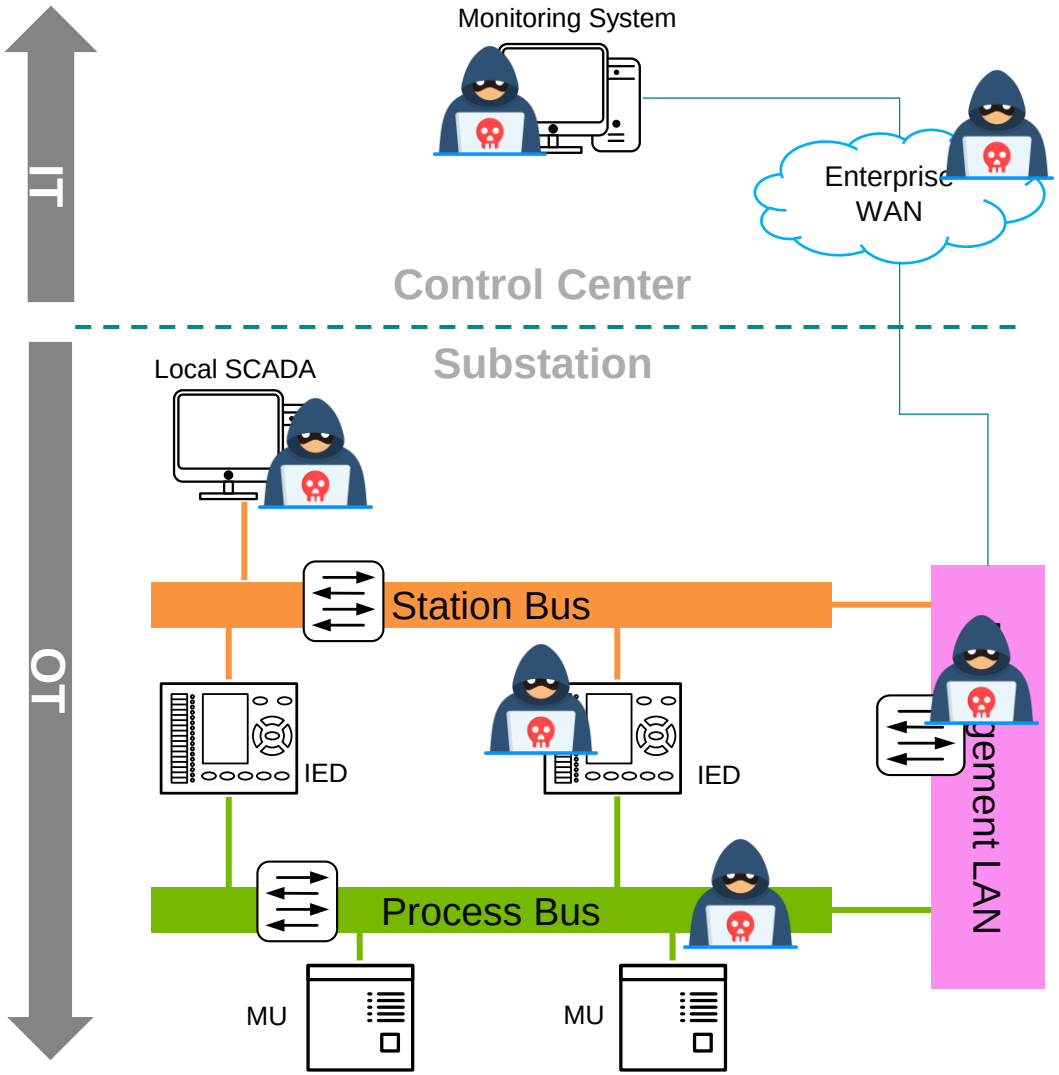
- Dubai Cyber Security Strategy

Security Requirements and Focus in Substation

	Purdue Model	Security Focus
Dispatch Center / IT	Level 4-5 Enterprise	Separate the Control center form the enterprise, physically and electronically
Substation Level / OT	Level 3.5 DMZ	Isolates vulnerable, to protect the internal network
	Level 3 Supervision: SCADA, HMI	Authorizes users for analysis and visualization
	Level 0-2 Process and Control IED, Relay	Provides baselines and continuously monitors the system



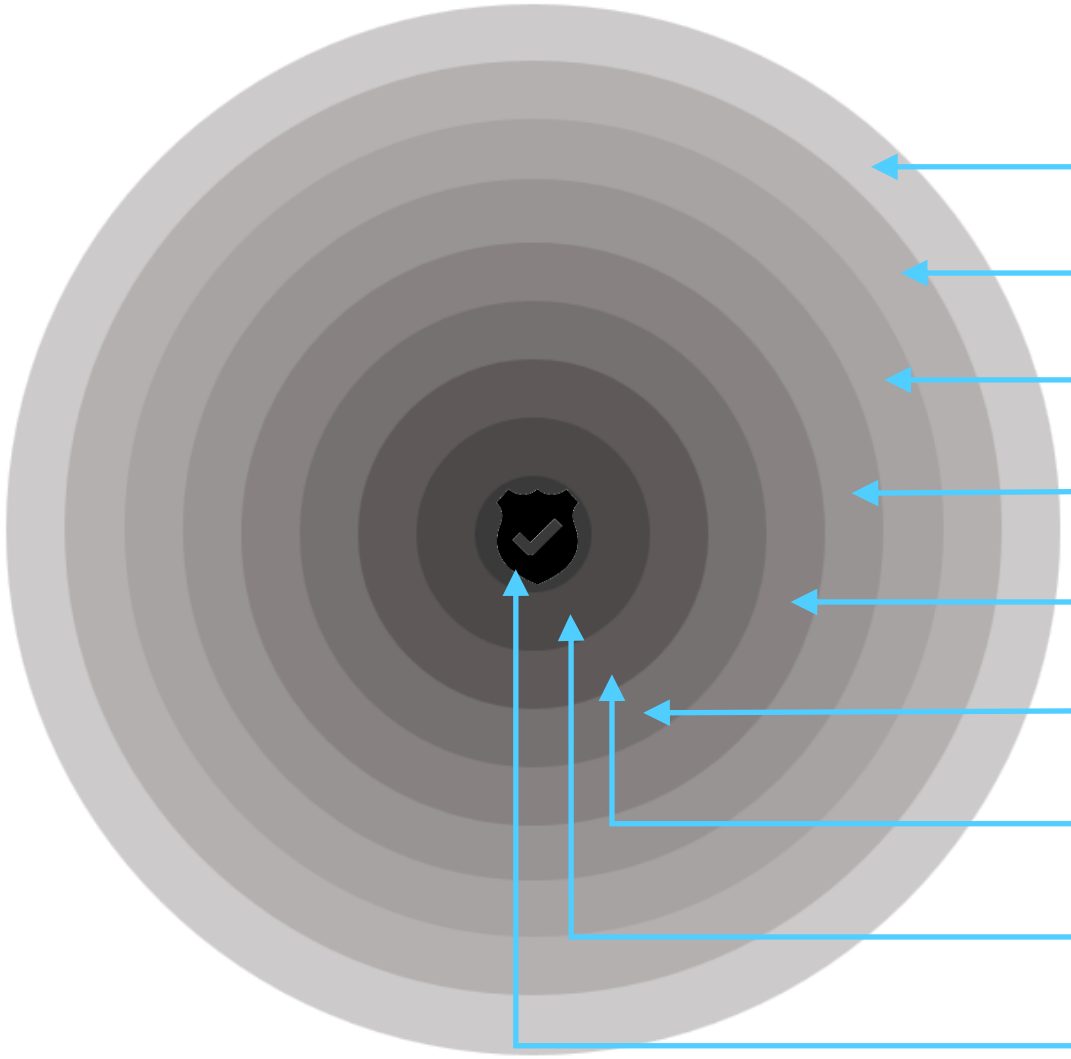
Attack Vectors



- **Phishing & Social Engineering** –
  - Attackers trick users into revealing sensitive information through fake emails, messages, or phone calls.
- **Denial-of-Service (DoS) Attacks –**
  - Overloading systems with excessive traffic to make them unavailable.
- **Malware (Viruses, Ransomware, Trojans, etc.) –**
  - Malicious software infects systems to steal data, encrypt files, or disrupt operations.
- **Unpatched Software & Vulnerabilities –**
  - Exploiting outdated software with known security flaws to gain unauthorized access.
- **Weak or Stolen Credentials –**
  - Using brute-force attacks, credential stuffing, or leaked passwords to access accounts.
- **Insider Threats –**
  - Employees or trusted individuals misuse their access for malicious purposes.
  - Using infected USB drives or external devices to spread malware.
- **Man-in-the-Middle (MitM) Attacks –**
  - Intercepting communications between two parties to steal data or inject malicious content.

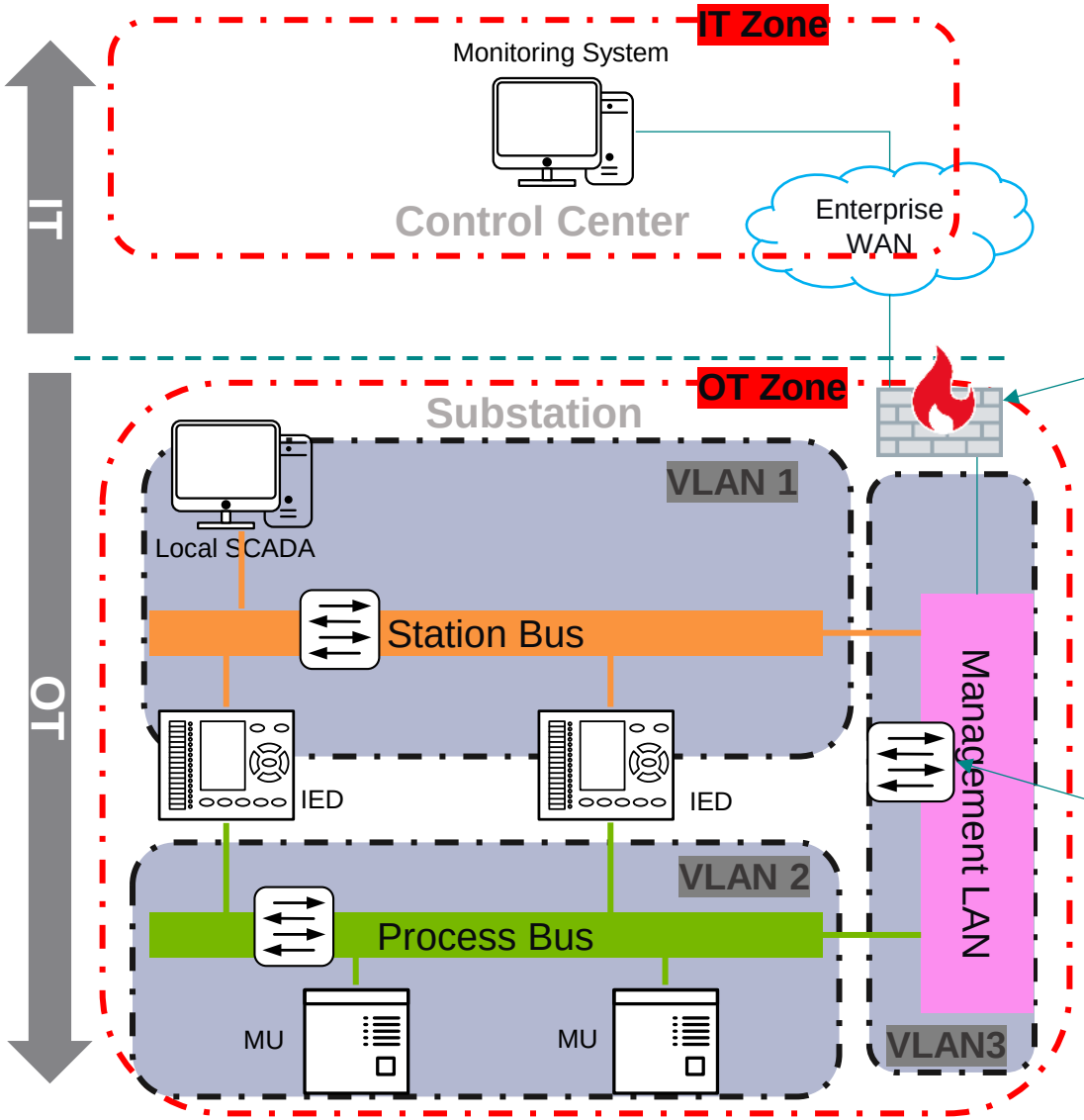
Defense in Depth Strategy

That employs multiple layers of security controls to protect data and systems from threats. The idea is that if one layer fails, the others will still provide protection.



- **Policies, Procedures, and Awareness:** Security Policies, personnel training
- **Network Segmentation:** IP subnet, VLAN
- **Network Access Control:** Firewall policy, switch ACL
- **User Identify and Authentication:** RBAC, AAA
- **Network Threat Defense:** IPS, DoS protection
- **Threat Detection and Incident Response:** IDS, CS dashboard, patch
- **System Monitoring and Management:** Network management, asset management
- **Substation Application Protection:** GOOSE, SV, MMS, PTP
- **Substation Critical Asset Protection:** IED, MU, GMC, BCU

Network Segmentation



Network segmentation is the practice of dividing a network into smaller, isolated sections to enhance security, improve performance, and reduce attack risks

Boundary Firewall L3 segmentation

IP Interface

Providing routing and traffic filtering functions to create secure segmentation between different networks

DMZ

Building a DMZ that only allows limited access from external networks and restricts unauthorized users from accessing the entire networks.

NAT

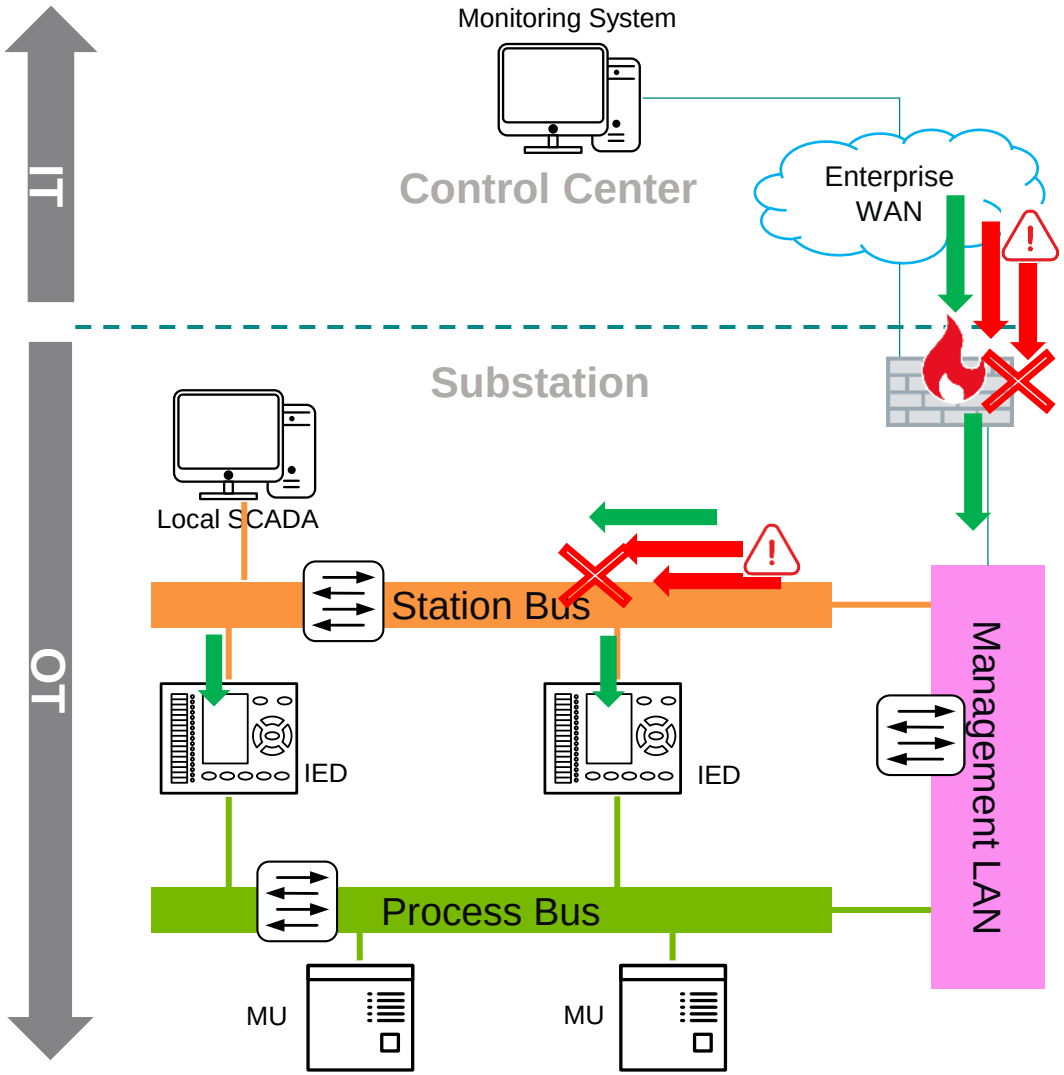
By NAT, it can establish a private local zone to hide internal network information from external probing.

LAN Switch L2 segmentation

VLAN

To isolate broadcast domain. It can restrict the traffic to be transmitted in the specific micro segmentation and minimize the accidental scale.

Network Access Control



Network Access Control ensures that data communication within a substation network is controlled, monitored, and limited to reduce cybersecurity risks.

Boundary Firewall

Policy Rules

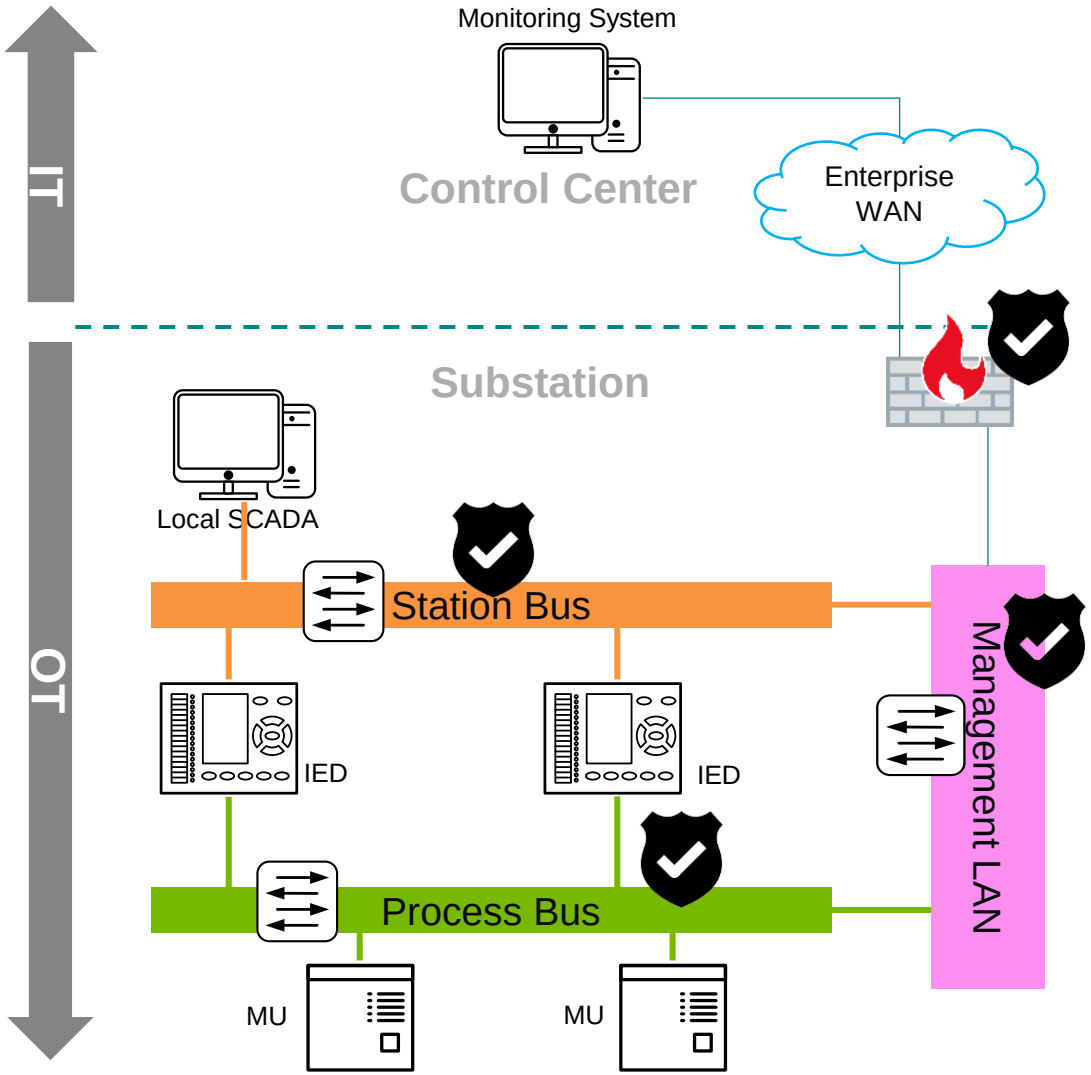
By IP addresses and ports, only allow permitted traffic flows on the network.

LAN Switch

ACL

By IP or MAC addresses, only allow users to access data and networks based on the rules.

Network Threat Defense



Network Threat Defense enhances security by detecting and preventing cyber threats in real-time, protecting sensitive data, ensuring business continuity, reducing attack surfaces.

Key Methods of Threat Defense

DoS Protection

By detecting abnormal packet formats or unusual traffic flows, allowing your device to drop packets

Protocol Filters w/ DPI

By DPI, check the context of each packet payload to only allow the approved content (value & action) transmission on the network.

IPS

Protecting against cyberthreats by performing pattern-based detection and blocking known attacks.

Traffic Storm Protection

Preventing the network from flooding caused by a broadcast, multicast, or unicast traffic storm on a physical network layer

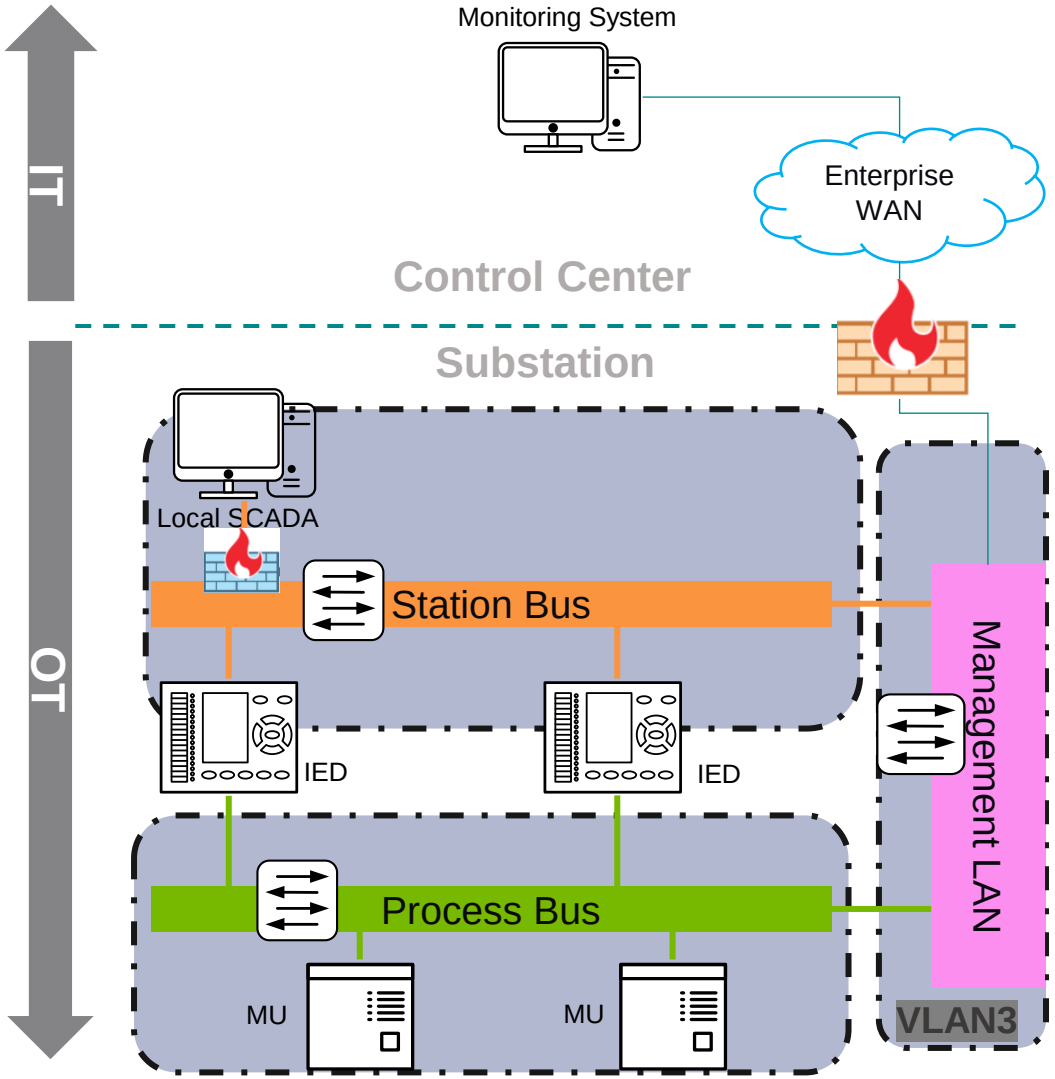
Rate Limiting

Control ingress or egress traffic rate to protect the critical equipment

Critical Packet Inspection

By real-time monitoring substation critical protocols, such as GOOSE, SV, PTP, detecting the abnormal behavior.

Enhance Network Security With Industrial Firewall



LAN Firewall Solutions

EDF-G1002-BP Series
Industrial LAN Firewalls

Boundary Firewall Solutions

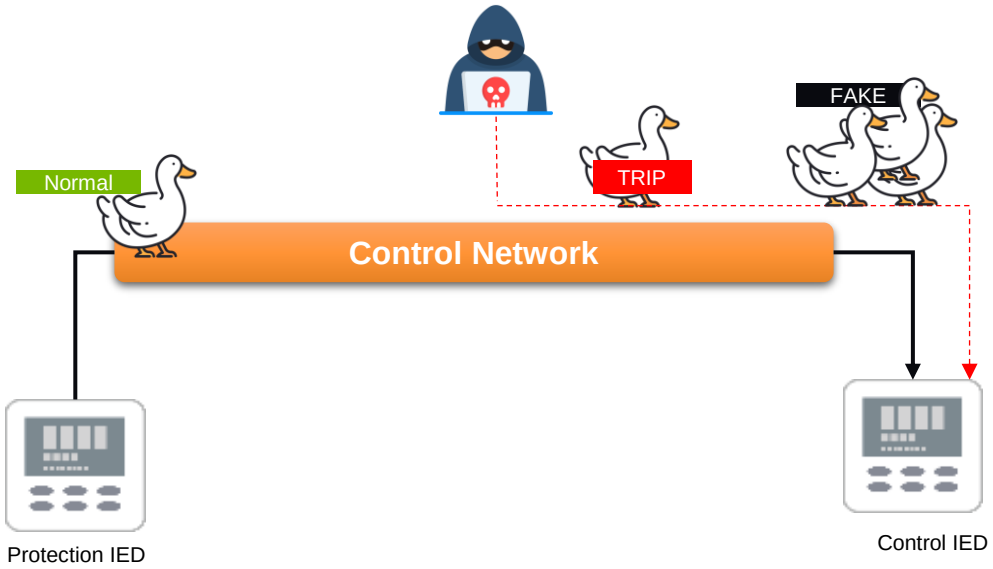
EDR-G9010/G9004/8010 Series
Industrial Secure Routers

Substation Application Protection

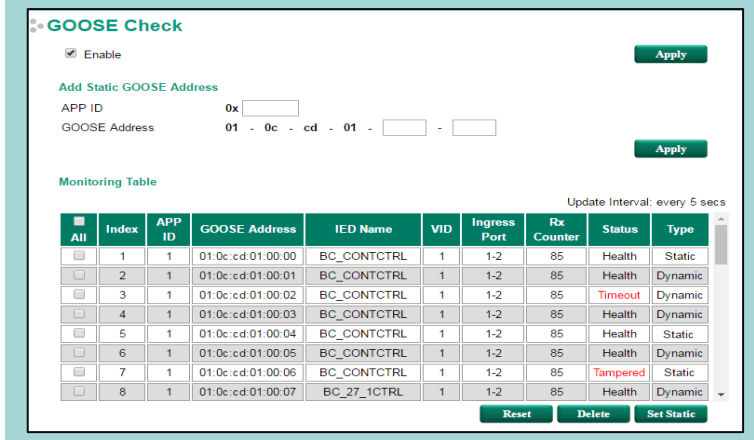
Critical protocol: GOOSE

Security Attacks on GOOSE

- GOOSE is multicast packets, it's easy to sniff messages
- Not practical to implement firewall between IED



GOOSE Check

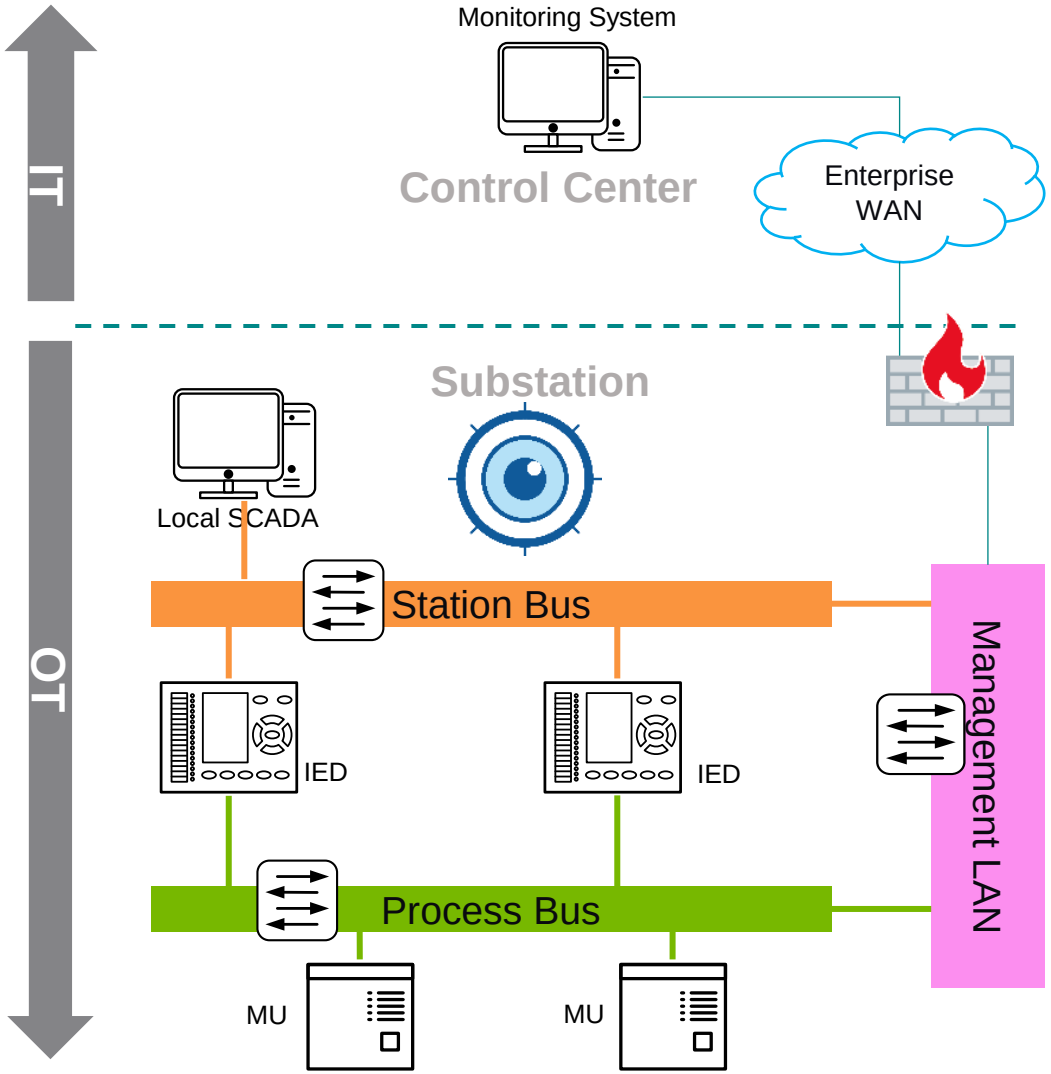


- GOOSE Check involves Ethernet switches in the substation network to detect the GOOSE packets and continuously monitor their behavior.
- Timeout and tamper events warnings can be sent via SNMP trap or MMS report

GOOSE Lock

- GOOSE whitelisting: Lock GOOSE configuration to allow valid GOOSE stream in the network

System Monitoring & Management



Visibility empowers you to secure and control your industrial control systems, and asset management helps organizations identify, track, protect, and manage all IT and OT assets to reduce security risks and ensure compliance.

Network Monitoring

Topology Monitoring

By collecting data from devices, it helps administrators visualize network topology and detect its changes quickly.

Traffic Analysis

By collecting data from devices, it helps administrators monitor traffic loading on each node & route, and understand the heath status of the network.

Asset Management

Configuration Management

It helps administrators consistently maintain a product's functional and physical attributes throughout its operational life.

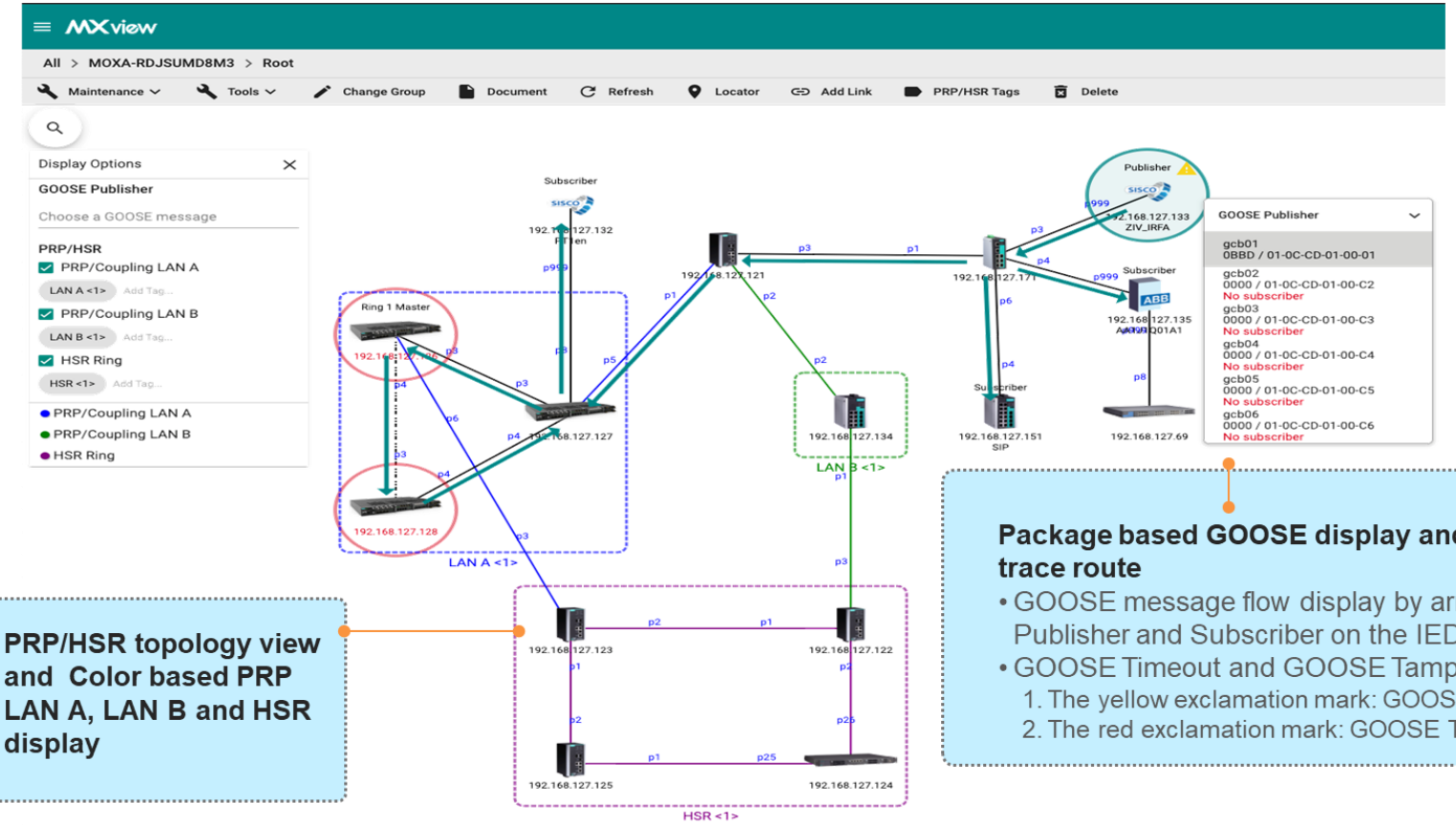
Device Policy Audit

It helps administrators audit all devices and ensures all devices comply with company policies.

Network Visibility and Management

MXview Power

Visualize GOOSE Flow and Detect Malicious GOOSE Messages

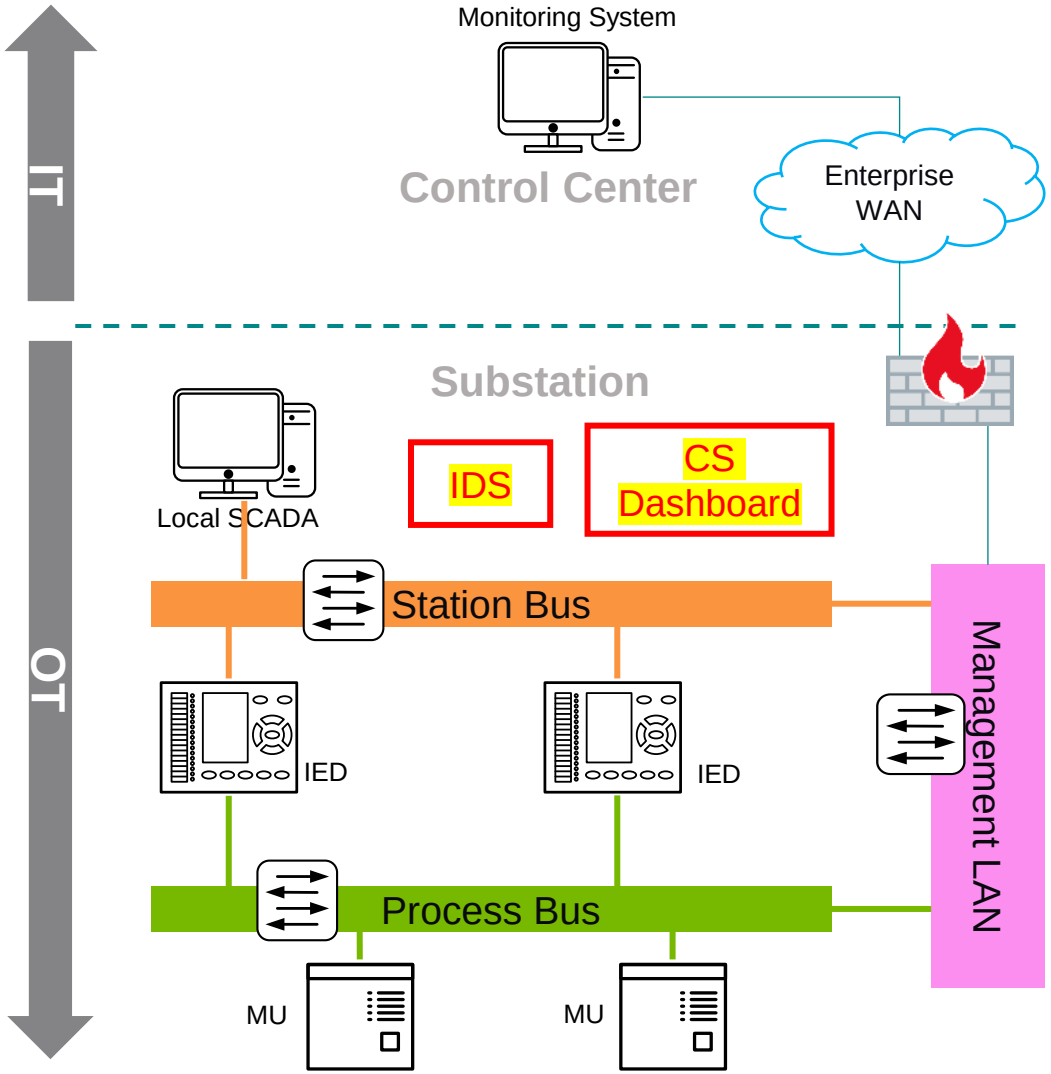


PRP/HSR topology view and Color based PRP LAN A, LAN B and HSR display

Package based GOOSE display and support trace route

- GOOSE message flow display by arrow and mark Publisher and Subscriber on the IED.
- GOOSE Timeout and GOOSE Tampered events
  1. The yellow exclamation mark: GOOSE Timeout
  2. The red exclamation mark: GOOSE Tampered

Timely Incidents Response and Security Patch



Ensuring that substation system can detect, respond to, and recover from cybersecurity incidents in a timely manner.

Response and Patch

Security incidence Detection & Logging

Adopting proper approach like IDS (Intrusion Detection System) to do constantly threat monitoring and logging.

Cyberthreats Responding

A well-planned cyber threat response minimizes damage, reduces downtime, and strengthens cybersecurity resilience.

Security Patch

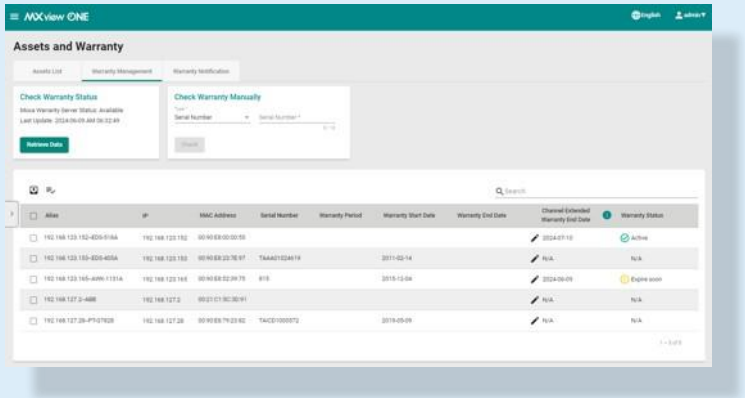
Regularly updating and applying security patches, bug fixes, and software updates to operating systems, applications, and network devices to protect against vulnerabilities and cyberthreats.

Network Visibility and Management

MXview ONE

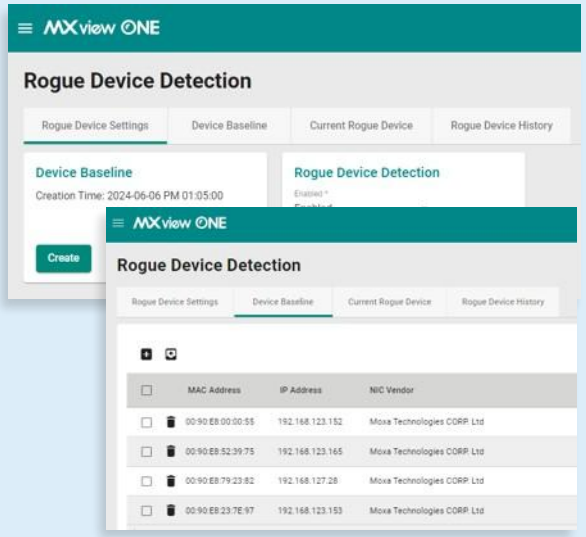
Cybersecurity Policies Require Annual Inventory Checks Errors.

Inventory Management

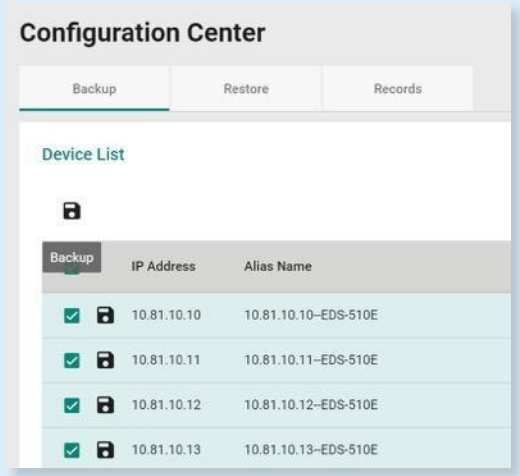


Display devices' warranty info

Create Baseline and enable Rogue Device Detection



Backup & Restore



Backup & restore device configurations

System DB backup & restore

MOXA

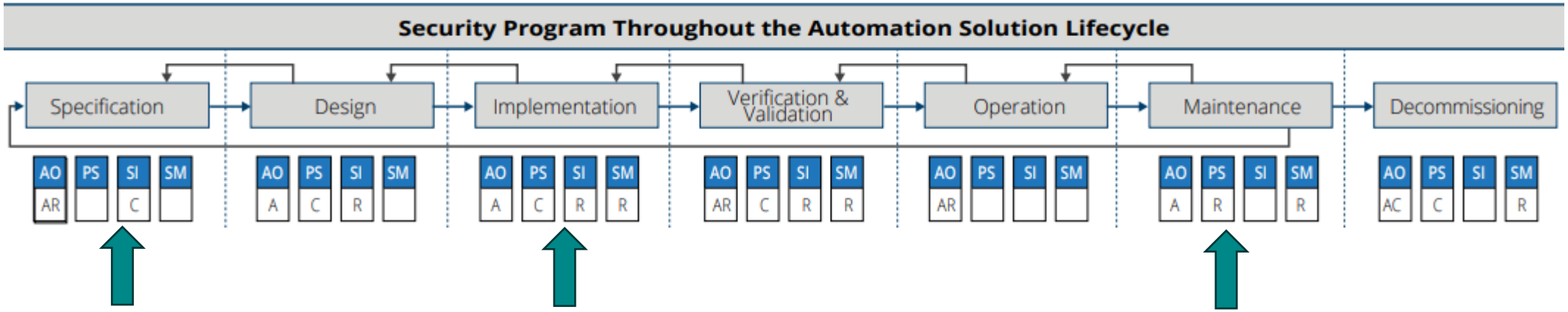
Bridge the Network Security Gap

MOXA

Bridge the Network Security Gap

AO Asset Owner PS Product Supplier SI Integration Service Supplier SM Maintenance Service Provider

A Accountable R Responsible C Contributor



缺乏”系統”資安觀念

Solution:

ISA 62443個人認證課程

資安功能未被如實導入

- 工期問題
- 缺乏資安知識

Solution:

產品教育訓練

系統網路設計服務

- **設定手冊**
- **大量部署工具**

資訊設備管理與補丁管理需求

Solution:

網管軟體 + 原廠通訊設備檢測服務

Ref. Guide to Security Lifecycles in the ISA/IEC 62443 Series of Standards

MOXA

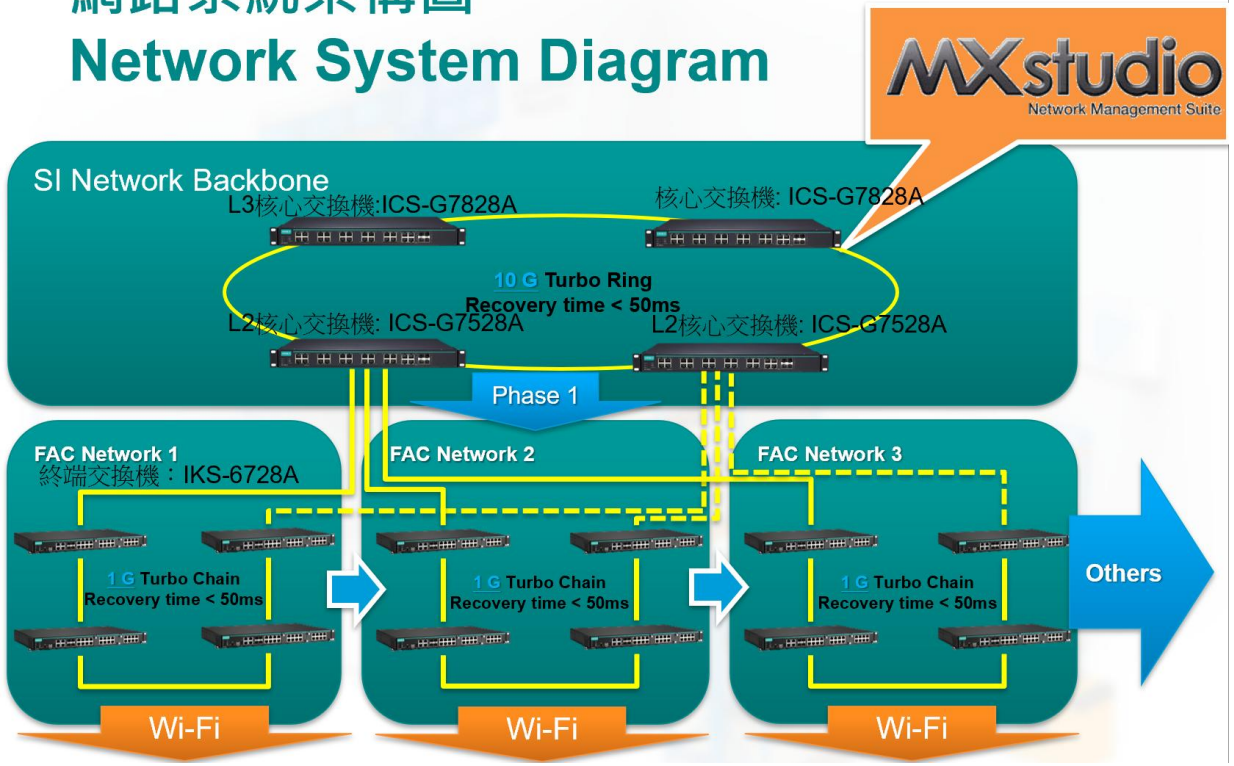
工業網路設計服務

設計階段 | 安裝階段 | 維運階段 | 技術教育訓練

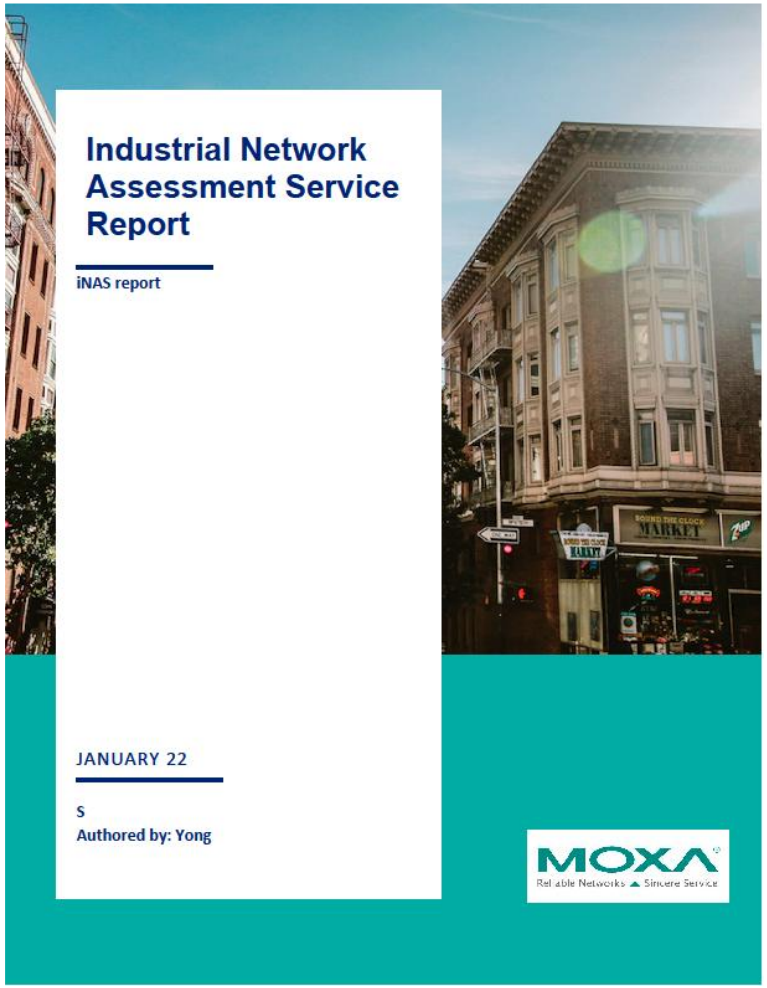
■ 服務內容

- ■協助定義技術需求與規劃網路架構
- ■提供工業網路設計報告
  - ■設備清單與網路架構
  - ■IP/ VLAN規劃
  - ■實體連接方式規劃
  - ■L2 & L3備援與路由規劃
  - ■**設備與網路資安建議與設定**
- ■小型PoC驗證
- ■[Optional] 客製化教育訓練服務

網路系統架構圖
Network System Diagram



原廠通訊設備檢測服務



透過專業檢測報告
輕鬆了解通訊設備年度狀況

檢測重點

- Network healthy summary
- Network status
  - Topology status
  - **Network asset management (網路資產管理)**
  - Average availability update
  - Average throughput update
  - Over threshold packet error rate update
  - Warning events summary
  - **Patch management & suggestions (補丁管理與建議)**
- Device life cycle update (設備保固訊息)

Summary

- Secure IEC 61850-3 Devices
- Switch & Firewall with Rich Security Features
- Monitoring and Management Software
- Cybersecurity Awareness Training

Cybersecurity Dashboard

MXsecurity

- Policy Management
- Incident Event
- Path Management

Network Monitoring and Management

MXviewOne

- Device Management
- NMS
- GOOSE flow visualization

Firewall

NGFW

Secure Router

- Boundary Firewall
- LAN Firewall

Switch

PT-G7000
RKS-G4000

EDS-G4000

- RBAC
- GOOSE/MMS
- Traffic mirroring
- ACL

Thank You

For further information, visit www.moxa.com.