

《通訊與電網資安》

標準導入、解決方案與實務案例分享

莊峻富 Jun Chuang

Moxa 能源事業處協理

May 31, 2024



- 電網資安標準
- 通訊與電網資安解決方案
- 全球實務案例分享

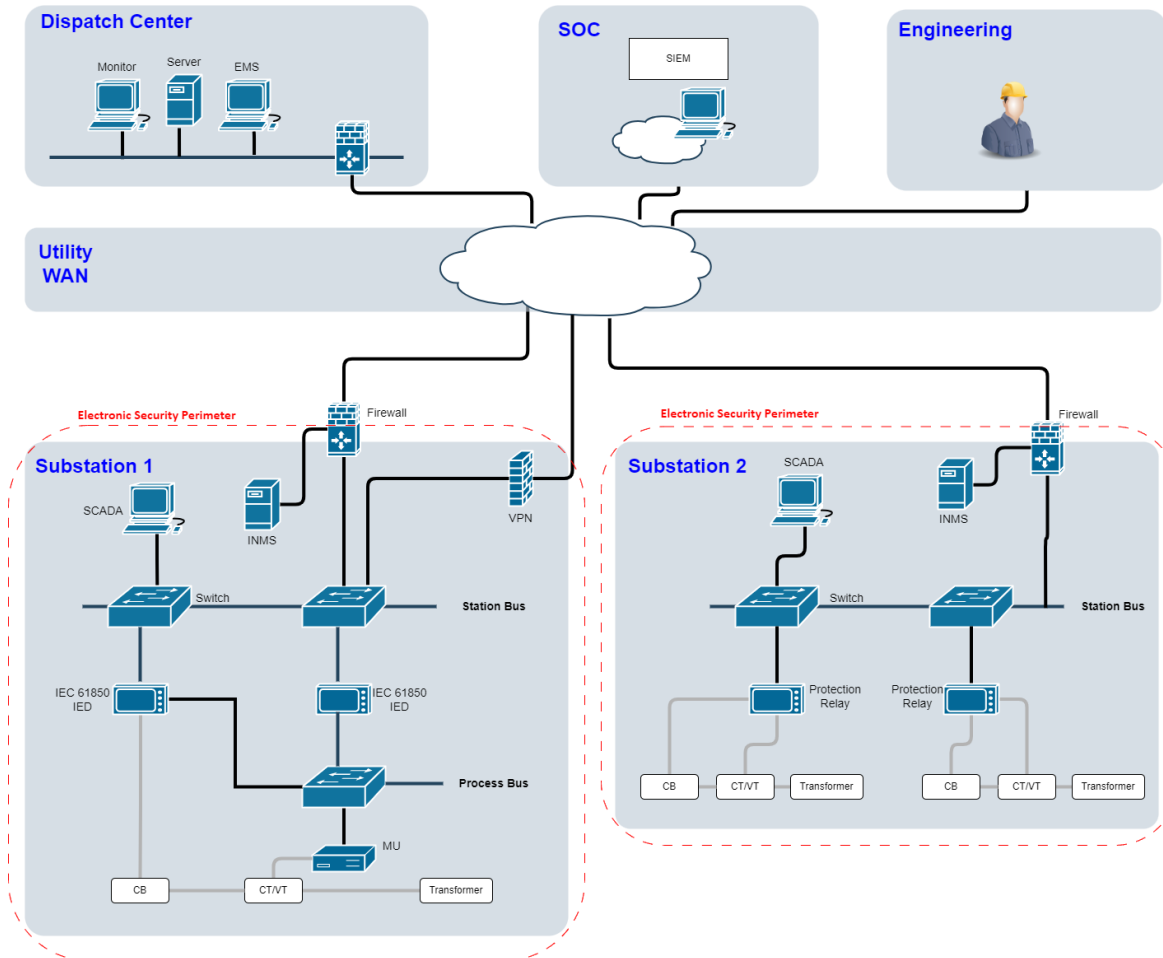




電網資安標準

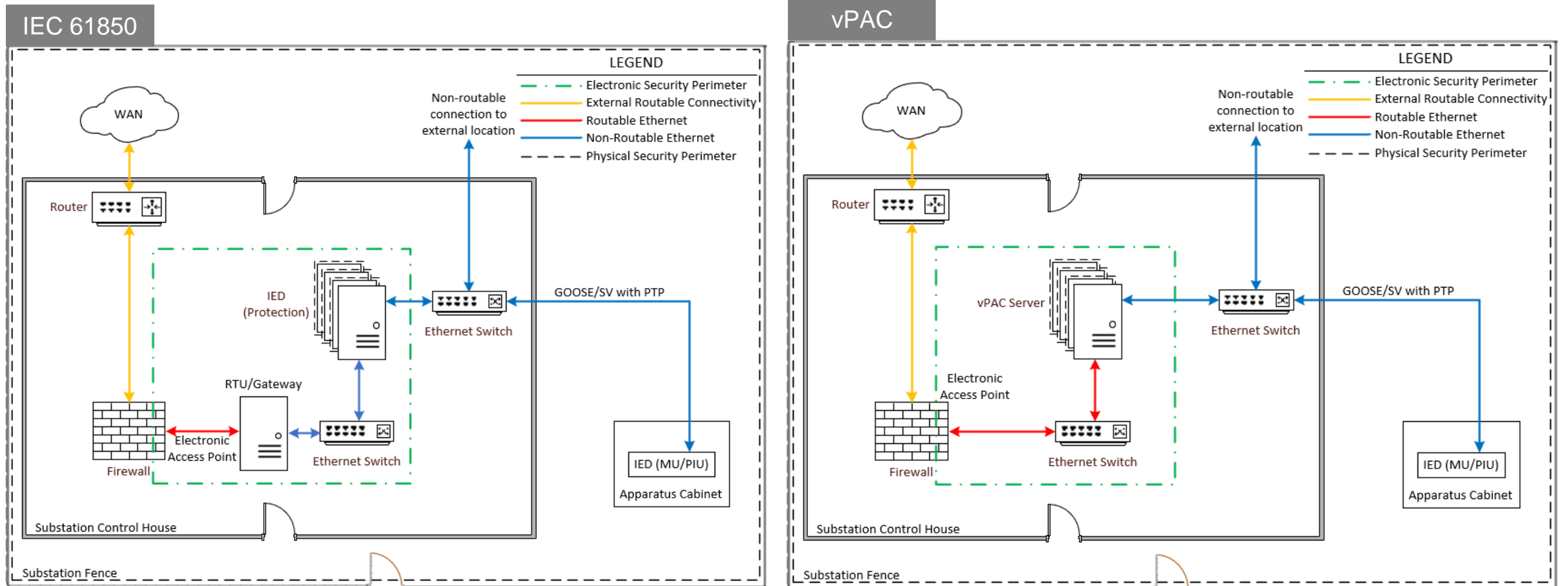
- NERC CIP
- IEC 62443 & IEC 62351
- AESCSF

NERC CIP Requirements



NERC CIP Part	Requirement
CIP-002-5.1a BES Cyber System Categorization	Monitor and manage cyber assets in BES
CIP-005-6 Electronic Security Perimeter(s)	<ul style="list-style-type: none"> • Monitor the cyber assets within ESP • ACL & Firewall policy management • IDS in EAP • Secure remote access • Implement DMZ to prevent directly access
CIP-007-6 System Security Management	<ul style="list-style-type: none"> • Service port management • Physical port management • Security patch management • Malicious code prevention • Security event monitoring • System access control
CIP-008-6 Incident Reporting and Response Planning	Product Security Incident Response Team (PSIRT)
CIP-009-6 Recovery Plans for BES Cyber Systems	<ul style="list-style-type: none"> • Configuration recovery • Software recovery • Data recovery

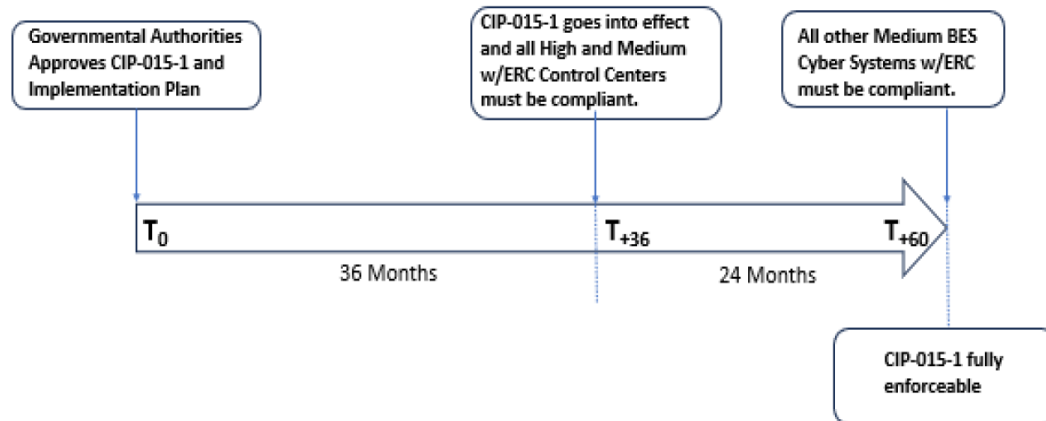
NERC CIP in Substation Automation



*Figure adopted from vPAC (virtual Protection Automation Control) alliance cybersecurity spec

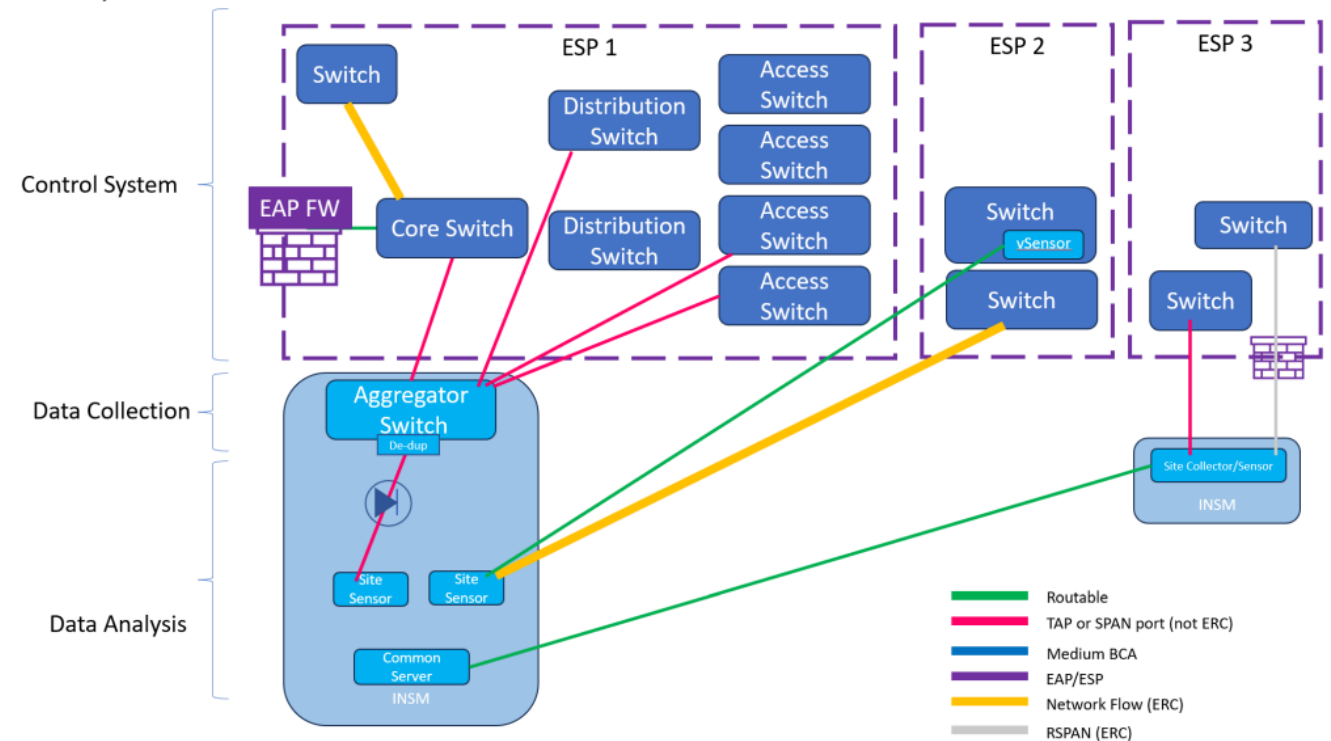
NERC CIP INSM (Internal Network Security Monitoring)

In January 2023, FERC issued a final rule directing NERC to develop new or updated CIP reliability standards, including requirements for internal network security monitoring (INSM), specifically for highly impactful Bulk Electric System (BES) cyber systems and medium-impact BES cyber systems with external connectivity.

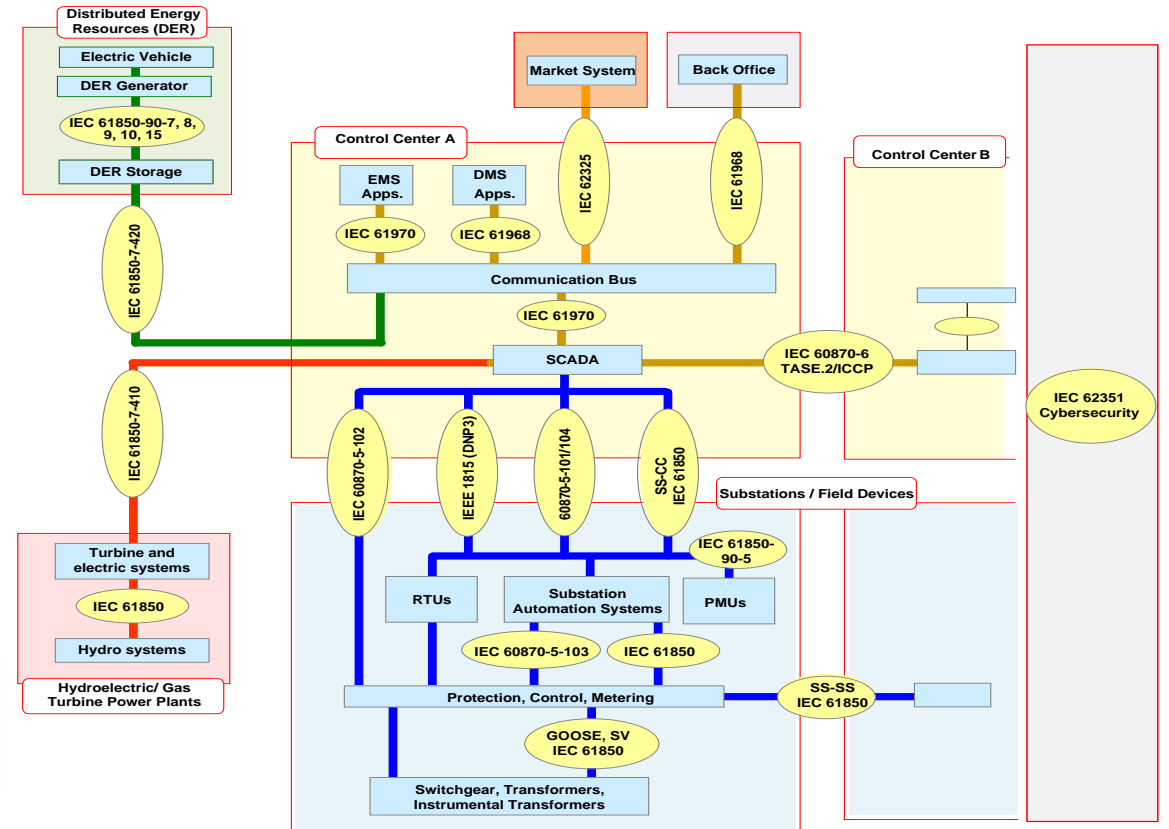
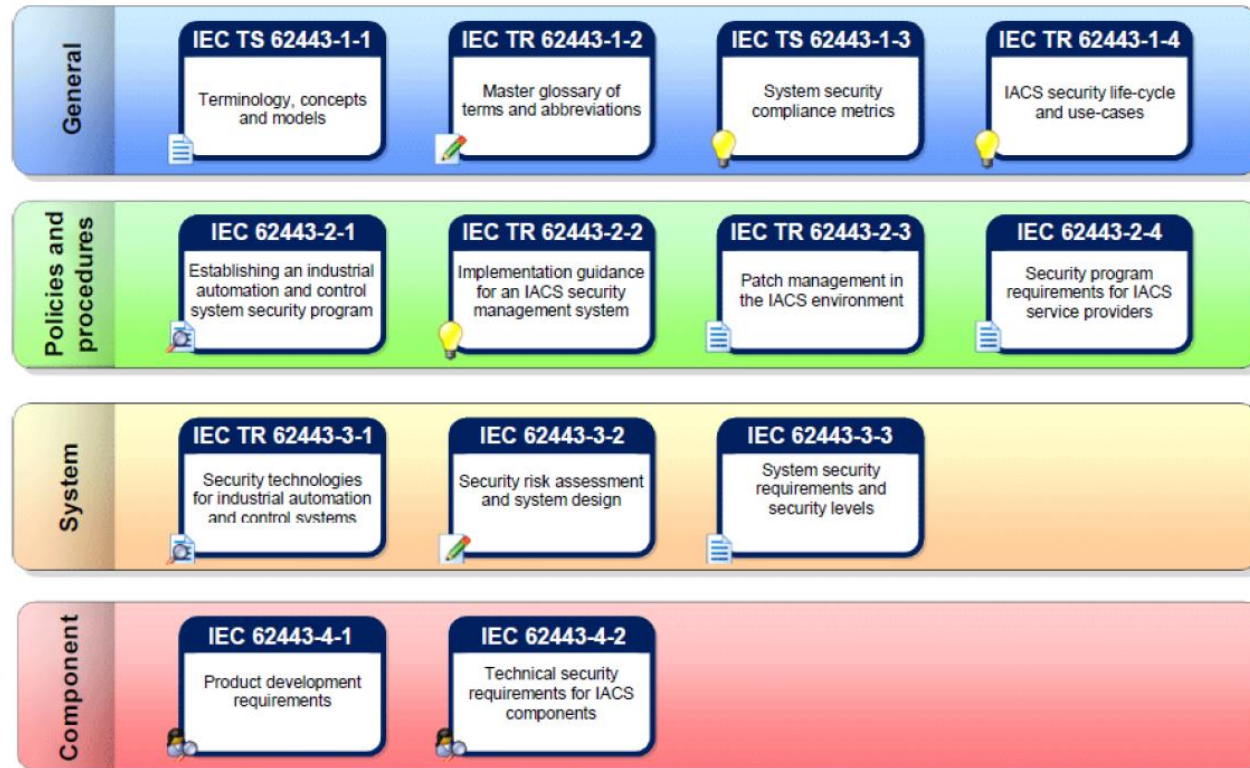


Reference Architecture

A sample reference architecture for INSM collection and logging data is shown below. This diagram is intended to show a wide variety of possible collection methods. Entities are not expected to implement all of these, but rather to choose and implement the collection methods that provide the most value to the entity.

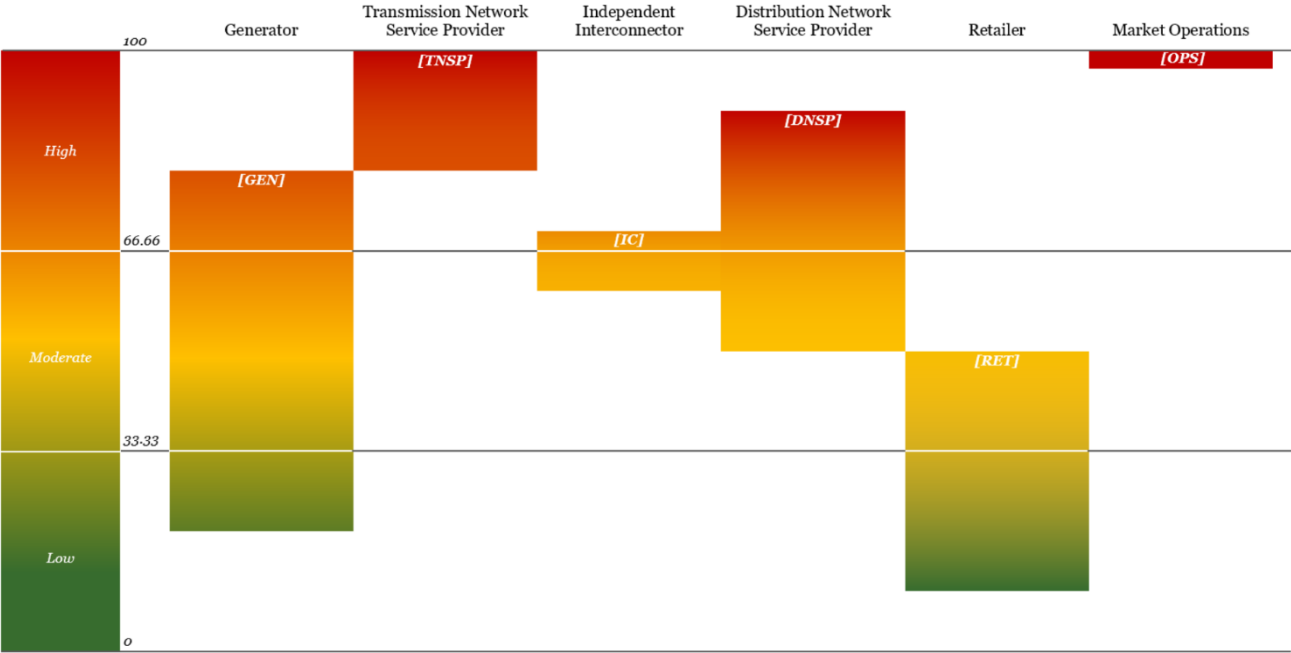


IEC 62443 & IEC 62351



AESCSF (Australian Energy Sector Cyber Security Framework)

Criticality Bands by Market Role



AESCSF Framework – Architecture

			Security Profiles [SP]								
			SP-1			SP-2			SP-3		
			Maturity Indicator Levels [MIL]								
			MIL-1	MIL-2	MIL-3	MIL-1	MIL-2	MIL-3	MIL-1	MIL-2	MIL-3
			Practices								
Domains	ACM	Asset, Change and Configuration Management	6	1	0	0	6	2	0	0	5
	CPM	Cyber Security Program Management	4	2	0	0	15	0	0	0	7
	EDM	Supply Chain and External Dependencies Management	4	0	0	0	11	2	0	0	4
	IAM	Identity and Access Management	6	4	2	0	8	4	0	0	2
	IR	Event and Incident Response, Continuity of Operations	12	5	2	0	9	3	0	0	15
	ISC	Information Sharing and Communications	2	1	0	0	4	0	0	0	5
	RM	Risk Management	2	4	0	0	7	0	0	0	7
	SA	Situational Awareness	4	5	0	2	10	3	0	0	9
	TVM	Threat and Vulnerability Management	7	2	0	0	9	0	0	0	9
	WM	Workforce Management	6	2	0	0	7	3	0	0	14
	APM	Austrailian Privacy Management	4	1	0	0	6	1	0	0	5
# Practices/SP & MIL			57	27	4	2	92	18	0	0	82
# Practices/SP			88			112			82		
Total Practices			282								



通訊與電網資安解 決方案

Power Utility Cybersecurity Challenges & Offerings

- **Challenges**

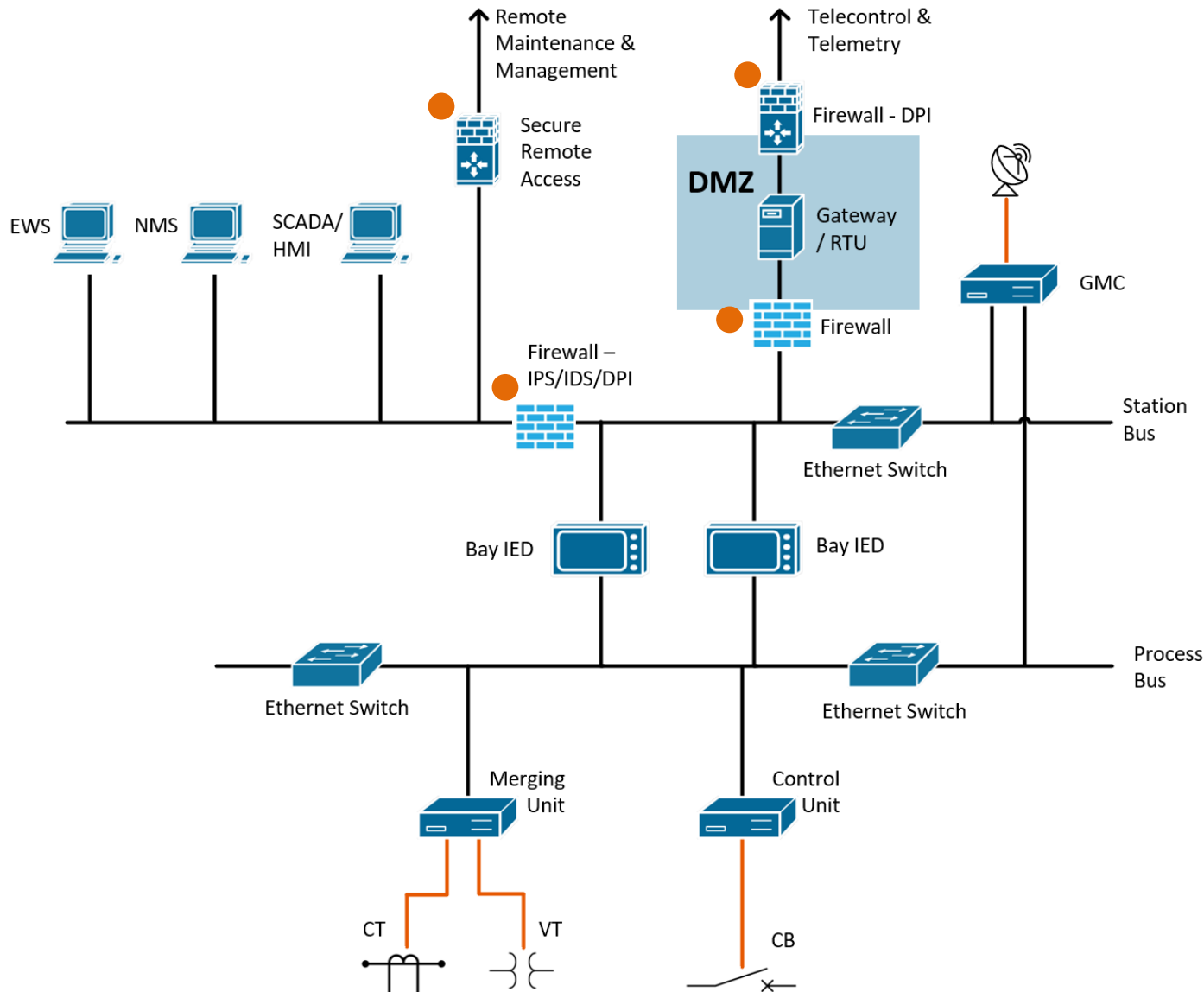
- Reliability and risk mitigation
- Asset management

- **Offerings**

- Detect & respond to cyber threats
- Visualize communication status



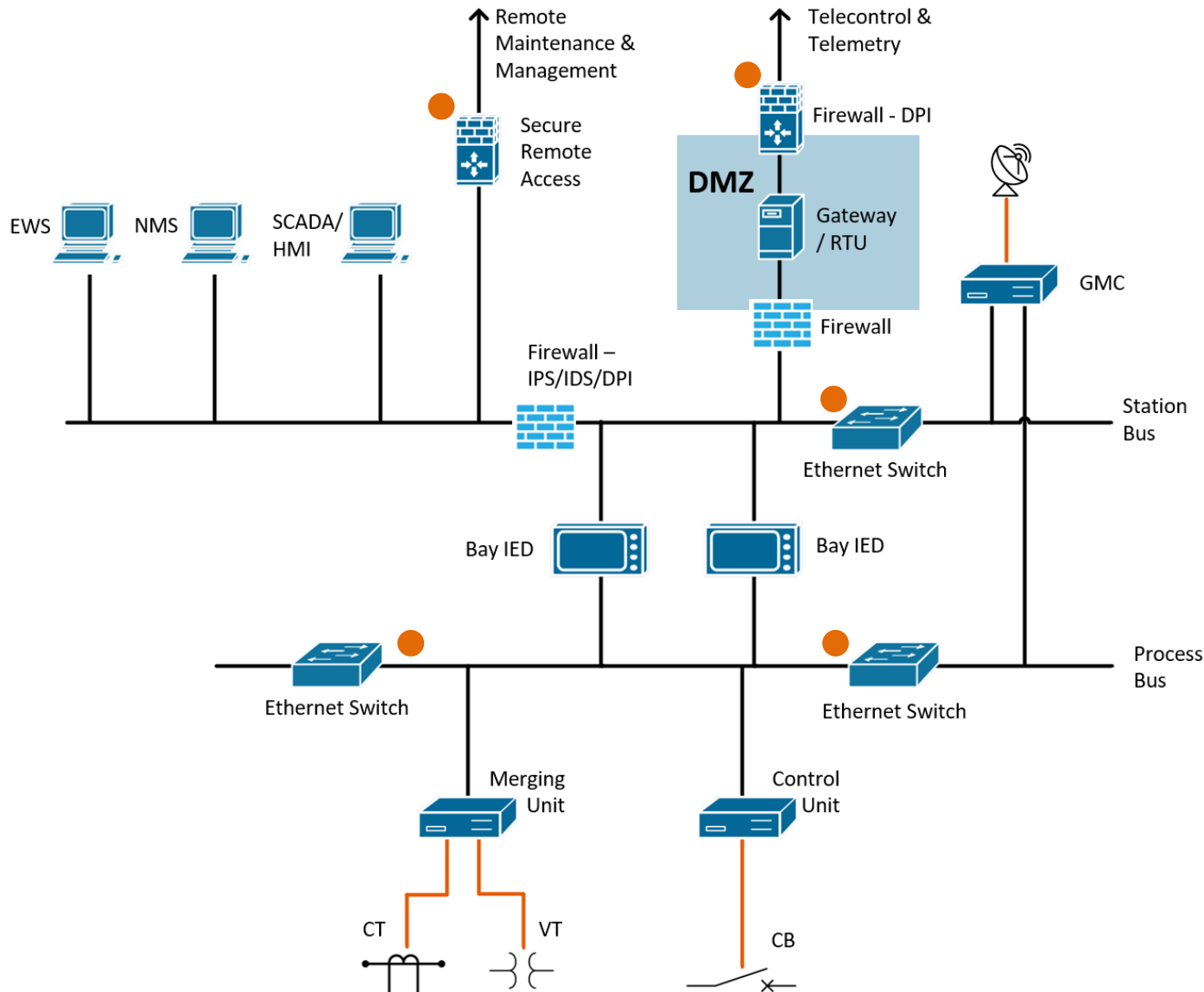
Cybersecurity Offering #1 Next-Generation Firewall



The **Next-Generation Firewall** may offer the following cybersecurity functions:

1. Firewall / VPN
2. IPS/ IDS (入侵防禦/偵測)
3. DPI
4. Virtual Patch (虛擬補丁)

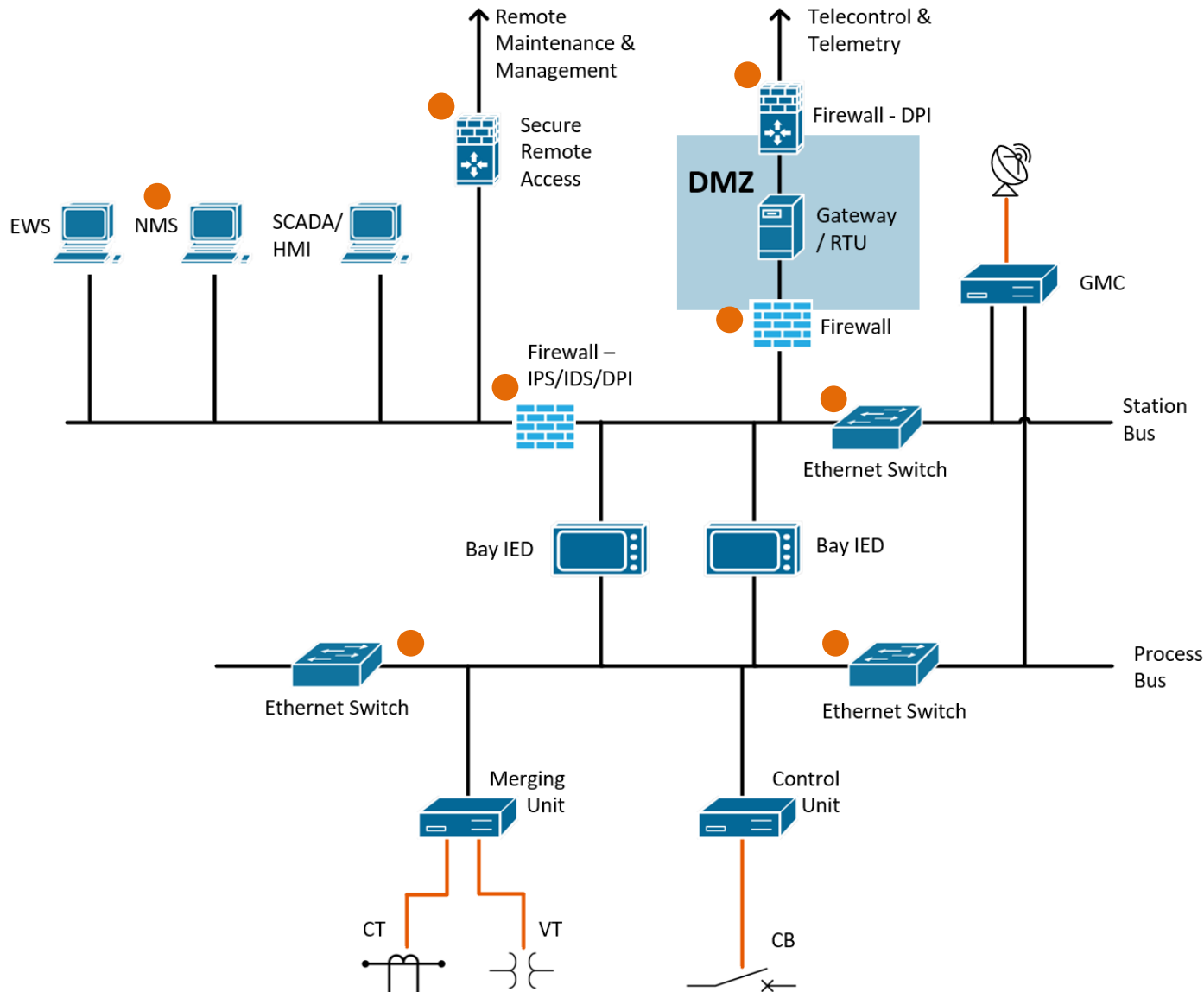
Cybersecurity Offering #2 Packet Analysis



The **Packet Analysis** may offer the following cybersecurity functions:

1. GOOSE monitoring
2. DNP3/MMS/GOOSE DPI

Cybersecurity Offering #3 Visibility Software



The **Visibility Software** may offer the following cybersecurity functions:

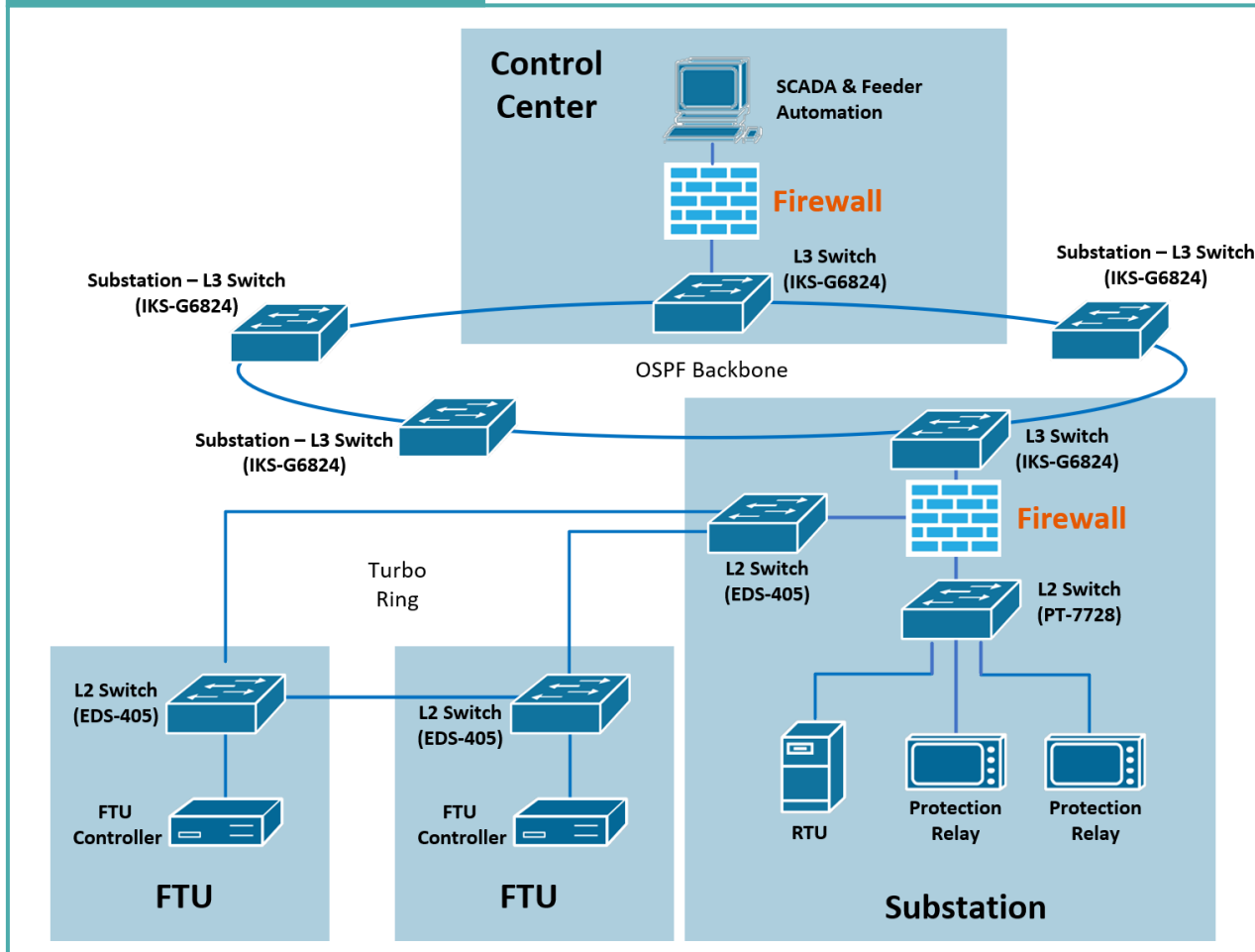
1. Network status monitoring
2. Visualize critical packets
3. SIEM integration

The background of the slide features an aerial view of an offshore oil rig in the middle of a vast blue ocean. The rig consists of several red and white derrick structures. Overlaid on the entire image is a network of glowing blue lines connecting various white circular nodes, creating a digital or global connectivity theme. The right side of the slide is partially covered by a solid teal-colored triangle.

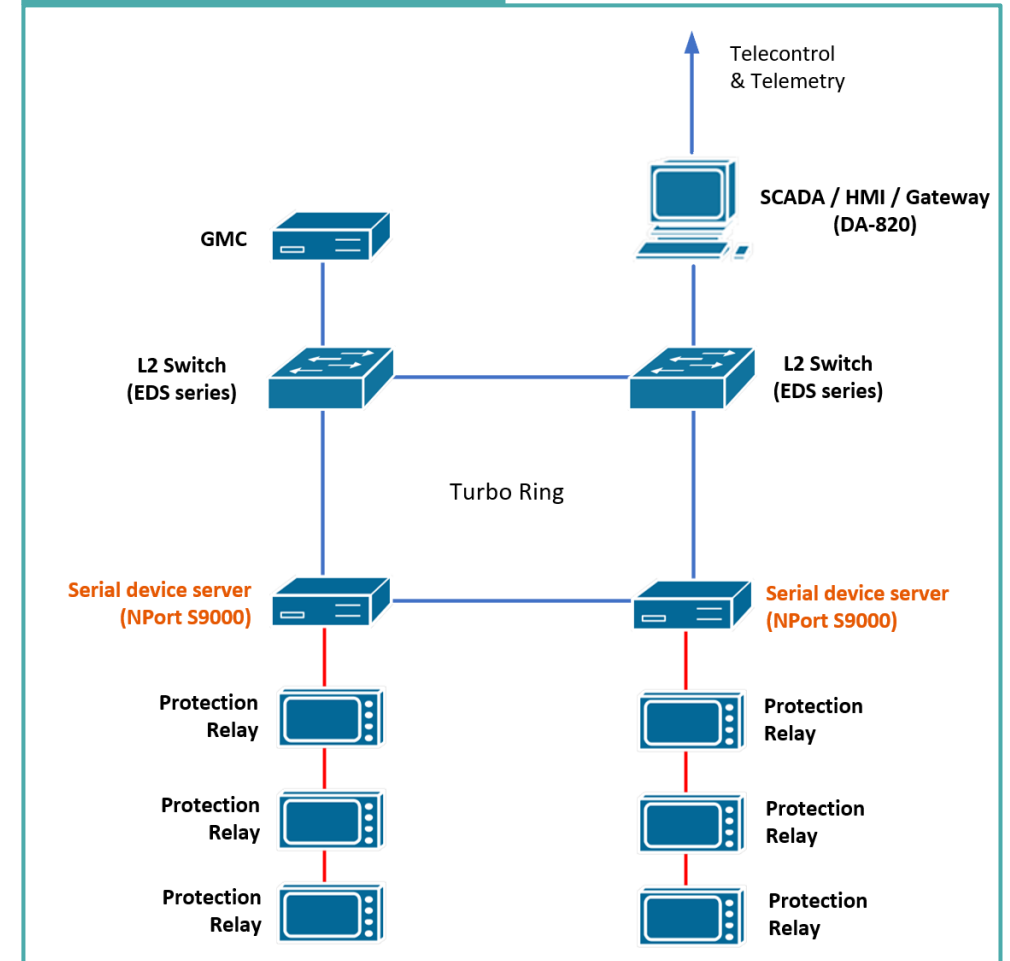
全球實務案例分享

US Power Utility Substation Automation

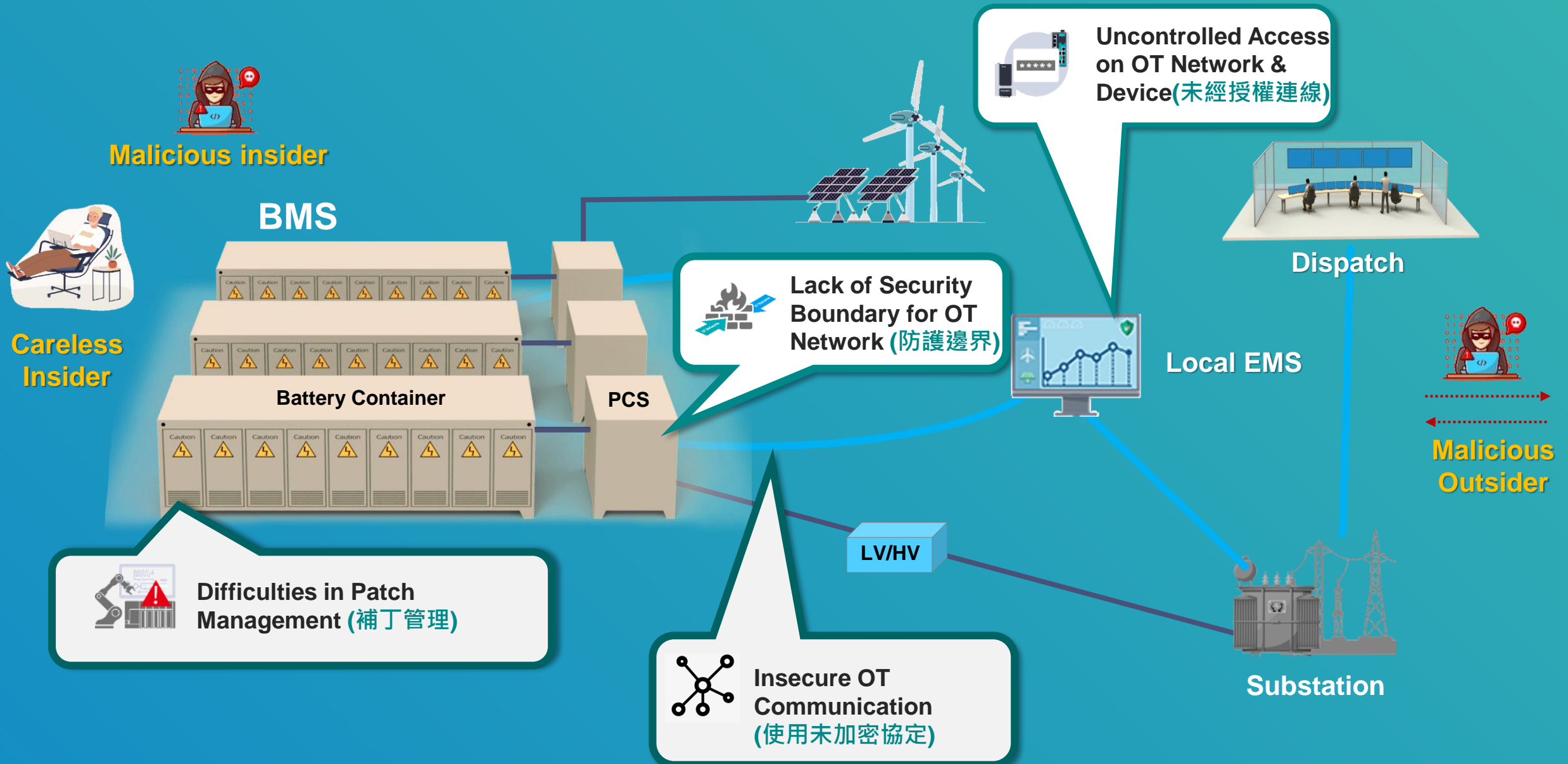
One Cooperative



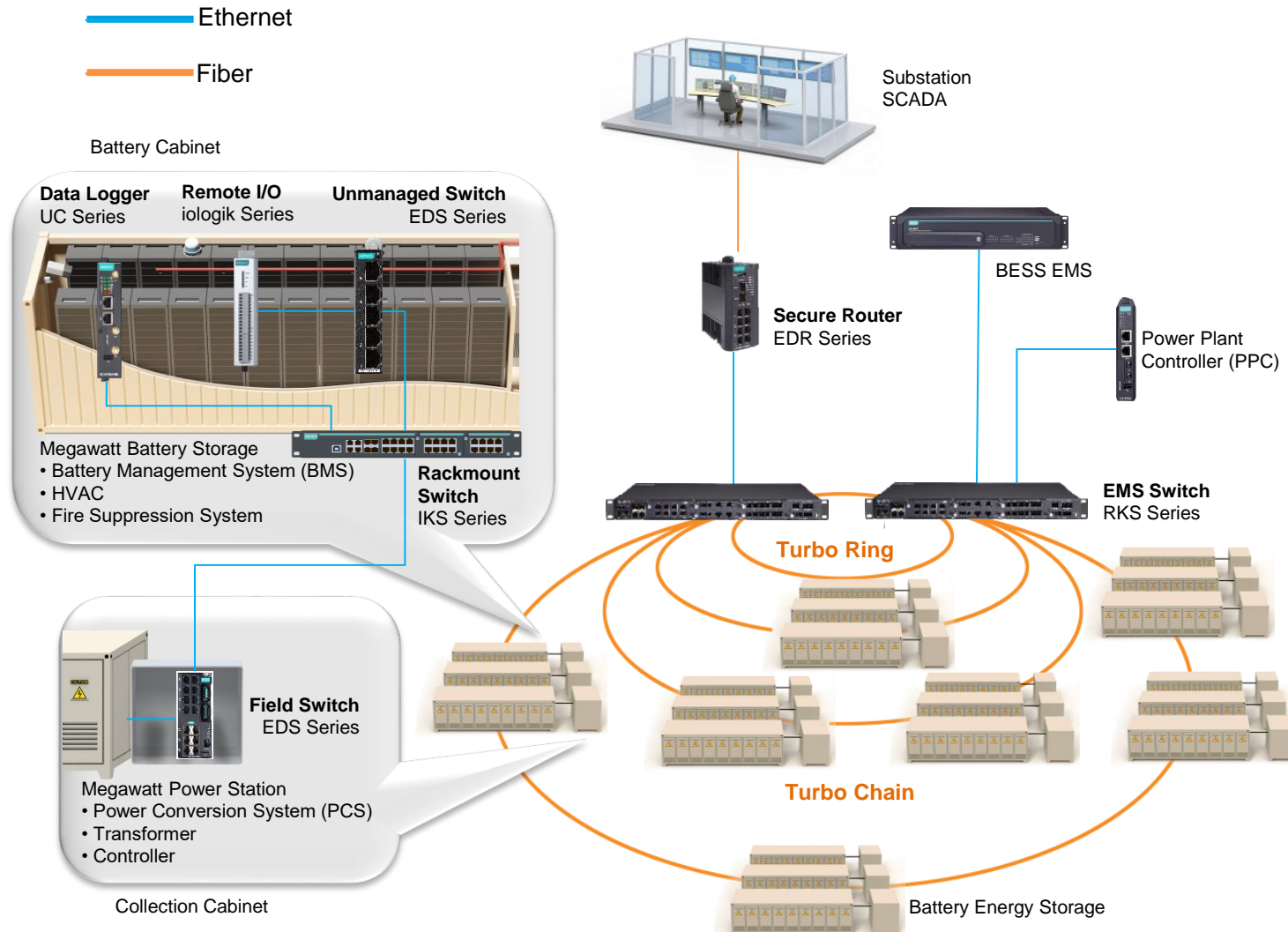
One Municipal



Security Risks of BESS Integration



AU Grid-Scale Battery Energy Storage Security Network



Customer Requirements

- Reliable network to support grid-scale energy storage system
- Fast recovery of network to support hundred-millisecond grid services
- Cybersecurity certified devices
- Secure connection to substation system
- Robust devices for data acquisition and logging in battery cabinets

Moxa Solutions

- Turbo Ring/Chain recovery time under 20ms ensures network reliability
- Cybersecure IEC 62443-4-2 certified offerings
- Complete offering of edge data acquisition and computing
- Network and cybersecurity design consultancy services

Thank You

For further information, visit www.moxa.com.

The Moxa logo is displayed in white on a teal background. It consists of the word "MOXA" in a bold, sans-serif font, followed by a stylized upward-pointing chevron symbol.

© Moxa Inc. All rights reserved.