

工業資安不斷鏈

OT 網路系統

變化趨勢與資安考量



郭彥徵 Robert Kuo

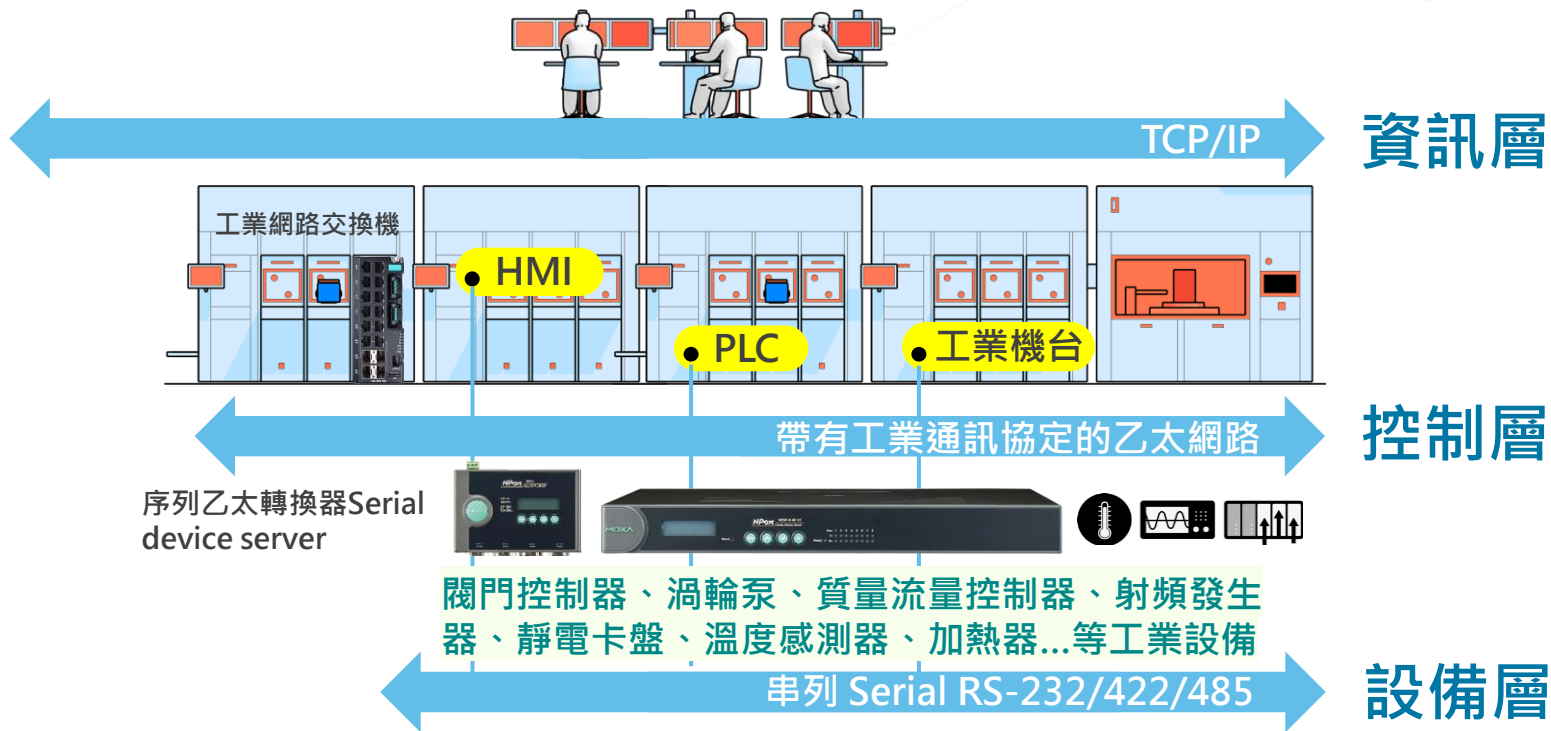
Product Marketing Manager, Moxa

Certified ISA/IEC 62443 Cybersecurity Expert

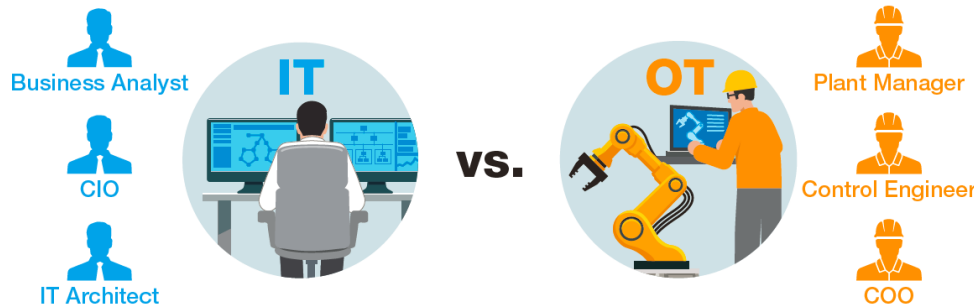
IT/OT 系統網路融合帶來資安威脅



網路系統變化趨勢 – 多網融合



資安視角 - IT/OT 考量差異



首要考量

資料保密性/完整性

系統可用性

系統焦點

數據整合/分析/應用

持續運作的控制控制流程

保護標的

Windows/Linux 為核心：
電腦和伺服器

工業設備為核心：
PLC, HMI, 感測器

現場條件

現場環境良好：
恆溫空調、穩定溼度

現場環境嚴峻：
極溫、震動、電磁波、侵蝕性氣體

資安考量 – 資安融合

- 技術公開資訊多，易由外部取得
- 使用者多元，非專業人士可理解
- 網路架構設計較為彈性/通用

IT
技術環境

以視窗作業系統
為核心運行

IT 系統安全

OT
技術環境

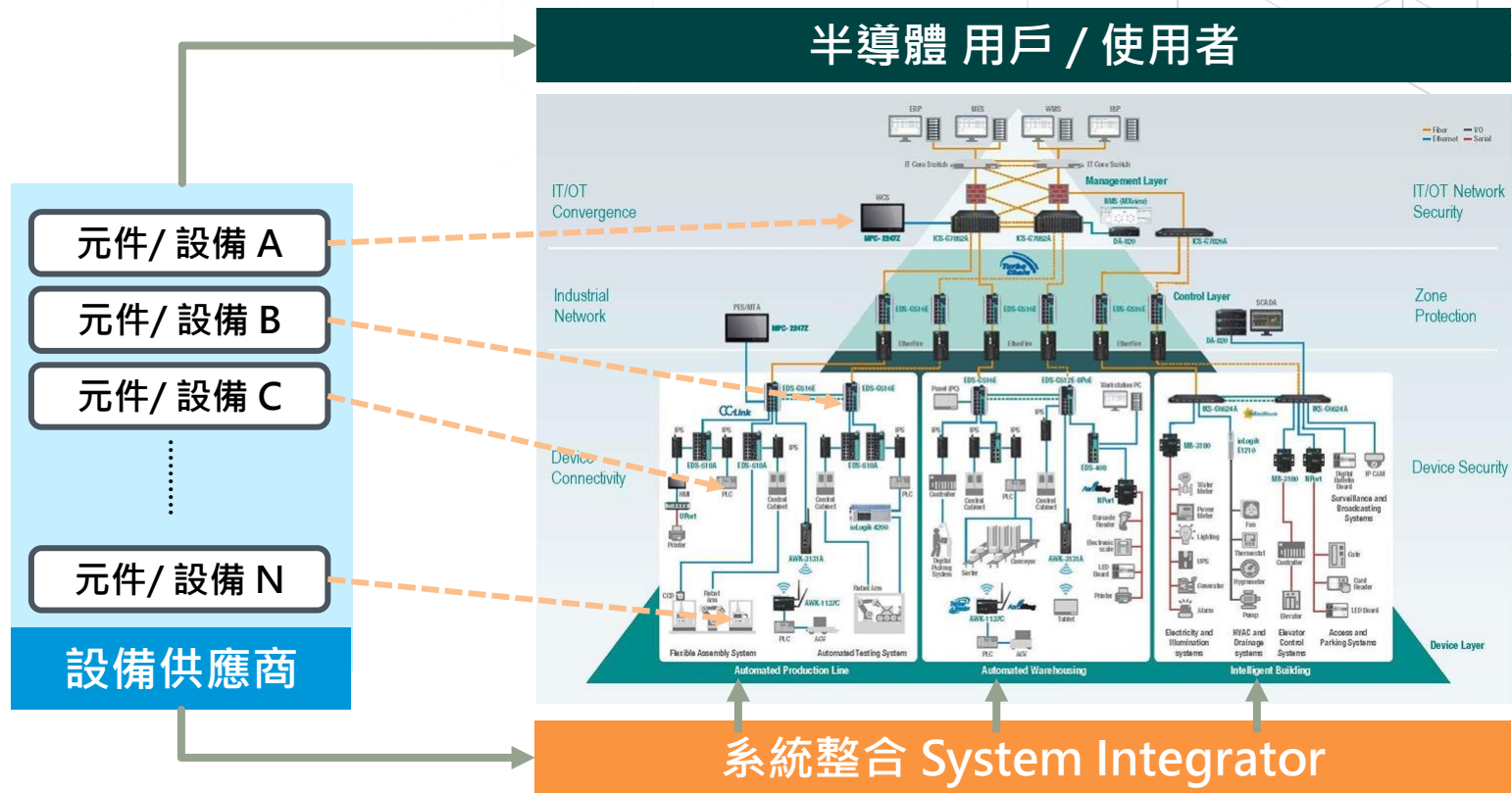
以工業設備
為核心運行

OT 系統安全

IT/OT
資安融合

- 技術封閉性高、多由內部傳承
- 相關的從業人員才有深入了解
- 網路架構設計隨應用屬性客製

OT 資安考量



OT系統安全對策

端點防護技術



- 在每個端點上導入防護軟體
(如: PLC/SCADA/workstations, etc.)
 - 安裝防毒軟體
 - 更新安全補丁
 - 資料加密管理
 - 人員授權控制

協同防禦



網路防護技術



- 透過網路 - 阻擋攻擊傳遞
 - 網路防護縱深防禦
 - 防火牆部署策略
 - 入侵偵測防禦系統 (IDS/IPS)
- 透過網路 - 協同防禦端點
 - 增強對 DoS 攻擊保護
 - 設備漏洞攻擊過濾
 - 設備病毒攻擊過濾

OT 資安建置考量

1) 透過網路 - 強化防禦端點



2) 安全網路架構 (網路防禦)

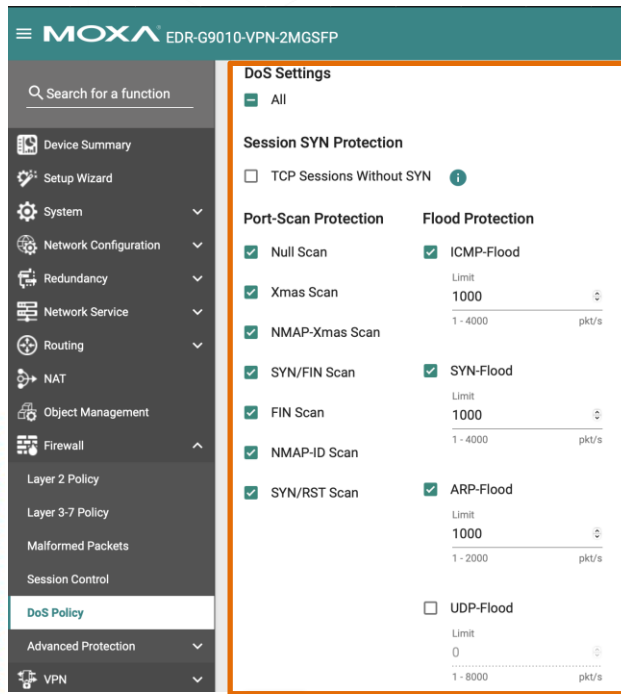
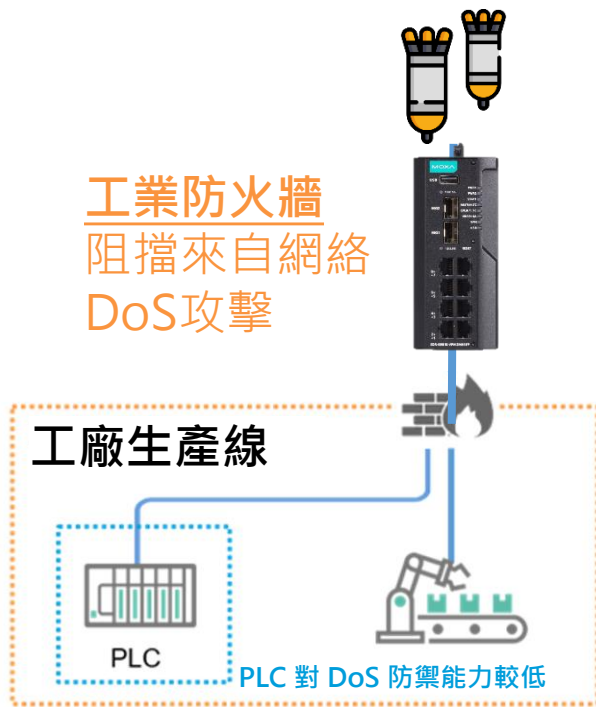
OT 資安建置考量

1) 透過網路 - 強化防禦端點

2) 安全網路架構 (網路防禦)

透過網路 - 強化防禦端點

- 防禦 DoS 攻擊工業控制器



多型態DoS
攻擊模式
非PLC 防護強項

透過網路 - 強化防禦端點

- 封鎖指令攻擊 (工業通訊協議過濾)



工業防火牆
從網路中阻擋
惡意指令攻擊

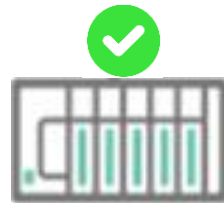


工業控制指令
(例如, Modbus 緊急停機指令)

封包傳入



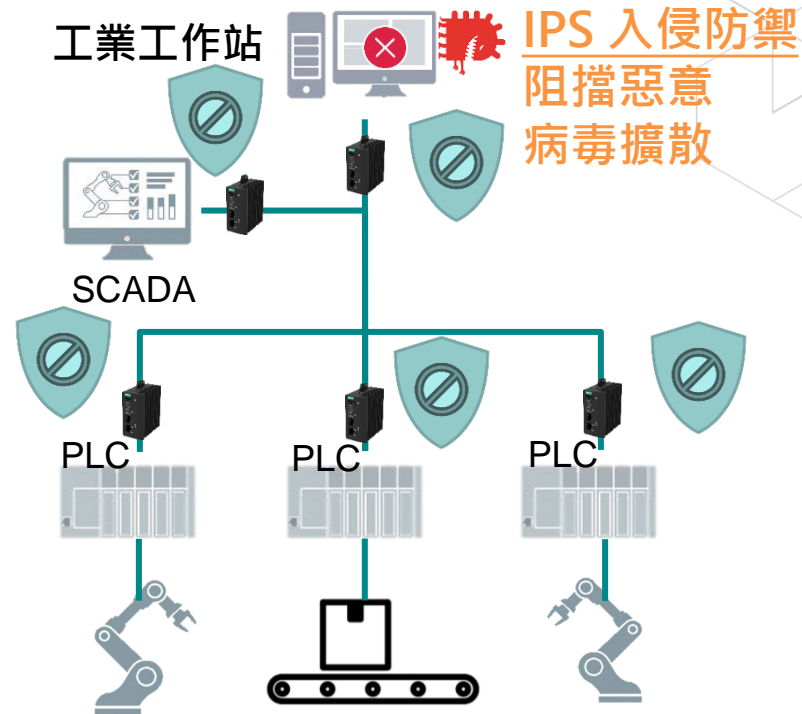
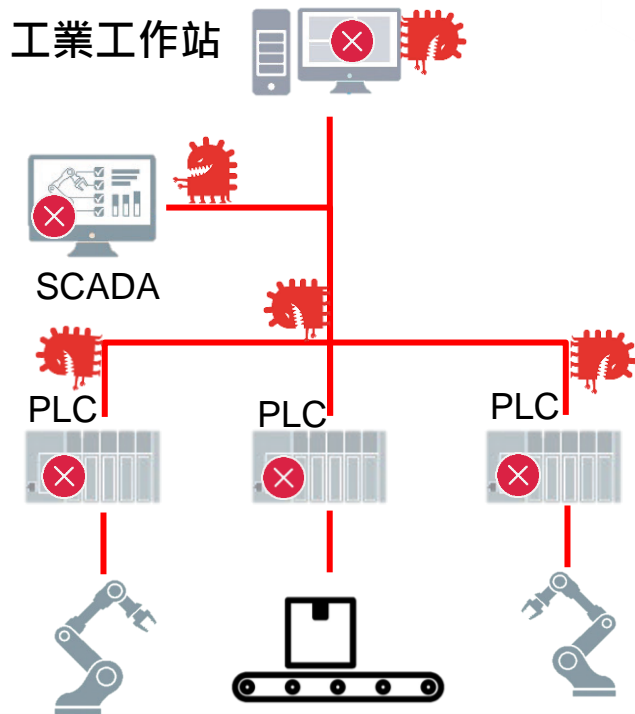
封包傳出



PLC

透過網路 - 強化防禦端點

- 阻擋病毒擴散侵 (IPS, 入侵防禦系統)



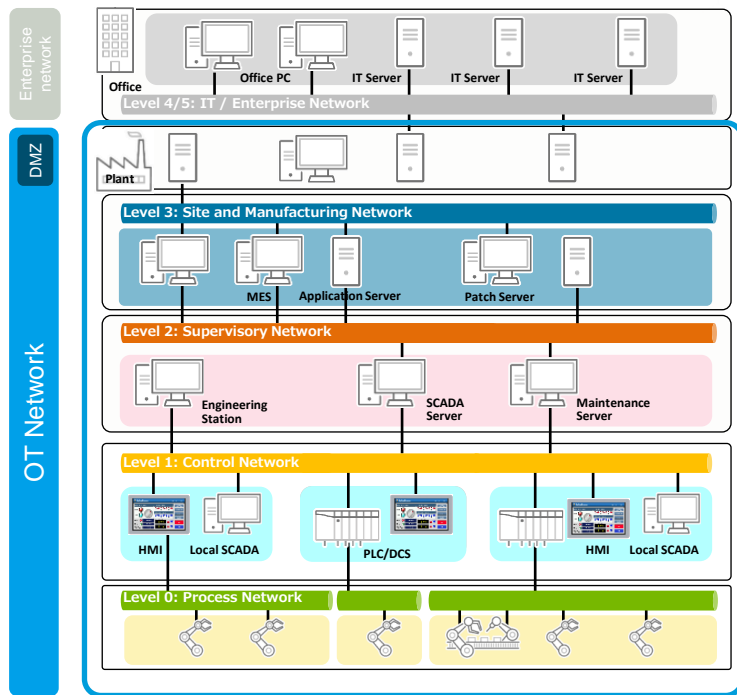
OT 資安建置考量

端點防護 1) 透過網路 - 強化防禦端點

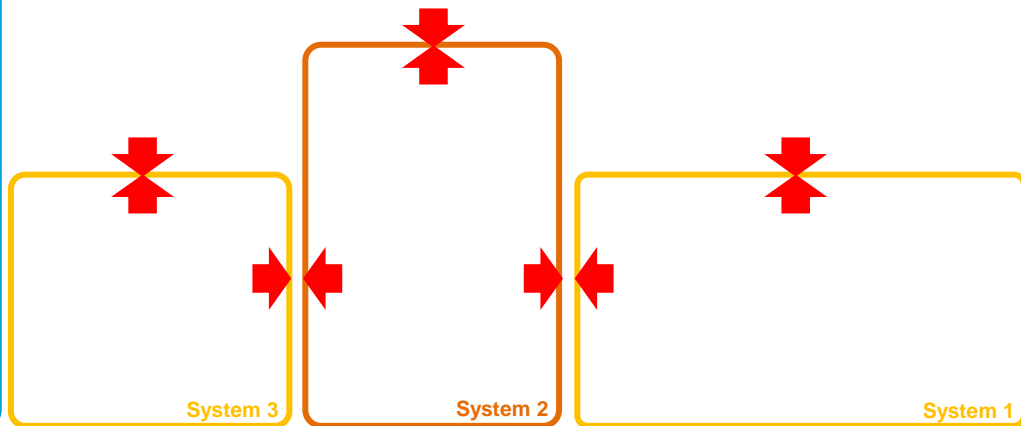
2) 安全網路架構 (網路防禦)

安全網路架構 (網路防禦)

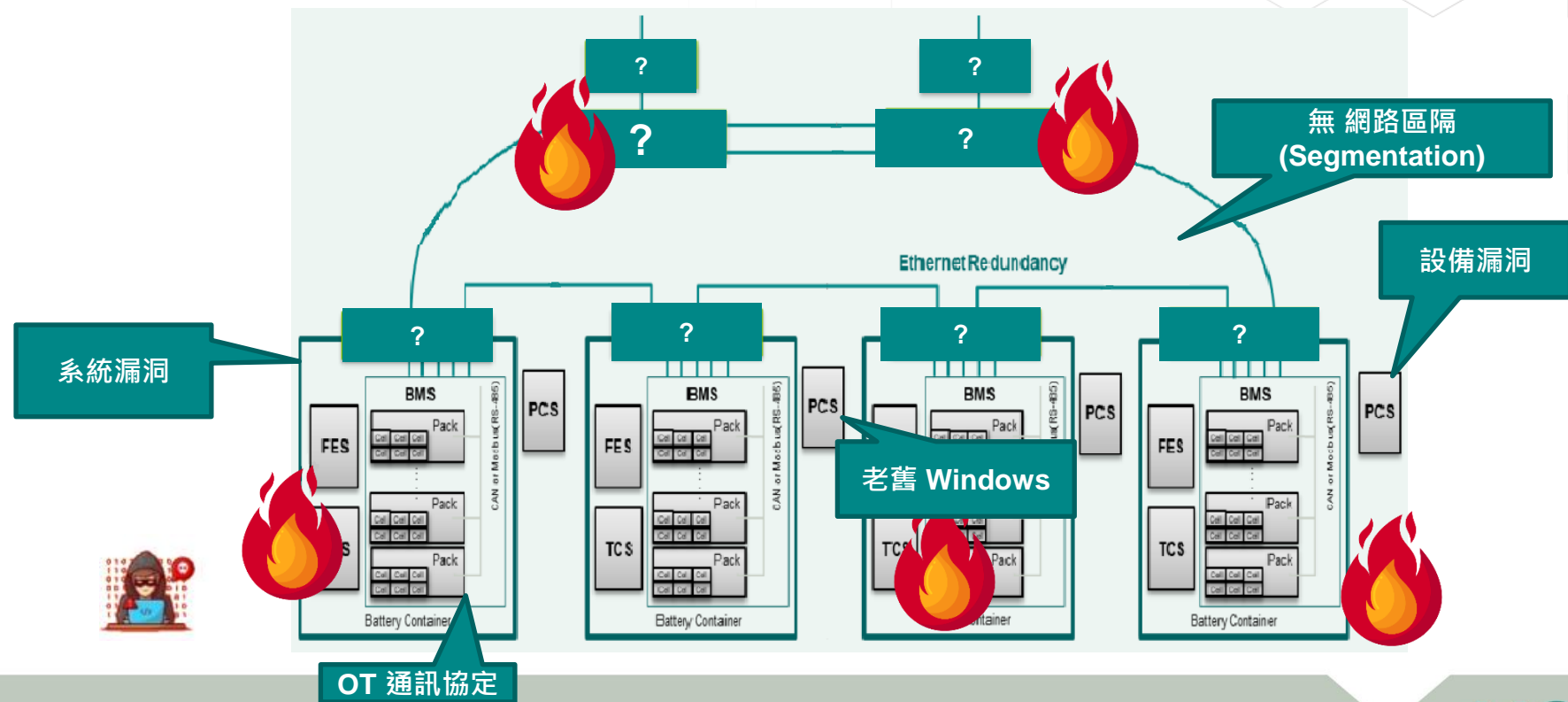
ISA 95 / Perdue Enterprise Reference Architecture (PERA)



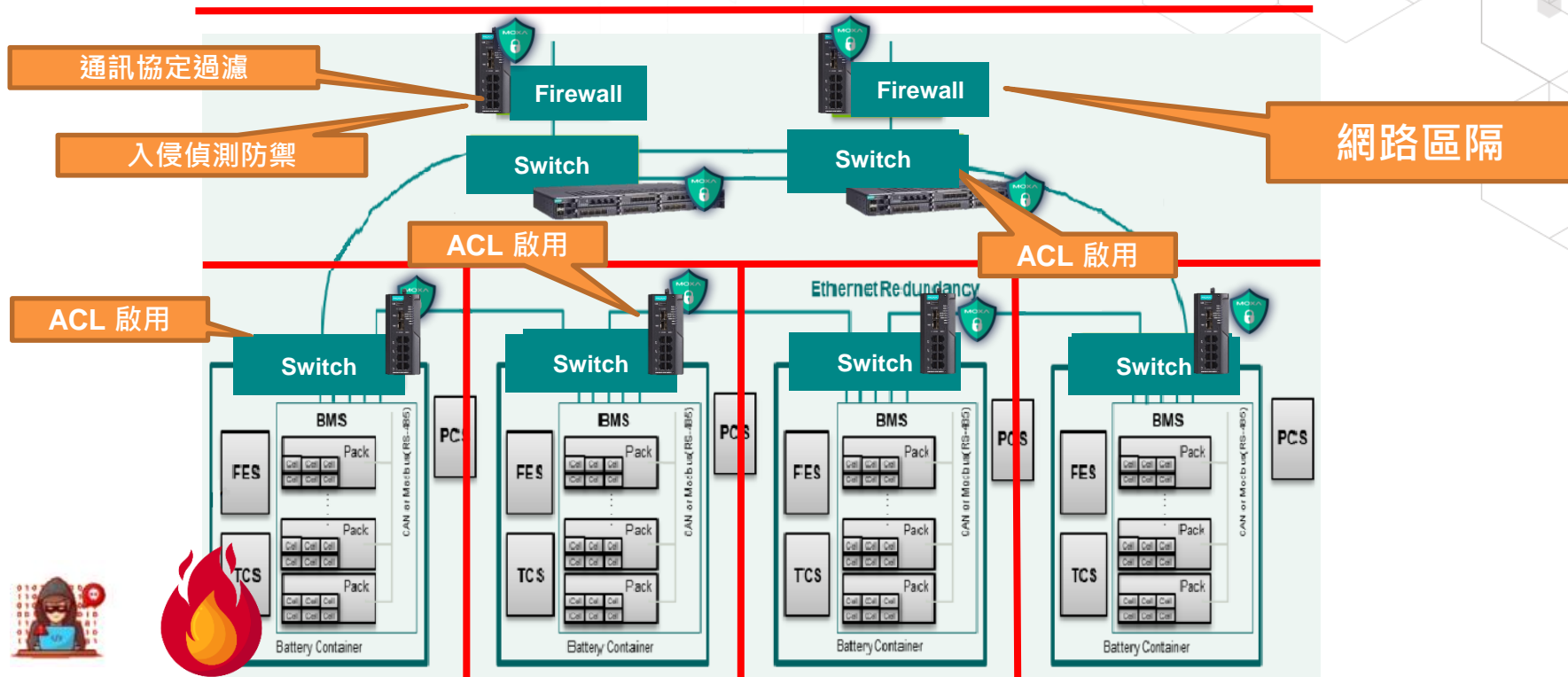
- OT 系統屬於整合性系統
- 系統整合考量
 - 垂直分割
 - 水平分割






案例分享 - OT 網路現狀 (一體化 / 缺網路區隔)



案例分享 - OT 網路強化 (縱深防禦架構)

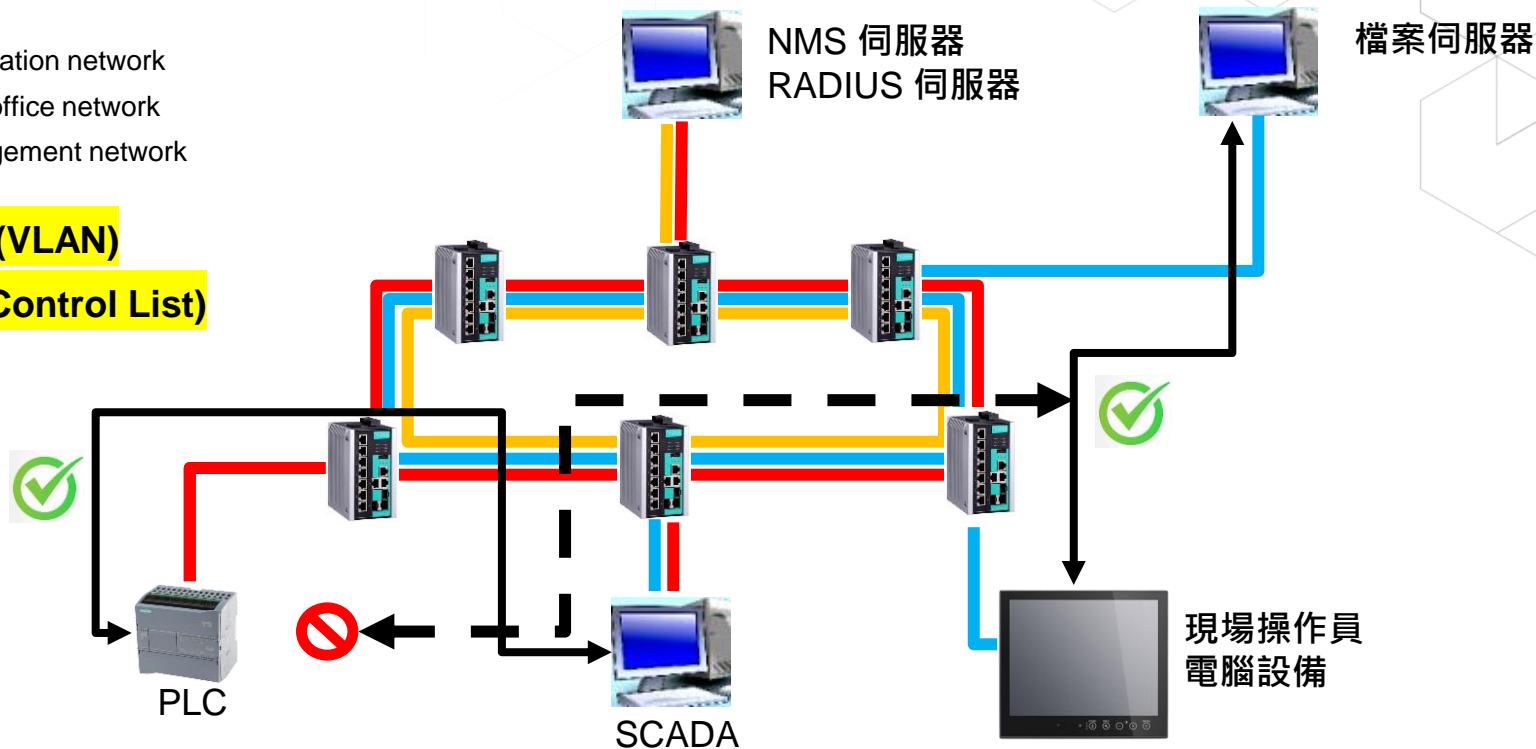


1) 縱深防禦 - 網路交換機進行基礎防護

-  VLAN10 Automation network
-  VLAN20 Field office network
-  VLAN30 Management network

Virtual LAN (VLAN)

ACL (Address Control List)

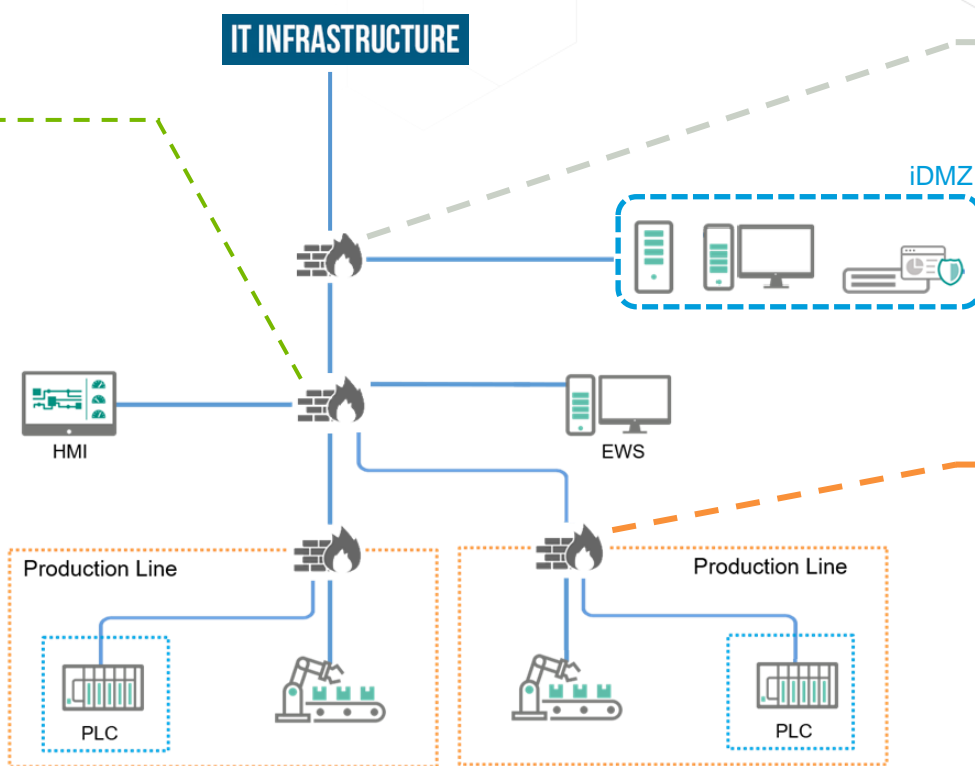


2) 縱深防禦 – 工業防火牆實行網路區隔



Core 次世代防火牆

- GbE supported
- High bandwidth
- Redundancy mechanisms
- IPS / IDS



工業 DMZ

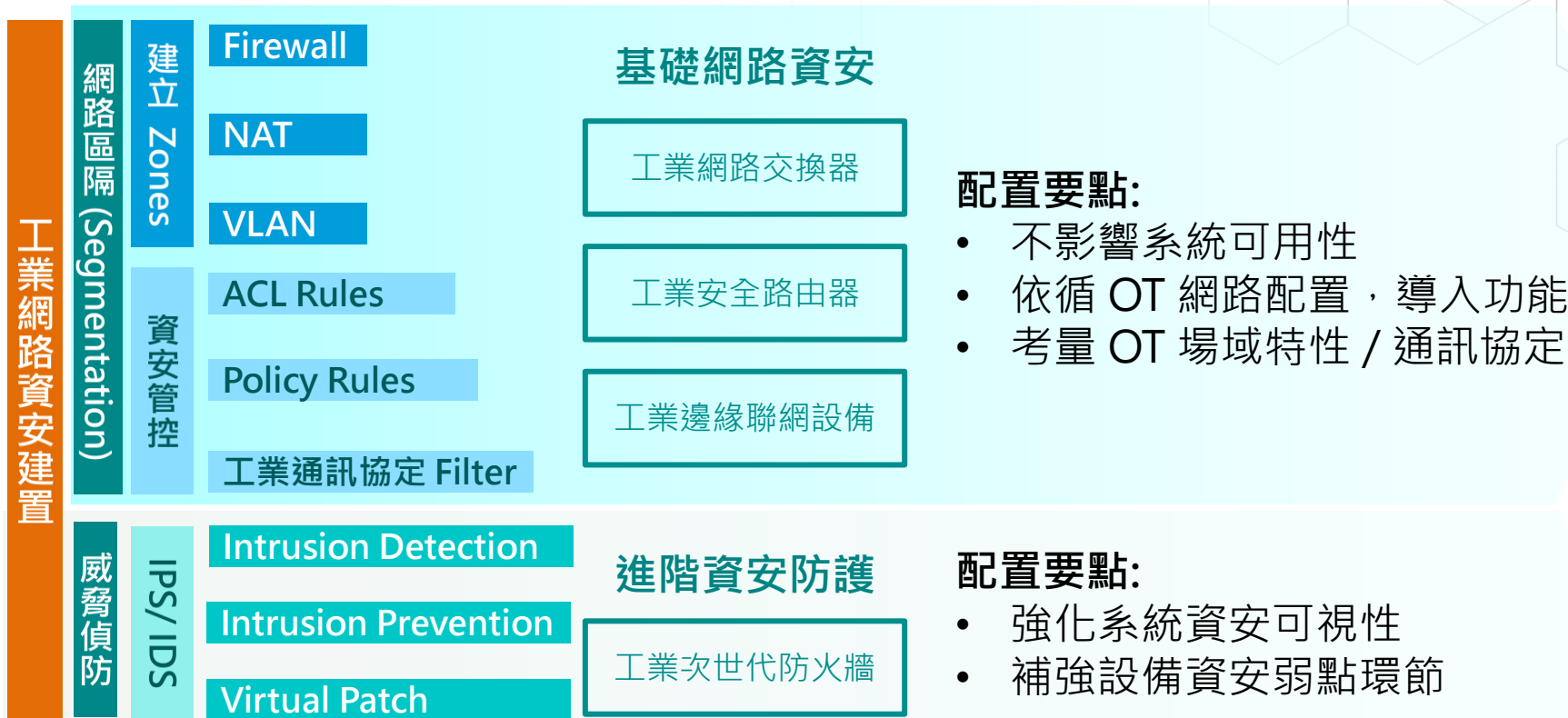
- 10/100/1000 GbE
- DMZ / VPN



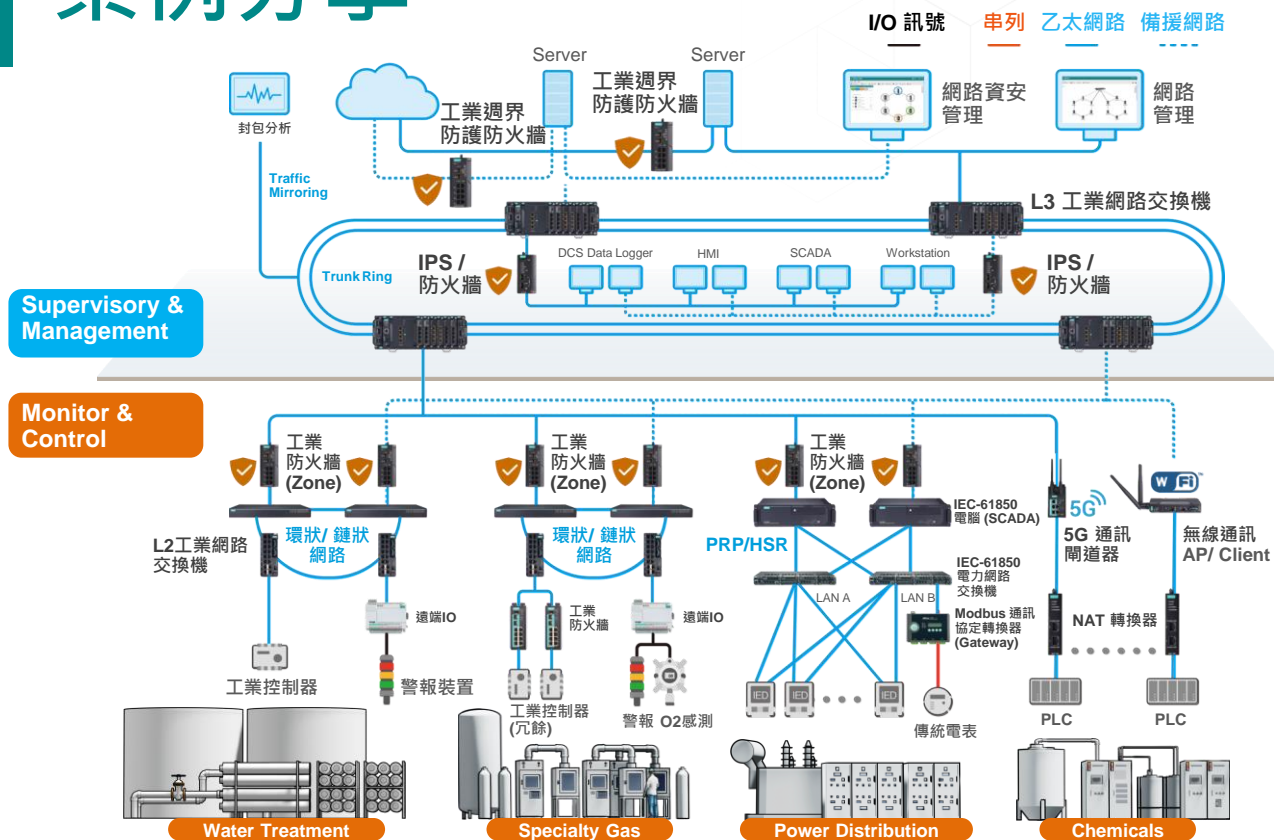
Edge 防火牆

- 10/100 Fast Ethernet
- Turbo Ring
- Firewall with DPI

縱深防禦 – 依照工業網路系統特性配置

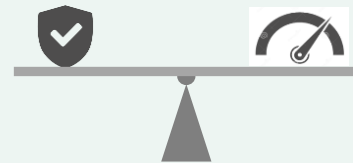


案例分享



資安首要考量

- 不影響系統效能及可用性
- 依工業系統網路規劃防禦



Recap

端點防護對策



- 在每個端點上導入防護軟體
(如: PLC/SCADA/workstations, etc.)
 - 安裝防毒軟體
 - 更新安全補丁
 - 資料加密管理
 - 人員授權控制

網路防護對策



- 透過網路 - 阻擋攻擊行為
 - 防火牆部署
 - 網路保護
 - 入侵偵測防禦系統 (IDS/IPS)
- 網路協同防禦端點
 - 增強對阻斷服務 (DoS)
攻擊保護
 - 漏洞攻擊的過濾
 - 病毒攻擊的過濾

專注工業聯網 新技術發展36年



參與全球六大重點
TSN 測試床，確
保技術高度穩定性
和可靠性

次世代
工業乙太網



5G-ACIA 唯二
OT董事成員之一
推動5G技術於
工業領域應用

OT 5G
領域應用



與趨勢科技結盟，整
合 IT-OT網路資安 /
SEMI E187 設備資
安標準參與成員

次世代工業
安全網路



亞洲唯一參與開發
歐盟新世代列車通
訊網路 (NG-TCN)
網路設備商。

歐盟次世代
列車控制系統