More security,
More freedom

AhnLab Data Diode

單向資料傳輸

AhnLab

台灣區代理商湛揚科技

Contents

01.背景資料

02.產品概述

03.主要功能

04.優勢

05.主要參考

01.
背景資料

1. 增加 OT-IT 連線
2. 超越 OT 環境中的防火牆
3. 單向安全性簡介

增加 OT 與 IT 連線

隨著數位轉型趨勢持續推動網路和系統的互聯，工業設施和關鍵基礎建設逐漸成為安全威脅的首要目標。

	目標	威脅與問題
2022	豐田	豐田日本零件供應商遭駭客攻擊 日本所有工廠停工，每天 10,300 台的生產中斷
2021	佛羅里達州 Oldsmar 水處理廠	破解自來水系統 試圖操控危險化學品的濃度
	殖民地管道	勒索軟體犯罪團體的攻擊導致所有基礎設施癱瘓
	JBS 食品	贖金軟體攻擊關閉大部分程序，支付 1,100 萬美元的比特幣
2020	本田	贖金軟體攻擊導致美國和巴西 9 家工廠停產
	以色列水處理廠	負責以色列供水的工業電腦遭到攻擊 試圖操控混入國家水源的化學物質比例
2019	Norsk Hydro	勒索軟體 (LockerGoga) 感染導致多個金屬擠型作業癱瘓 損失約 477 億韓圜
	杜克能源	因未遵守網路安全規範而支付罰金
2018	石油化工	ICS 目標惡意軟體 (Triton) 感染 利用 Triconex SIS 的漏洞阻斷安全控制系統的執行，導致工廠癱瘓
	台積電	透過損毀的 USB 感染駭客程式 (WannaCry) 部分工廠生產線停工，每天損失約 110 億韓圜
2017	馬士基	以破壞系統為目的的贖金軟體 (NotPetya) 感染
	Mondelez	以破壞系統為目的的贖金軟體 (NotPetya) 感染
2016	烏克蘭	感染 ICS 目標惡意軟體 (Industroyer) 造成大規模停電
2015	烏克蘭電網	控制系統服務因惡意程式碼流入而停止 (BlackEnergy)
2012	Aramco	資料刪除惡意軟體 (Shamoon) 感染造成超過 1 兆的損失

超越 OT 環境中的防火牆

單靠防火牆和 VPN 並不能保證 OT 系統的完全封閉和安全。為了在 OT 與 IT 網路之間建立安全的資料交換，需要更強大的網路週邊安全方法。

防火牆的安全漏洞

有限的安全服務
無法偵測允許流量中的惡意意圖

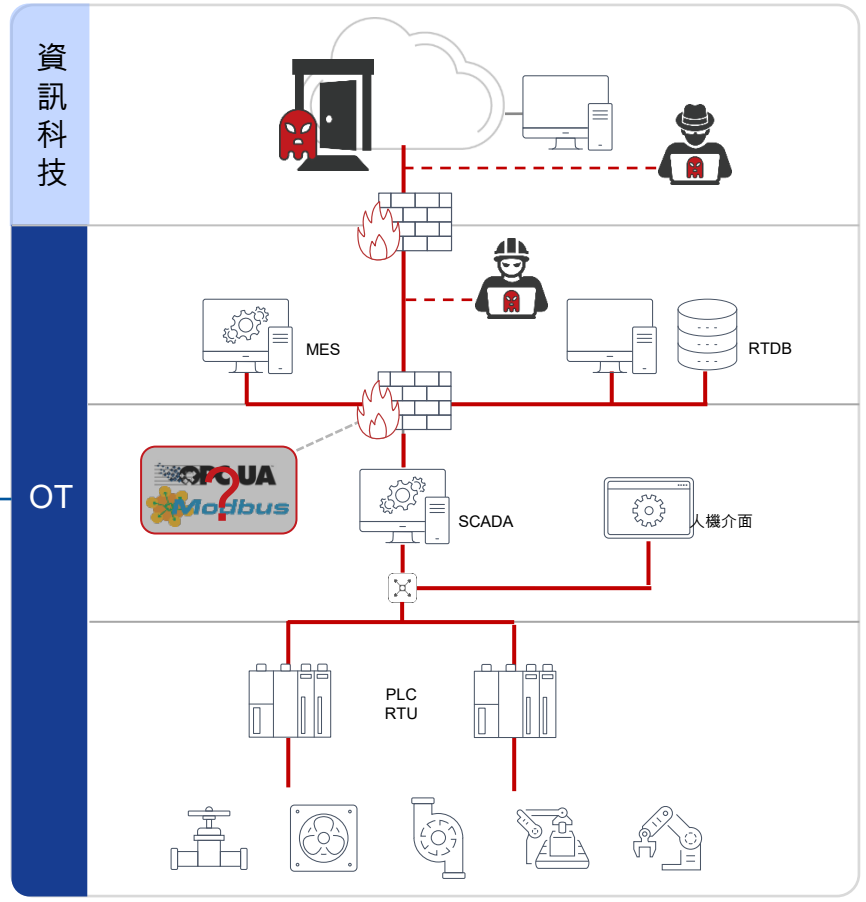
威脅旁路
容易受到隱藏的繞過攻擊，例如後門

內部使用者威脅
即使有嚴格的存取控制，內部人員仍有可能滲透資料

被利用為外部入侵路徑
可能透過暴露於外部網路的開放連接埠入侵

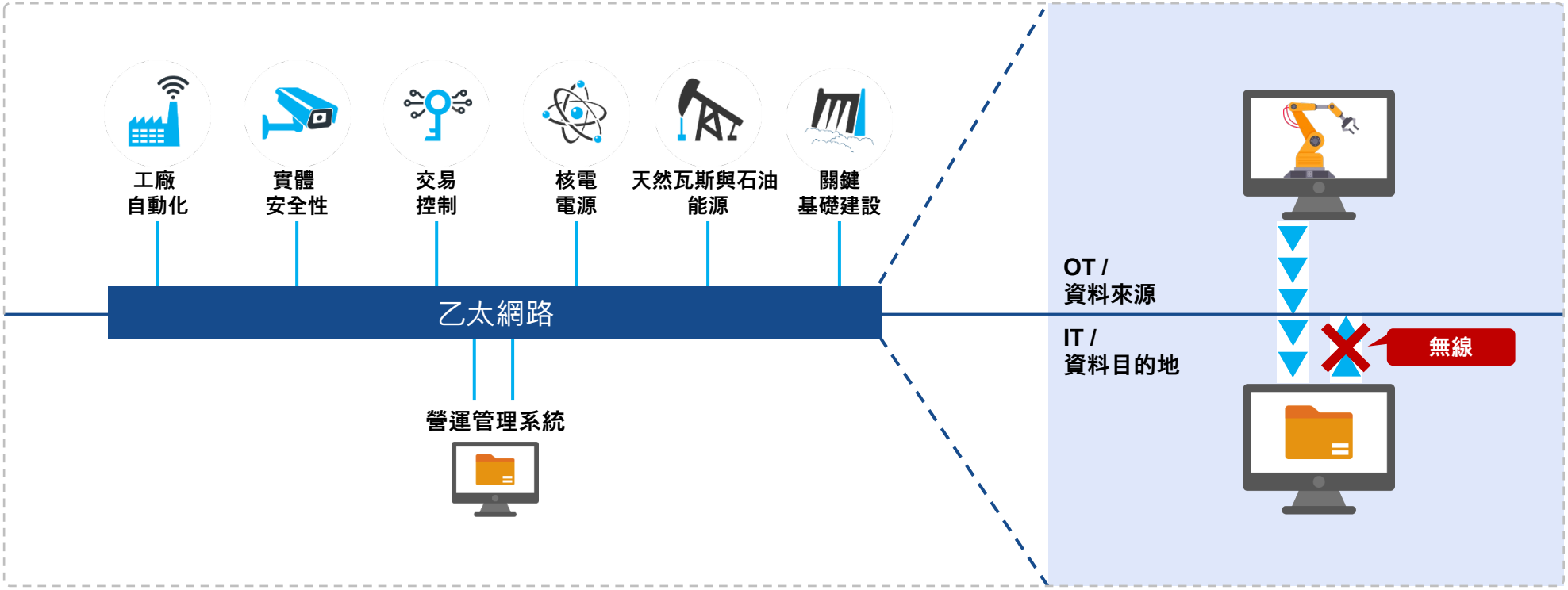
不支援的 OT 通訊協定
防火牆無法辨識工業通訊協定

無法有效對抗不斷演進的網路攻擊
僅能防禦基於 5 元組的預測攻擊



單向安全性簡介

單靠防火牆和 VPN 並不能保證 OT 系統的完全封閉和安全。為了在 OT 與 IT 網路之間建立安全的資料交換，需要更強大的網路週邊安全方法。



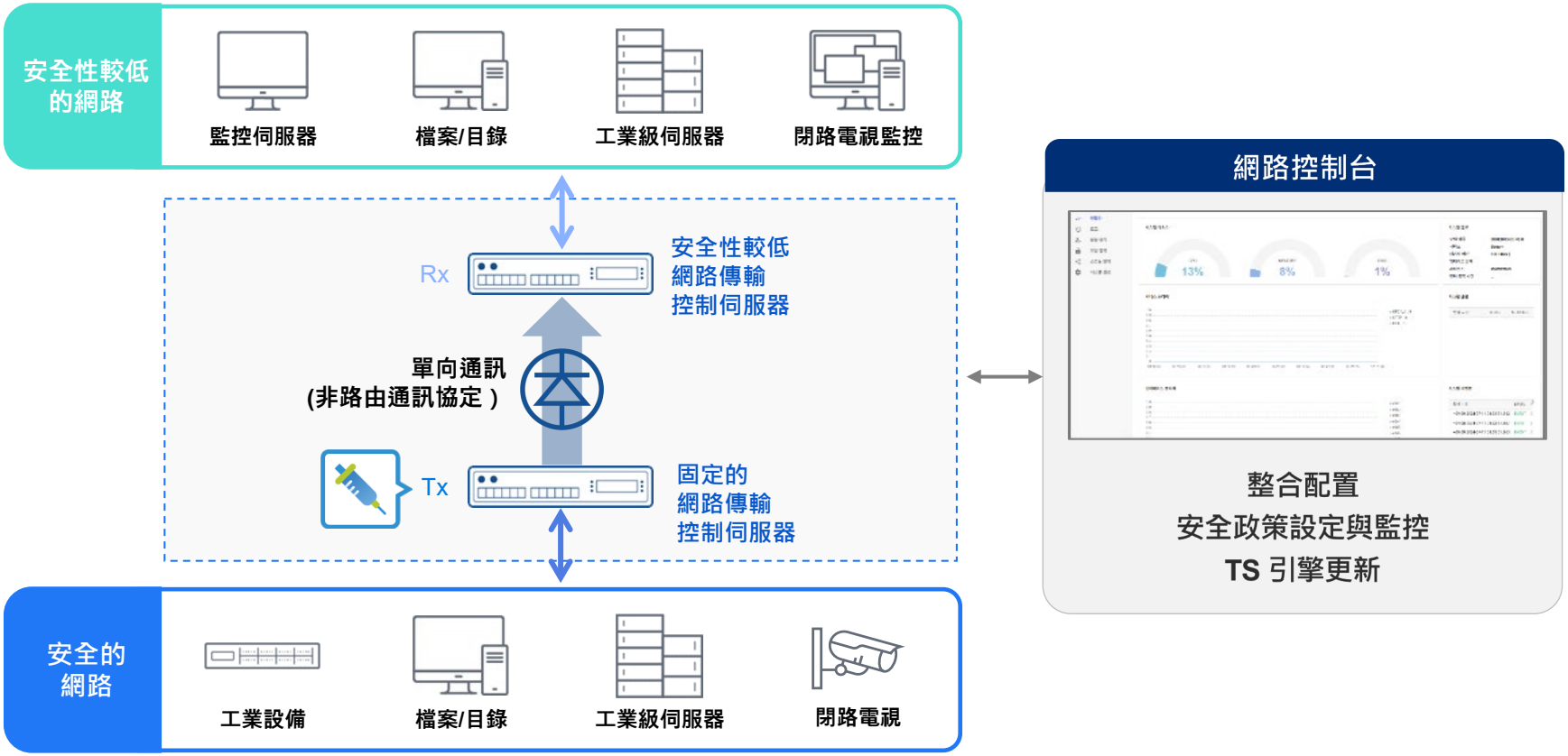
物理單向通訊可保護控制網路，並實現安全的網路整合。

02.
產品總覽

1. 概觀與部署方法
2. 預設設定
3. 產品類型
4. 支援服務與規程

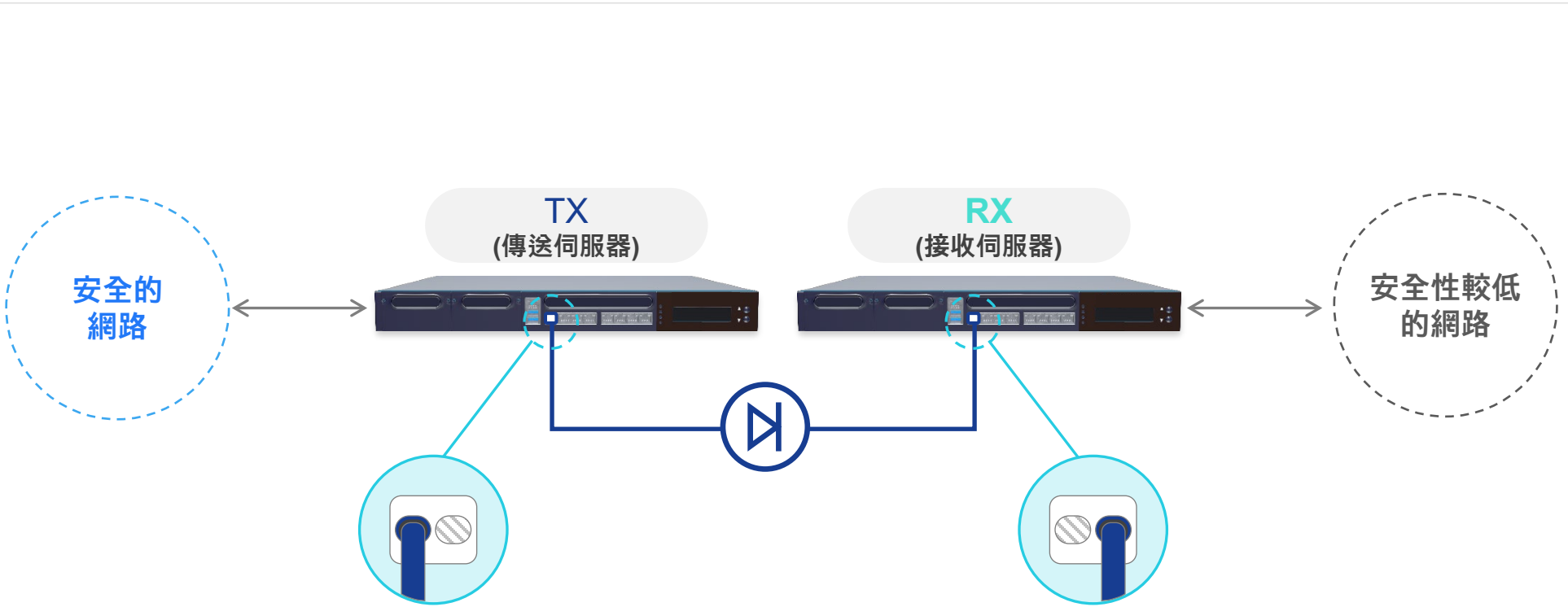
概觀與部署方法

AhnLab Data Diode 是一種實體單向安全解決方案，可在不同安全層級的網路之間進行安全整合。
它由單一組件組成：安裝在資料來源的安全網路中的 TX 伺服器，以及安裝在較不安全網路中接收資料的 RX 伺服器。



預設設定

TX（發送）單元連結至安全網路，可擷取資料並執行物理邏輯單向通訊。位於上層系統的 RX（接收）單元則接收並整合單向安全傳輸的資料。此架構可從根本上阻止任何從較不安全的網路到安全網路的存取嘗試。



由一個 TX 和一個 RX 組成的單組設定範例

產品類型

依據客戶的環境和需求，**AhnLab Data Diode** 提供兩種硬體類型，分別為可拆式和迷你型，並可選擇備援配置。

可拆式

CPU	Intel 四核心 3.6GHz
RAM	16GB
硬碟機	1 TB
NIC	10/100/1000Mbps 8 連接埠
單向 NIC	1/10 Gbps 光纖 * 2 連接埠

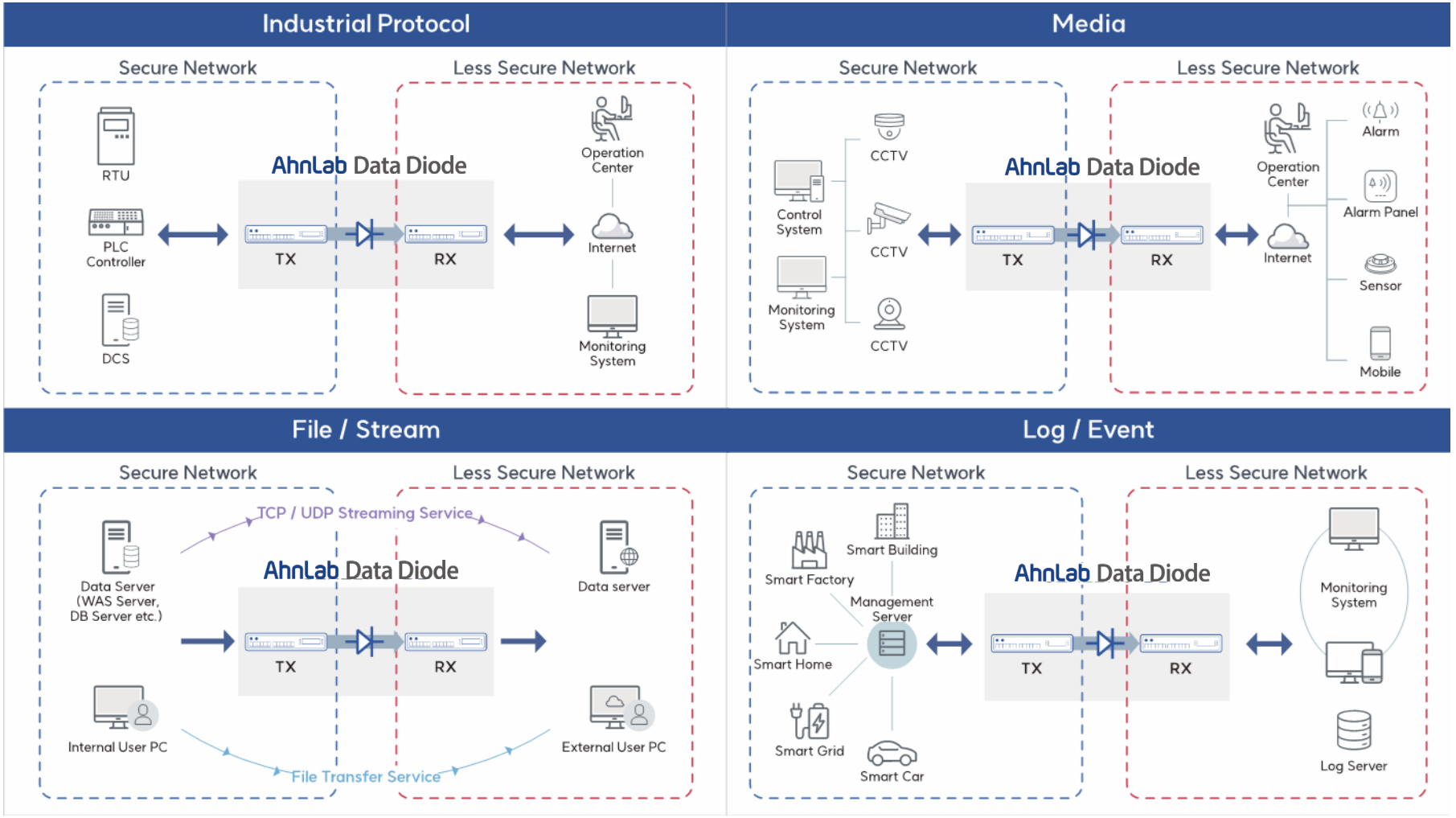
迷你型

CPU	Intel 雙核心 2.2GHz
RAM	8GB
硬碟機	120GB
NIC	10/100/1000Mbps 6 連接埠
單向 NIC	1 Gbps 光纖 * 2 連接埠

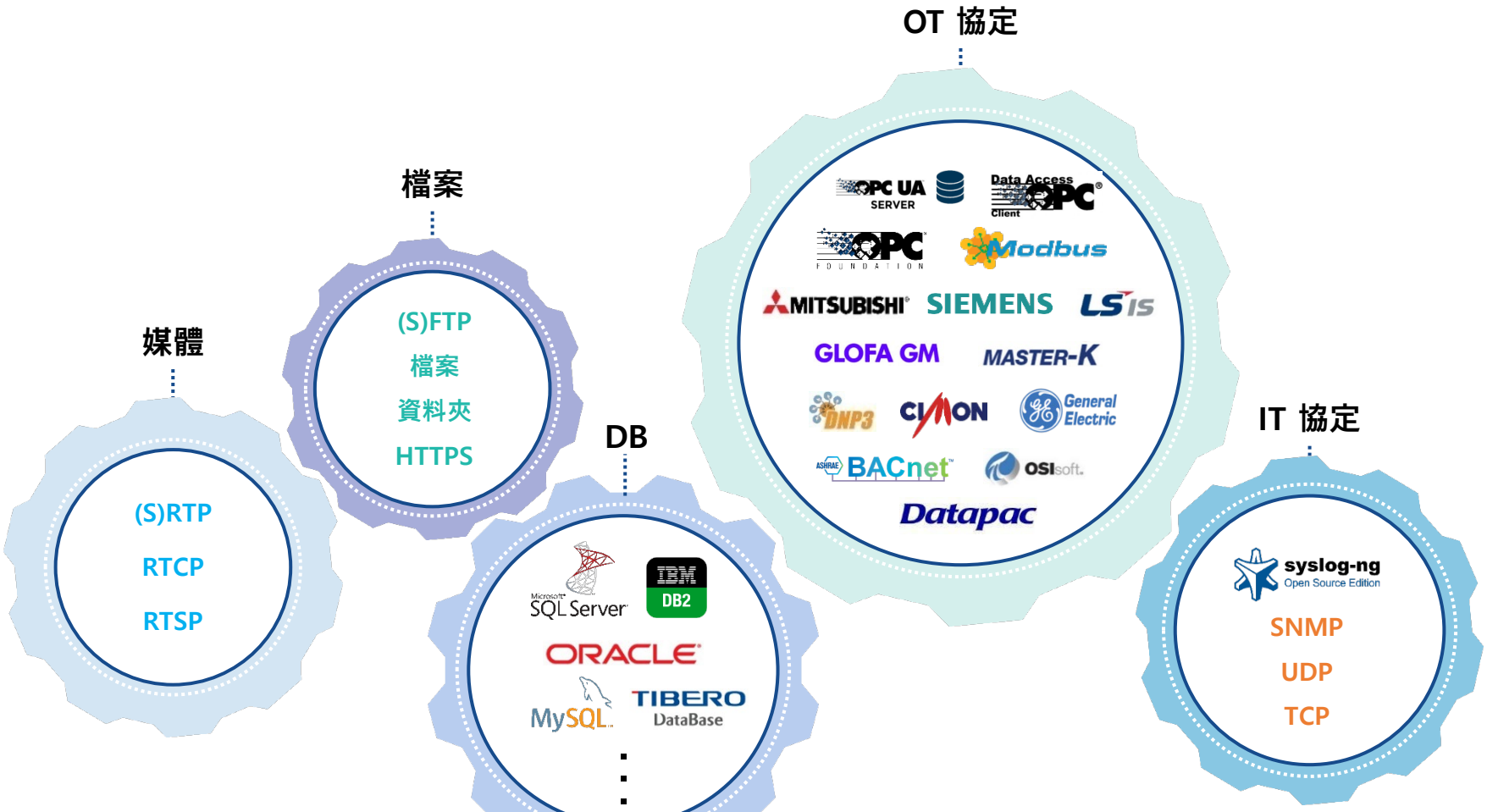
- ❖ 規格僅代表最低要求，可能會依環境而有所修改。
- ❖ 伺服器型號會根據製造商的情況而變更。

支援服務與規程

AhnLab Data Diode 支援各種環境，例如 OT/ICS、檔案與串流連結，以及日誌與事件連結。



支援服務與規程



❖ 可透過專業服務提供額外的通訊協定支援。

03.
主要功能

1. 主要功能
2. 功能詳情
   - 高可靠性
   - 傳輸資料的安全功能
   - 內建通訊協定整合

主要功能

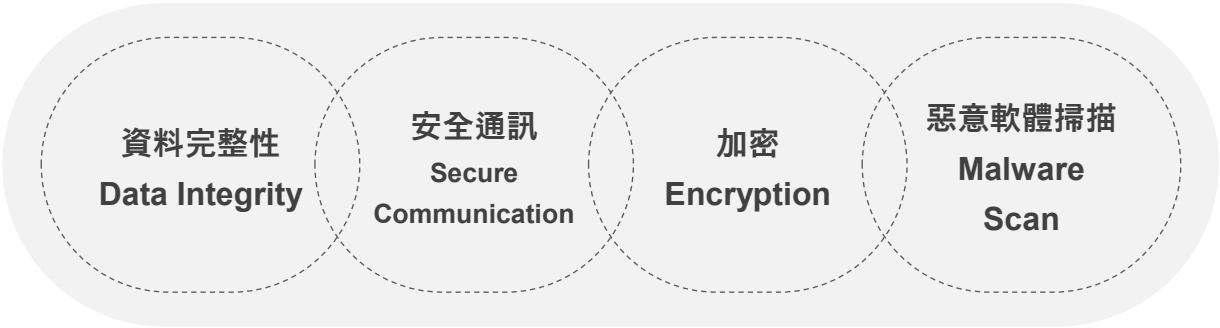
單向通訊

- 配備單向網卡的硬體
- 單向傳輸的通訊協定

- Tx 和 Rx 實體分離
- 只有 Tx 實體連接，而 Rx 則斷開連接
- 不會從較不安全的網路反向傳輸至安全的網路
- 即時資料傳輸，不會遺失資料

傳輸資料保護

- 單向資料傳輸加密
- 前向錯誤校正 (FEC)
- 防毒 (AV) 的 TS 引擎



支援 各種使用個案

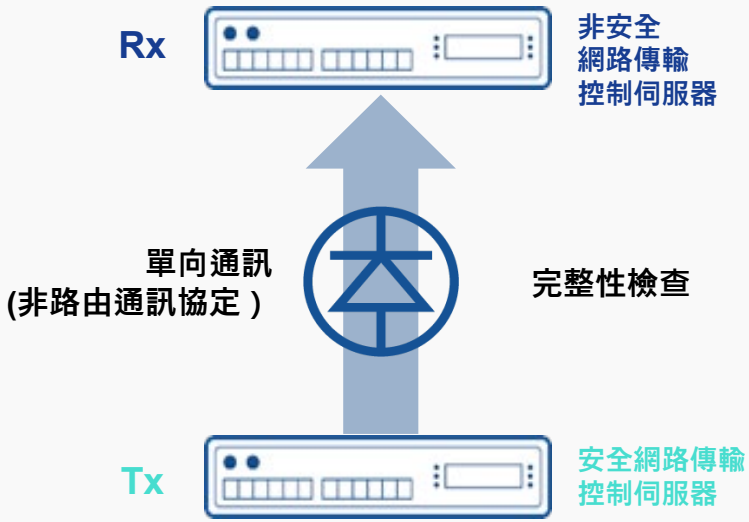
- 與 CCTV、OT 設備、DB、檔案等整合。
- 異質通訊協定轉換

媒體	(S)RTP、RTCP、RTSP	OT 協定	OPC UA/DA/AE、Modbus
檔案	(S)FTP、檔案、資料夾、HTTPS		Emerson、MelsecA/Q、SIEMENS S7、GLOFA-GM、Fatek、LS ELECTRIC XGK/XGI/XGB/XGR、MASTER-K、DNP3、CIMON、Unitronics、Omron、BACnet、Yaskawa、Yokogawa 등
DB	MS_SQL、Oracle、MySQL、DB2、Tibero 等	IT 協定	Syslog、UDP、TCP、SNMP

特點 (1) - 高可靠性

結合軟體強制的單向通訊協定與最佳化的硬體配置，此解決方案可提供最高等級的實體單向傳輸。

單向通訊協定 SW



用於單向通訊的 HW

RX 的 NIC 設定

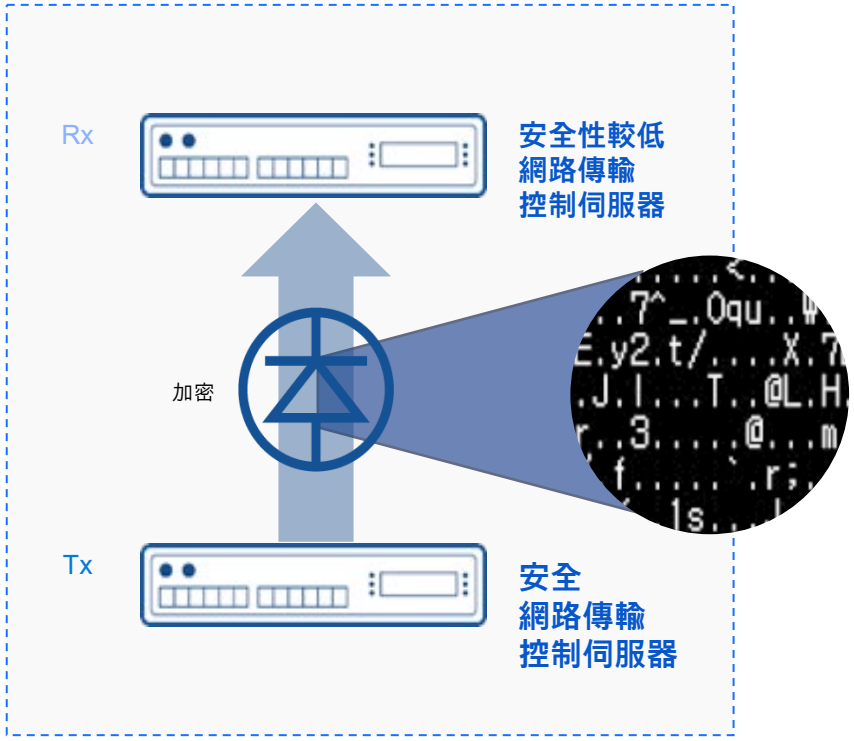
TX 的 NIC 設定

❖ 範例有助於瞭解硬體配置。實際設定可能有所不同

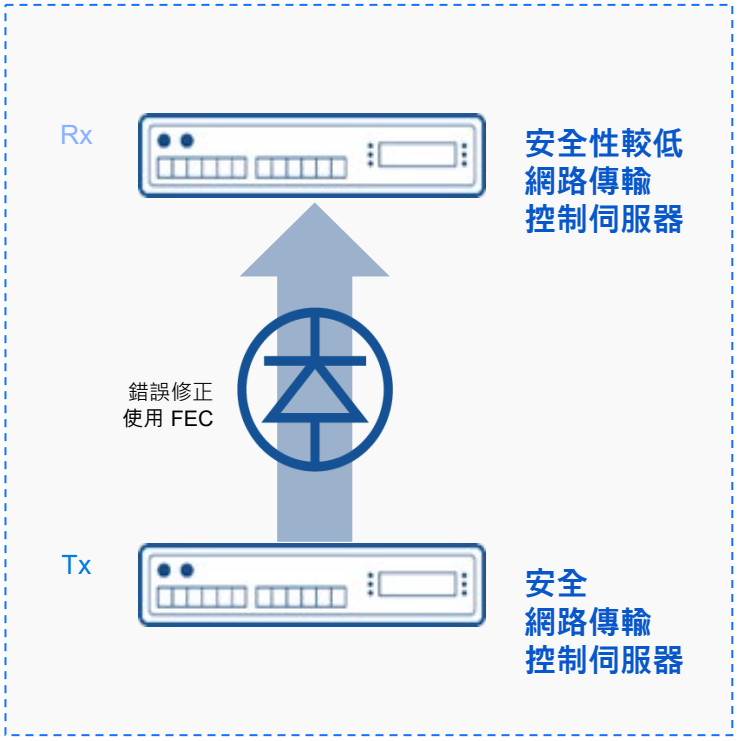
功能 (2) - 傳輸資料安全性

即使資料在傳輸過程中發生洩漏，也能透過加密來維護資料的機密性。此外，前向錯誤糾正 (FEC) 可在不可能重新傳輸的物理單向環境中，確保最大的資料完整性和可用性。

資料保密性

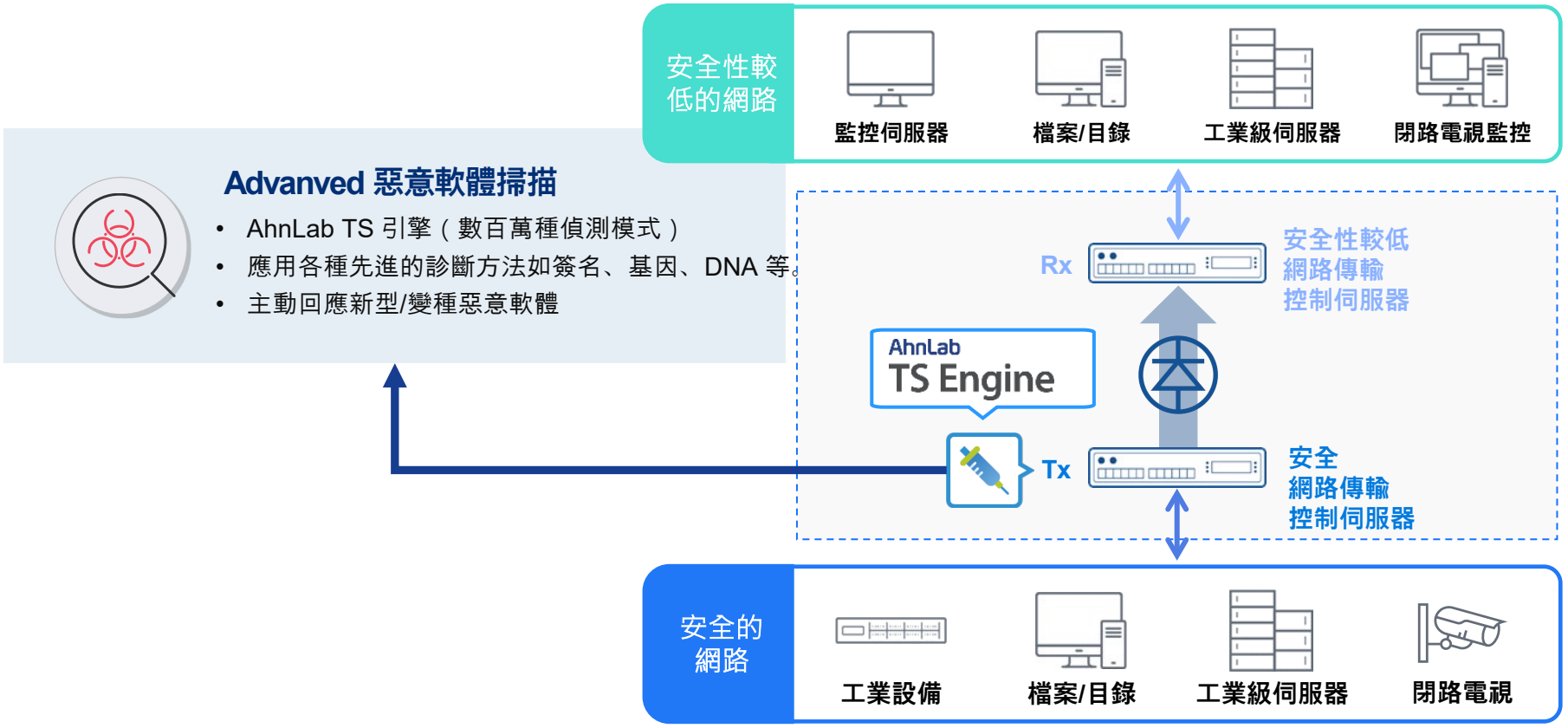


資料完整性與可用性



功能 (2) - 傳輸資料安全性

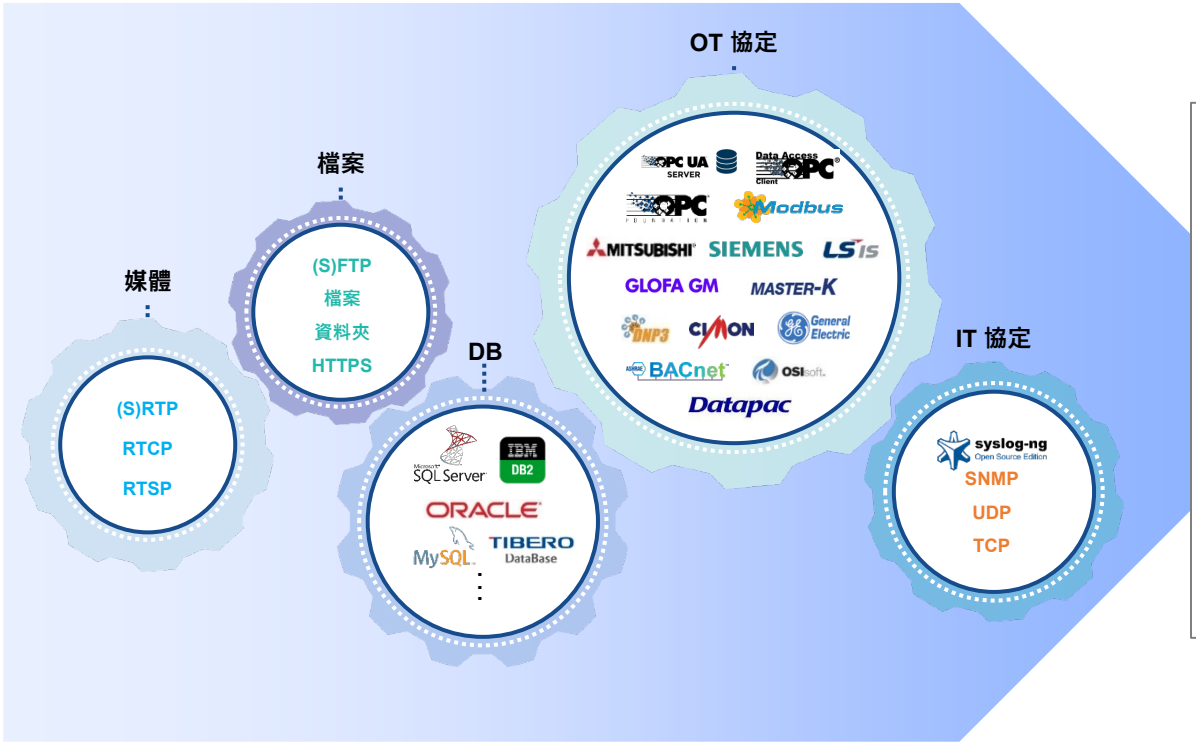
即使資料在傳輸過程中發生洩漏，也能透過加密來維護資料的機密性。此外，前向錯誤糾正 (FEC) 可在不可能重新傳輸的物理單向環境中，確保最大的資料完整性和可用性。

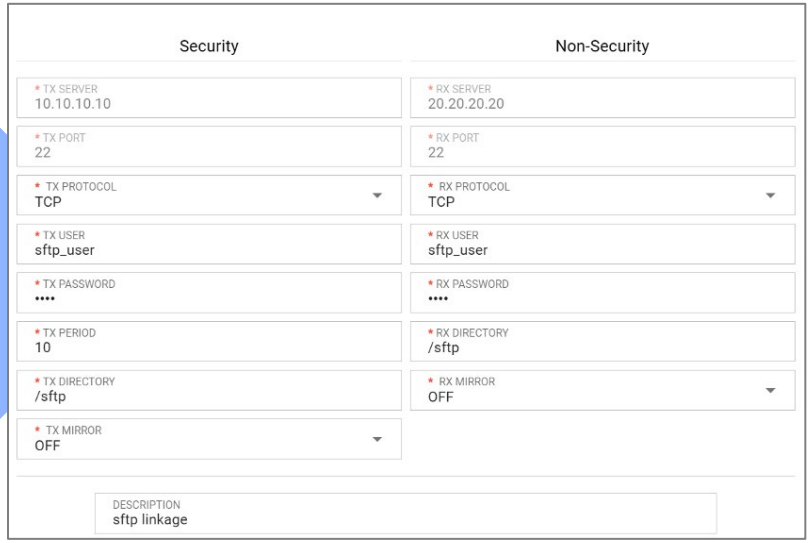


功能 (3) - 內建通訊協定轉換

透過可與工業設備和資料庫連線的專屬技術，以及內建的異質通訊協定轉換功能，支援安全且彈性的服務整合。

透過相關產品建立與 150 多個主要工業系統的可靠連線，提供彈性的服務整合





❖ 透過直覺式 GUI 介面提供獨立的整合功能。

04.
優勢

1. 增強可靠性與安全性
2. 彈性整合
3. AhnLab CPS PLUS - CPS 保護平台

優勢

單向通訊
One-way communication

- 配備單向網卡的硬體
- 單向傳輸的通訊協定

傳輸資料保護
Transmitted Data Protection

- 單向資料傳輸加密
- 前向錯誤校正 (FEC)

支援各種使用個案
Support Various Use Cases

- 與 CCTV、OT 設備、DB、檔案等整合。
- 異質通訊協定轉換

可靠性 Reliability

- 透過 FEC 提供傳輸可靠性
- 單向傳輸區段的通訊協定

安全性Security

- 遵守控制系統安全與資料傳輸準則
- 資料傳輸前進行管理政策/簽章/惡意軟體掃描

隨選擴充能力
On-demand Scalability

- 從 100 Mbps 到 1/10 Gbps 的可擴充傳輸速度
- 透過備援配置提供高可用性環境

彈性整合
Flexible Integration

- 與 CCTV、OT 設備、DB、檔案等整合。
- 異質通訊協定轉換
- 與專門的整合程式相容，並提供客製化的技術支援

優點 (1) - 強化可靠性與安全性

Data Diode 可利用其物理特性強制執行單向傳輸，確保資料的完整性、機密性和可用性，從而保證網路分割等級的安全性，並最大化資料可用性。(被公認為韓國唯一的物理單向傳輸創新產品)

1) 主動式防護 ：透過 TS Engine 回應惡意軟體

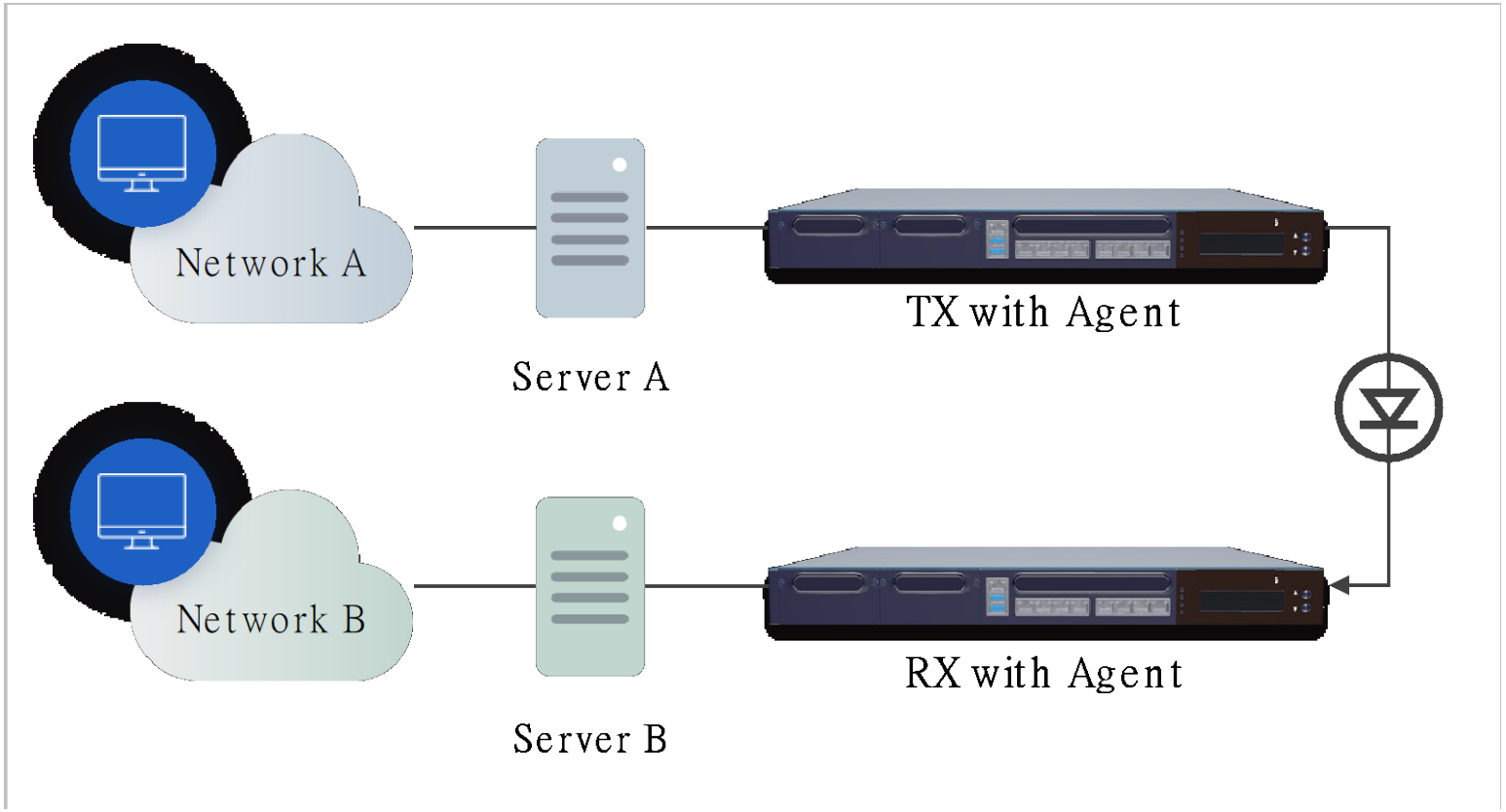
2) 資料保密性：單向通訊的通訊協定與加密

3) 完整性與可用性：前向錯誤校正 (FEC)、完整性檢查

4) 物理安全的單向傳輸路徑(Physically secured one-way transmission path)

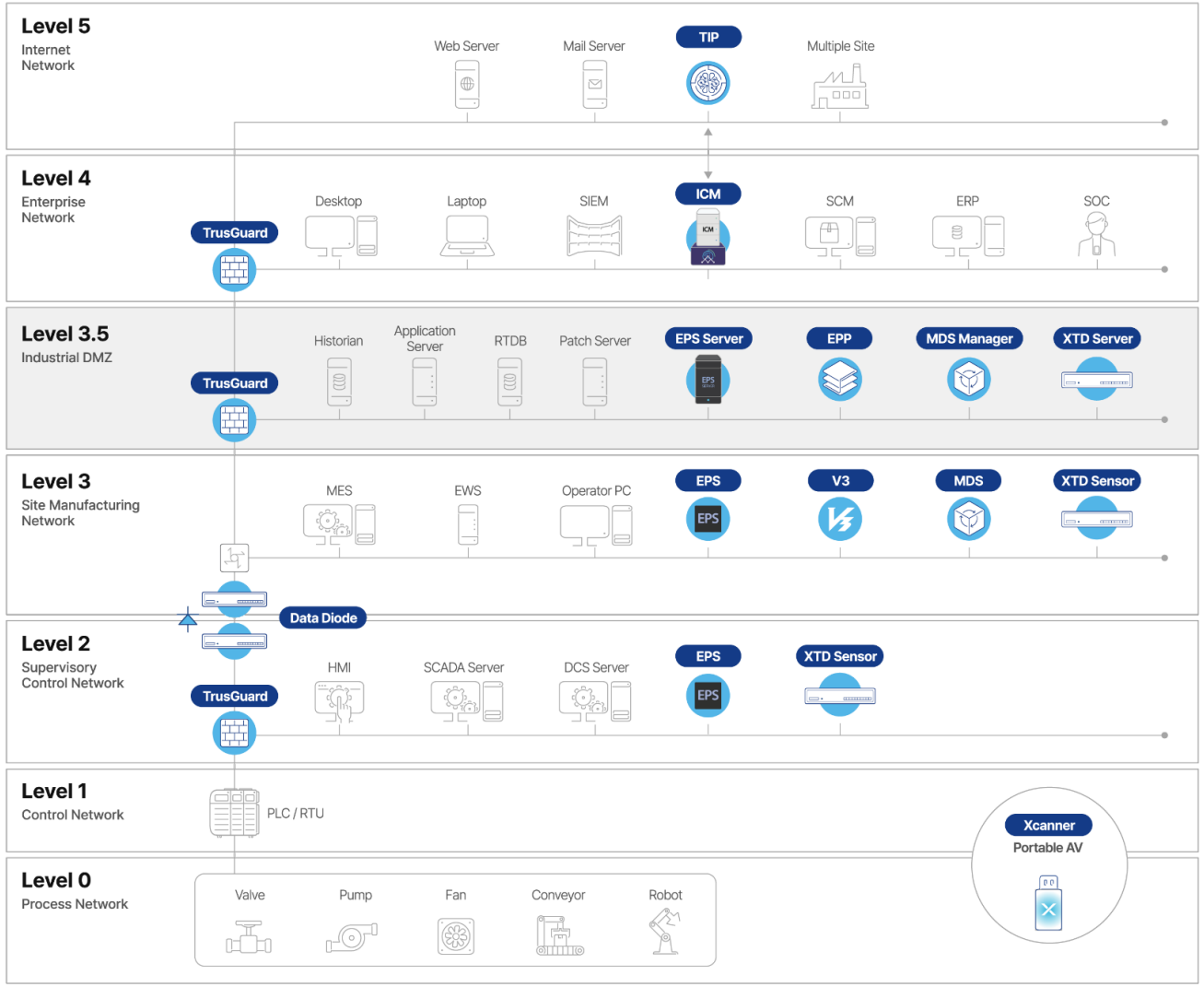
優勢 (2) - 彈性整合

Data Diode 採用內建的整合方式，可避免使用獨立的中繼伺服器，進而將管理點降至最低。它也透過專業服務支援客戶最佳化的組態，提供客製化功能，例如異質通訊協定的內建轉換，以及與專門整合程式的相容性。



優勢 (3) - AhnLab CPS PLUS

作為 AhnLab CPS PLUS 的一部分，AhnLab Data Diode可透過與其他 CPS 解決方案的協同作用增強安全性。



ICM
- CPS 的中央監控/管理
  - SIEM/SOC 互操作

EPS
- CPS 的端點安全
- 基於允許清單的應用程式/裝置控制

Xcanner
- 可攜式 AV
- 與 AhnLab EPS 整合

V3 / EPP
- 伺服器和個人電腦的 AV
- V3 中央和裝置修補程式管理

MDS
- 網路沙箱的威脅分析
- 漏洞與惡意軟體偵測

TrusGuard
- OT 的網路安全
- 網路分割

TIP
- IT/OT 威脅情報

XTD
- 用於資產/流量可視性的 IDS
- 惡意軟體/流量/通訊協定異常偵測

Data Diode
- 單向資料傳輸

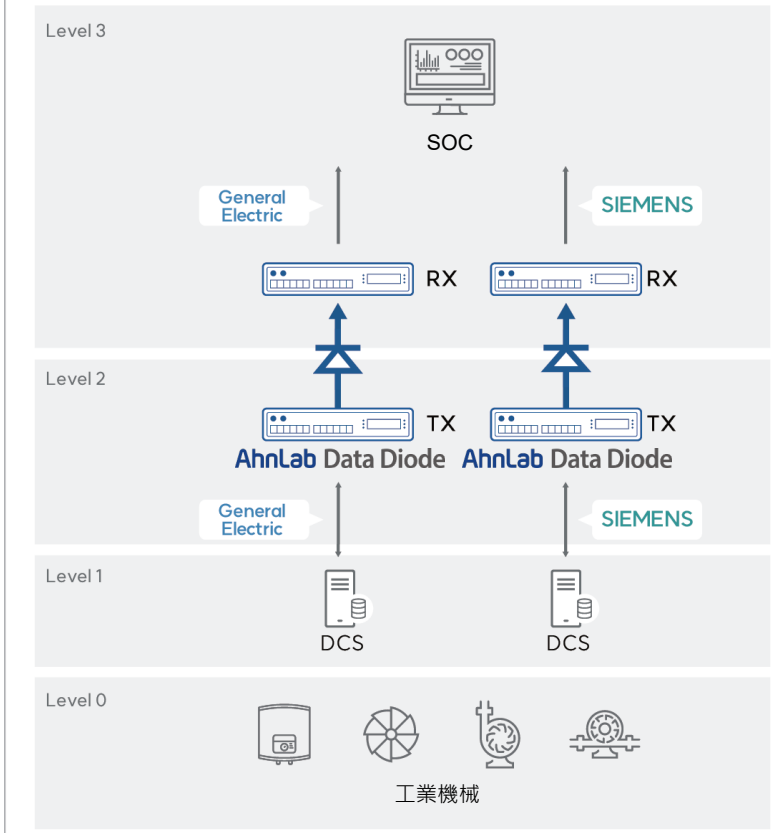
05.
參考

1. 工業設備
2. 辦公室自動化
3. 商業網路整合
4. 資料庫整合
5. 系統管理
6. 監控與監督

AhnLab 台灣區代理商湛揚科技

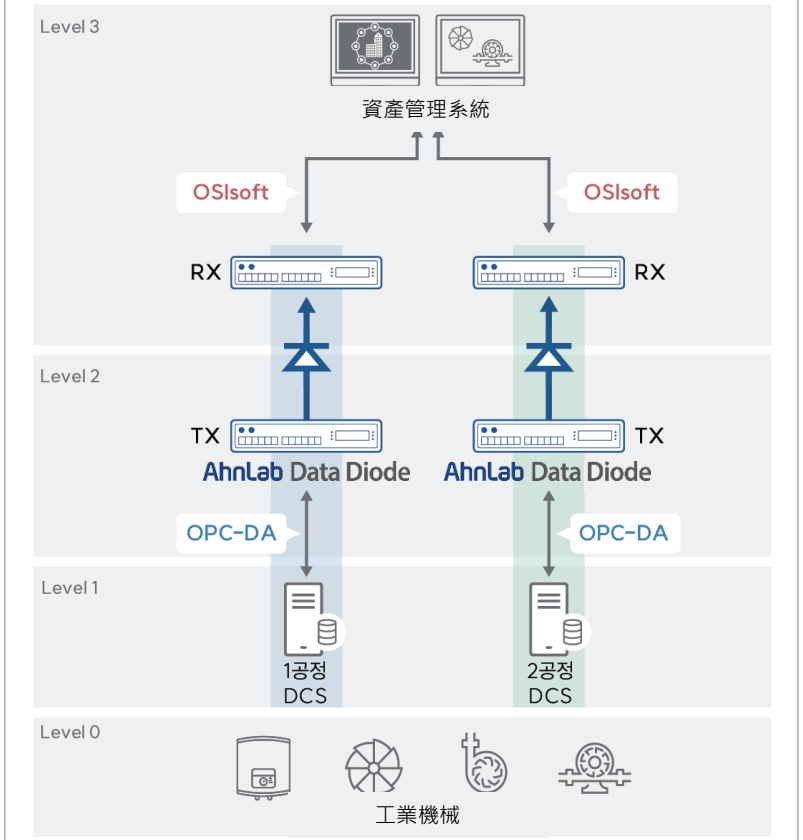
工業設備

安全控制系統



- 從整合發電網路到安全控制系統的單向連接

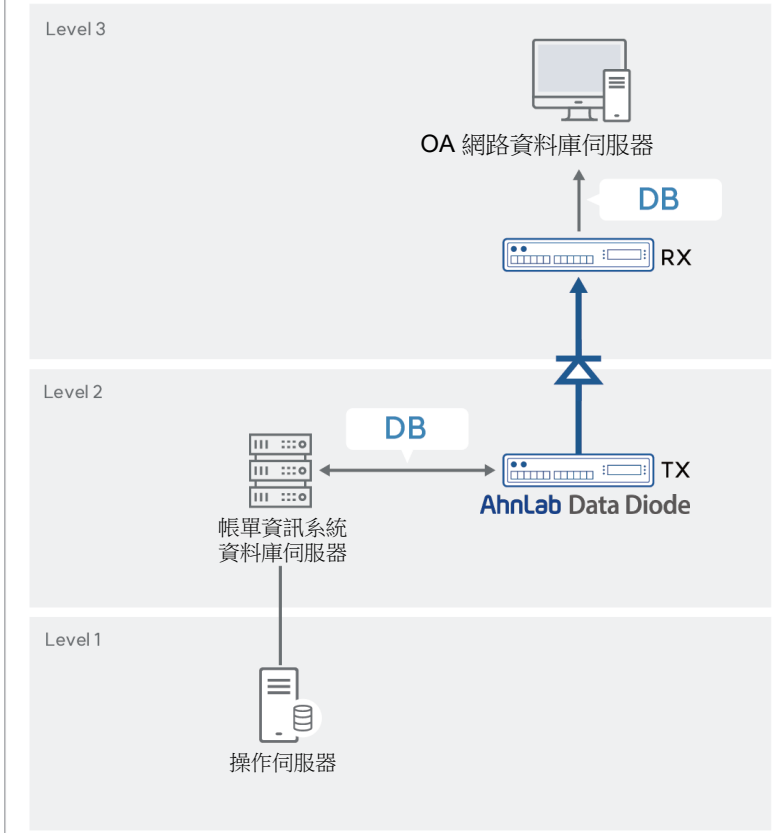
操作資訊資料連接系統



- 從電網 DCS 到 OSIsoft PI 資產管理系統的 OPC-DA 標籤資料單向連接

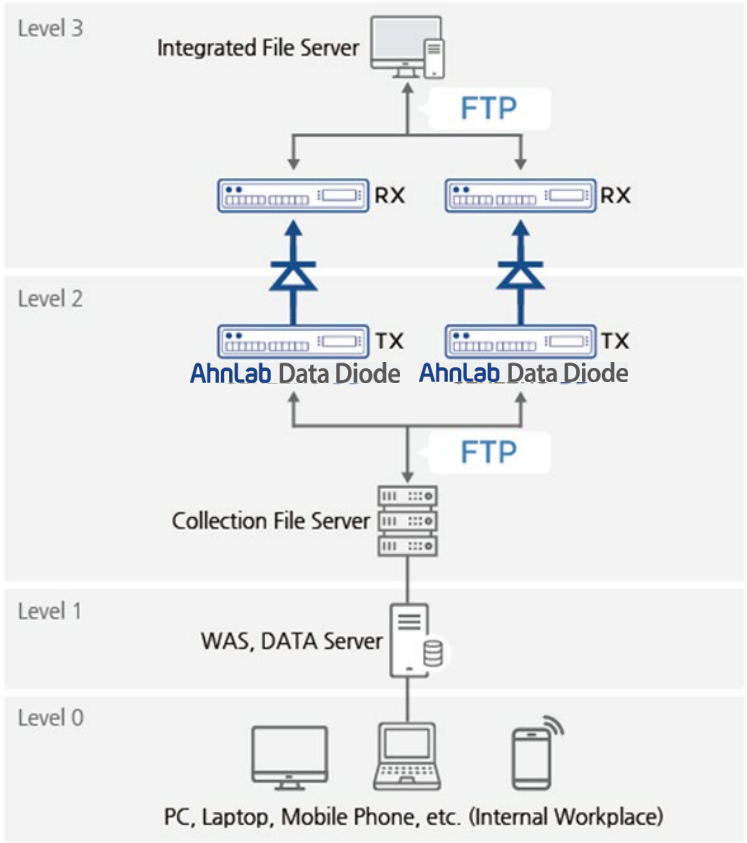
辦公室自動化

帳單資訊系統



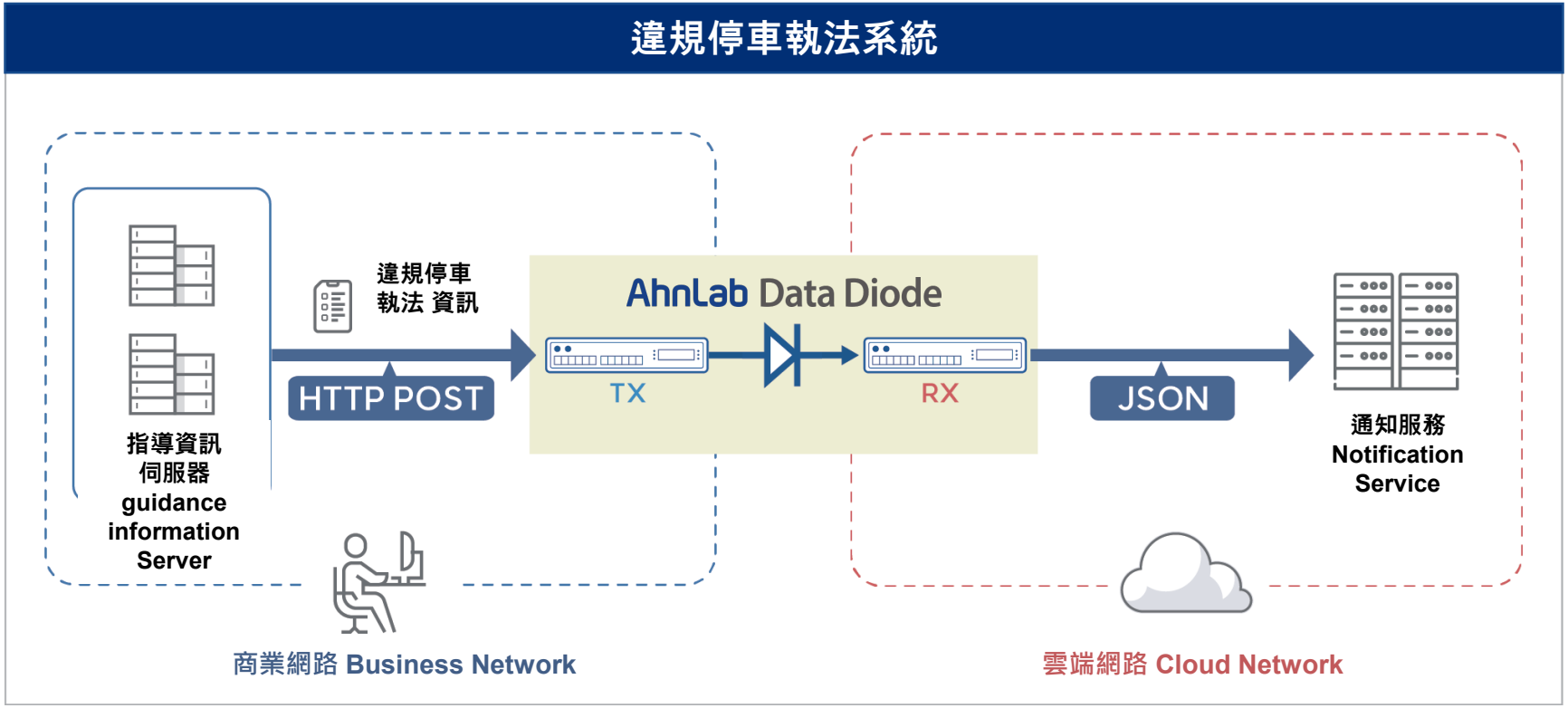
- **將地方政府分散的系統運行資料單向連接至整合的 OA 網路**

冗餘組態的OA 網路資料收集



- **單向連接 OA 資料檔案至整合式伺服器 (FTP)**
- **透過備援組態提供高可用性**

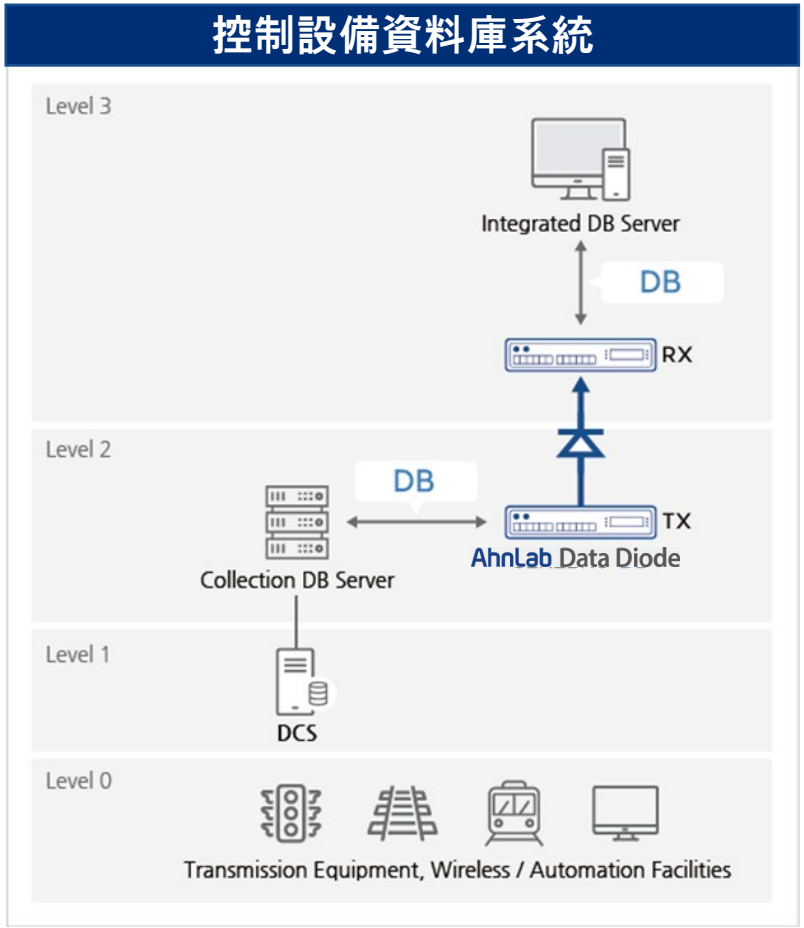
商業網路整合



- 違規停車執法系統的單向網路整合系統
- 從商業網路中的導引資訊伺服器向雲端網路中的伺服器單向傳輸違規停車執法資料

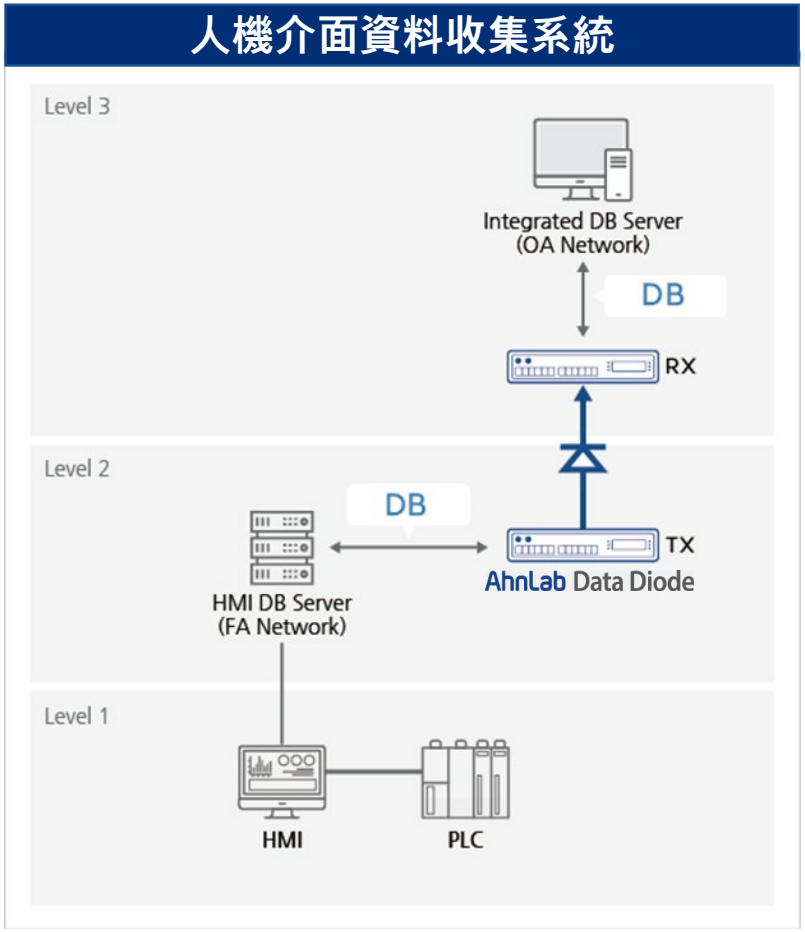
資料庫整合

控制設備資料庫系統



- 從收集 DB 伺服器單向連接至控制設備資料的整合 DB 伺服器 (Oracle DB)

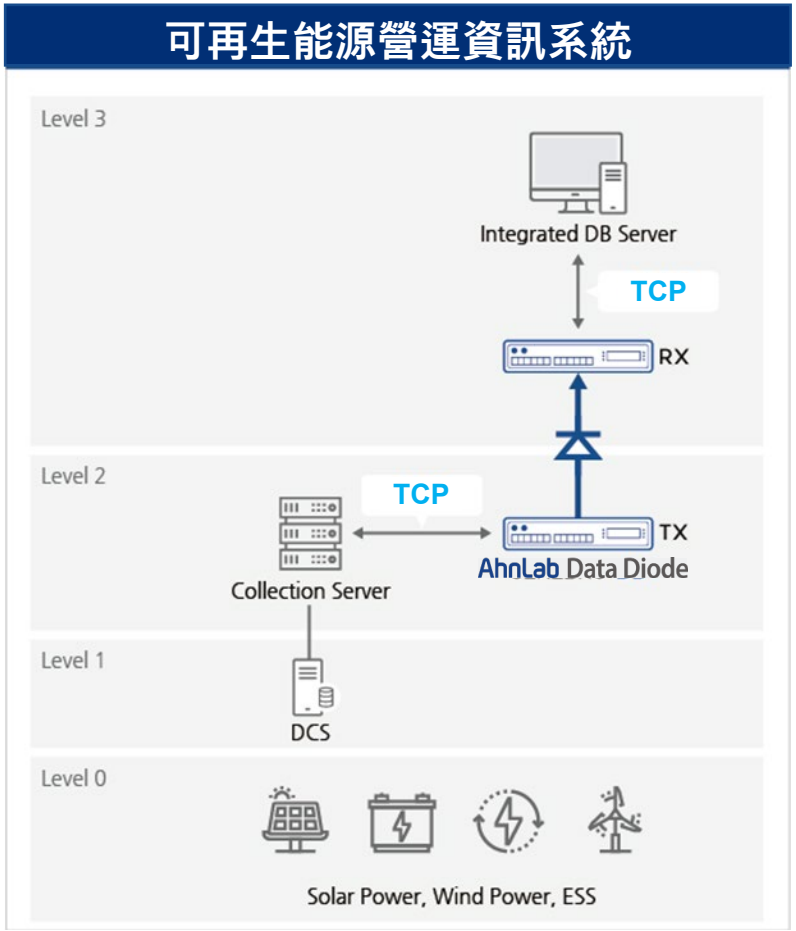
人機介面資料收集系統



- 從 FA 網路到 OA 網路中整合式 DB 伺服器 (Oracle, Tibero DB) 的單向 HMI 資料連接

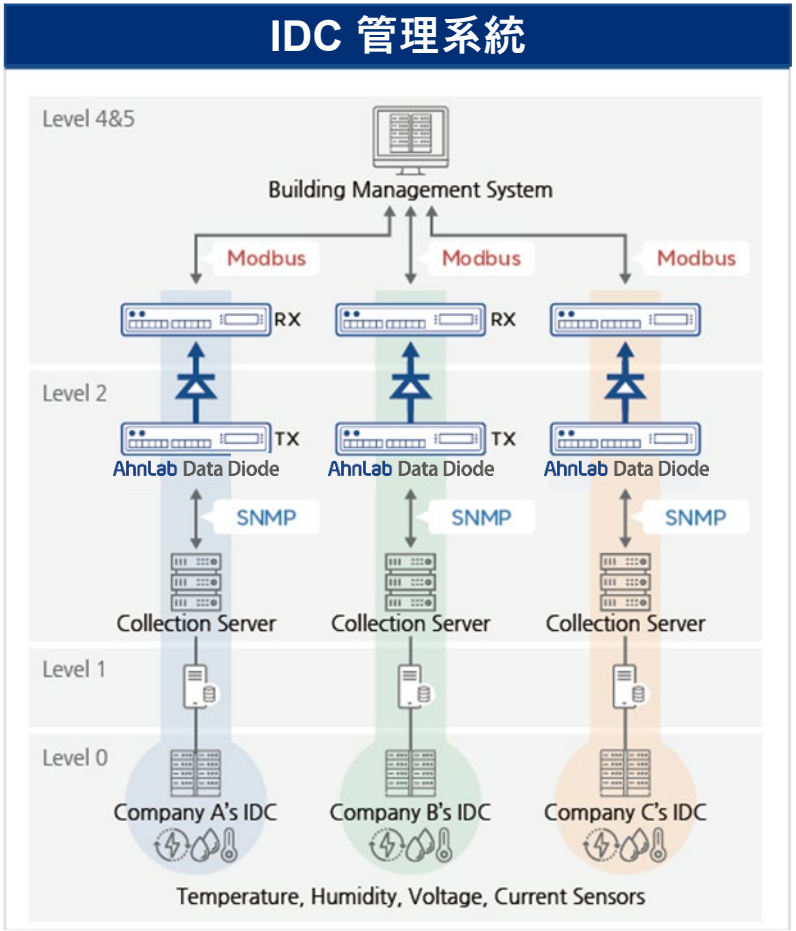
系統管理

可再生能源營運資訊系統



- 透過 TCP 將可再生能源設施的營運資料單向連接至中央資料庫伺服器

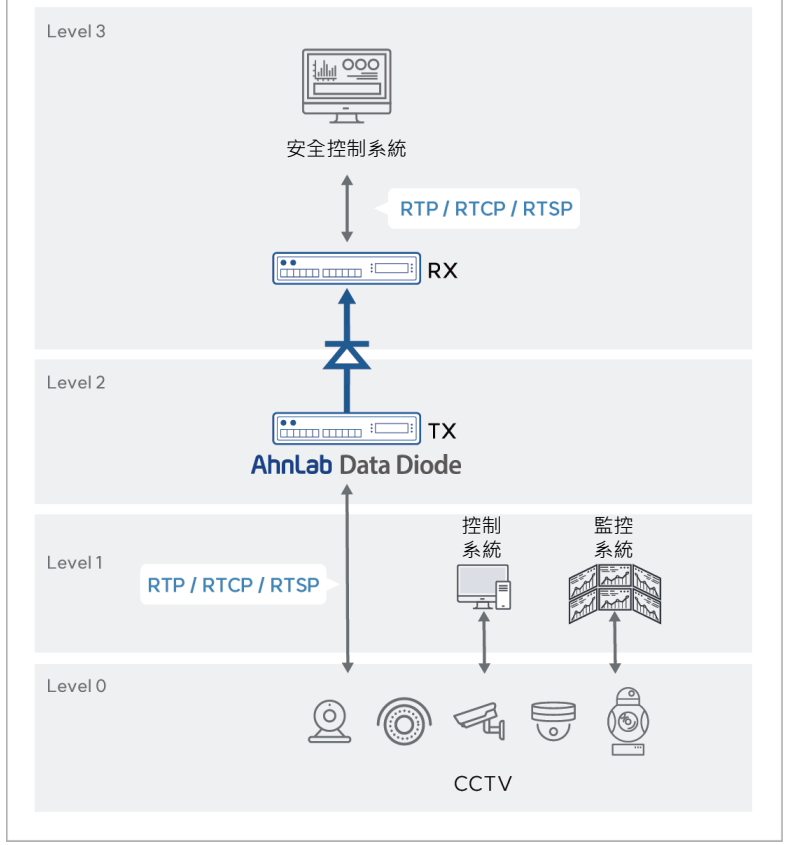
IDC 管理系統



- 溫度、濕度、電壓和電流感知器資料 (SNMP) 的單向資料連接，可從 IDC 連接到建築管理系統 (Modbus)

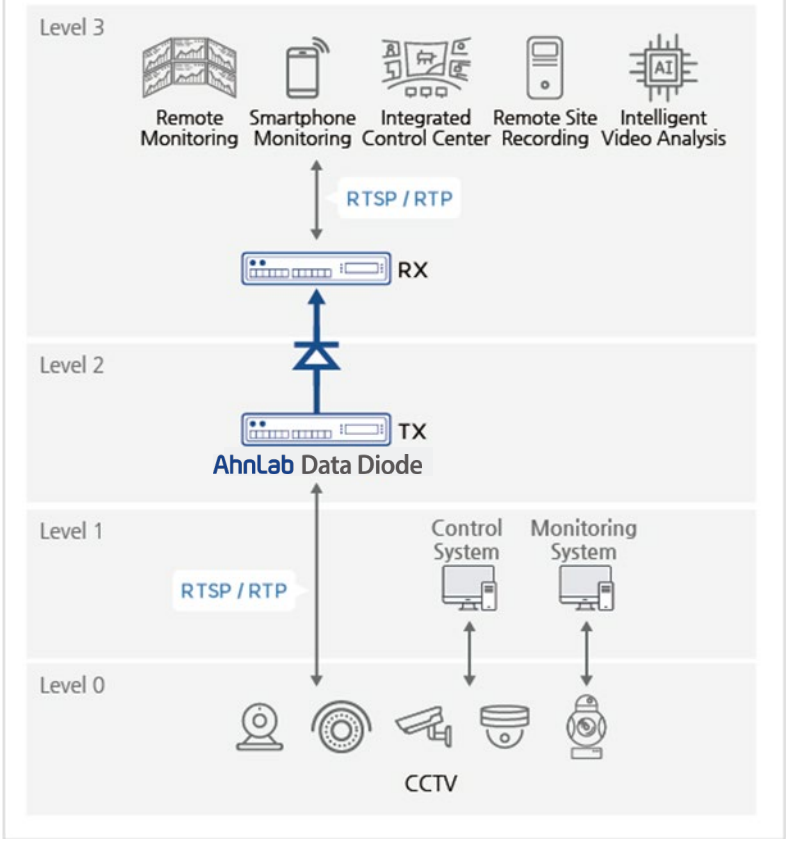
監控與監督

CCTV 視訊資料分析系統



- 透過單向閘道，將各種 CCTV 視訊資料從封閉式網路安全傳輸至安全監控系統

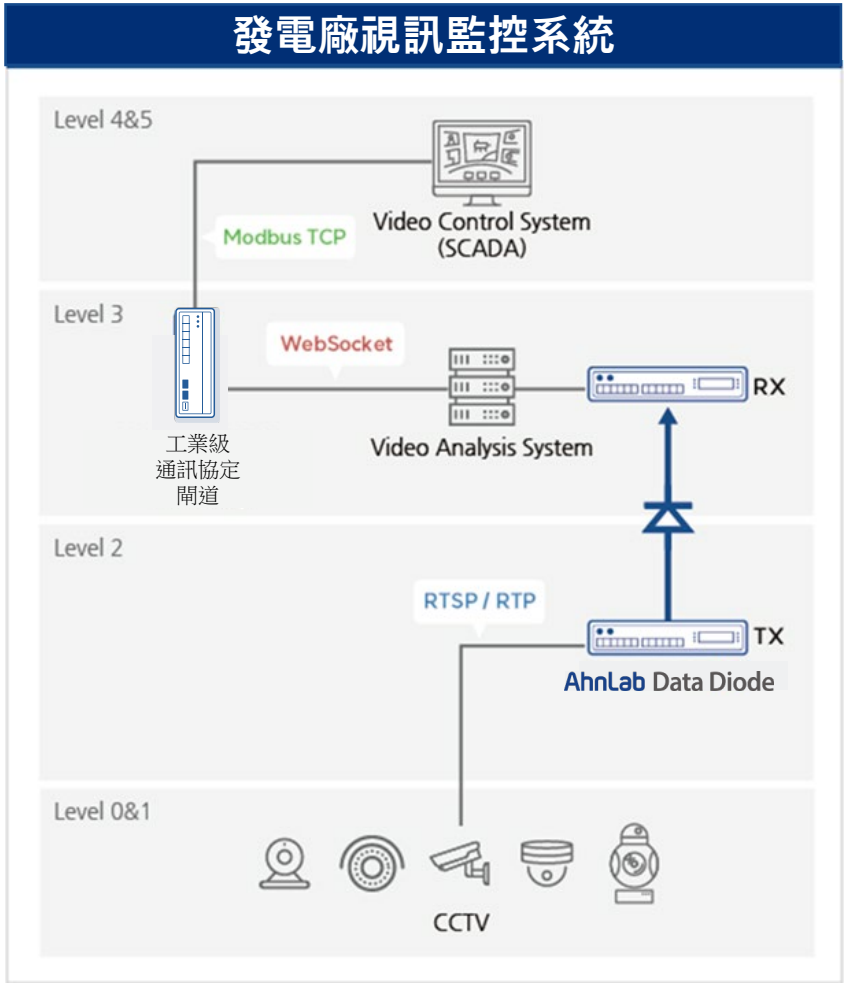
CCTV 視訊控制系統



- 透過單向閘道，將各種CCTV 視訊串流 (包括熱感應攝影機) 安全傳輸至監控,錄影,控制及智慧型視訊分析系統

監控與監督

發電廠視訊監控系統



CCTV 監控系統部署於發電廠內的 OT 網路監控。

為了確保視訊監控系統與發電廠控制網路之間的安全整合，在兩者網路的介面點安裝了單向閘道器。

- ✓ 視訊資料的單向串流可防止任何外部網路入侵控制網路。
- ✓ 資料傳輸可由管理員根據預先定義的政策進行管理。

More security,
More freedom

台灣區代理商 湛揚科技
台北市中山區民權東路三段58號15樓
北區：02-2515-1585 / 南區：07-972-7388

AhnLab Data Diode

AhnLab
台灣區代理商湛揚科技