Deloitte.

勤業眾信

隔離網路

隔離了什麼

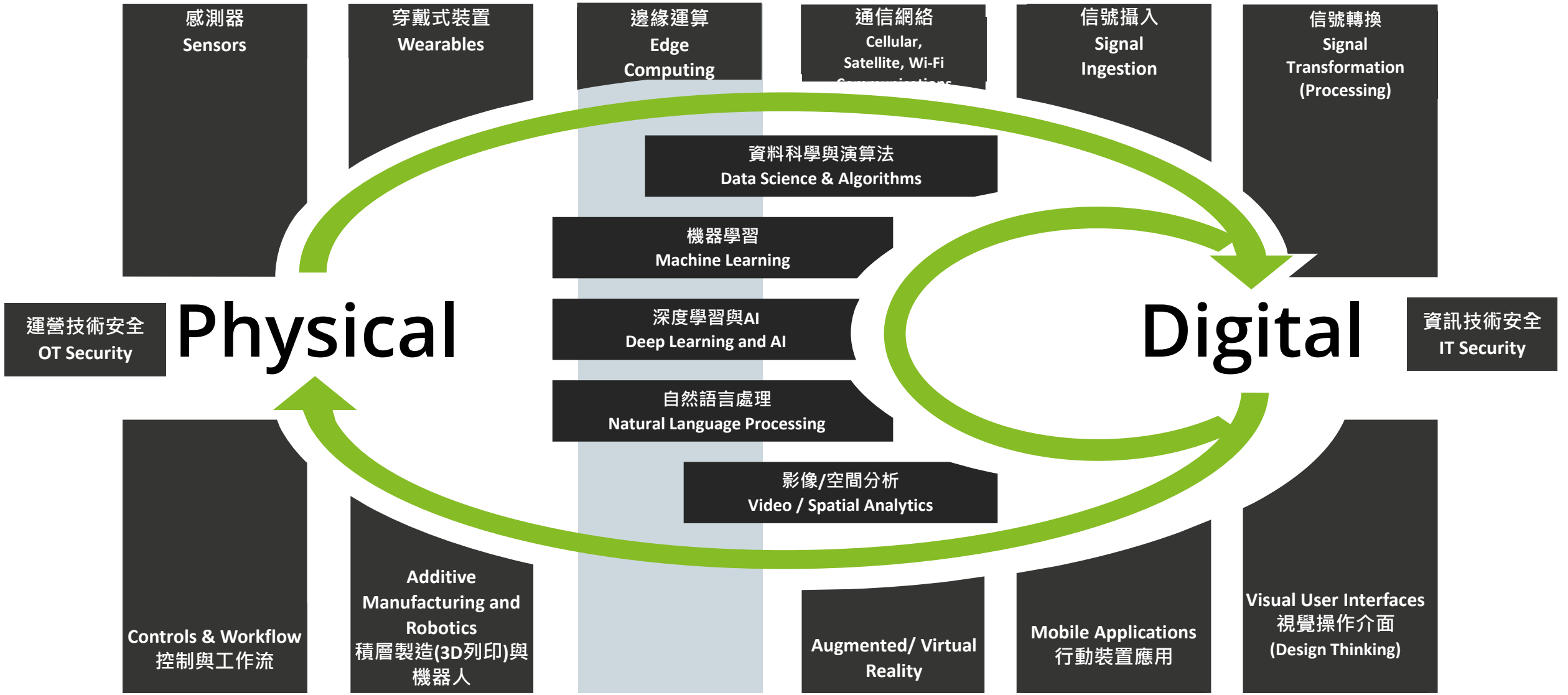
風險諮詢部門

2022.08

MAKING AN IMPACT THAT MATTERS since 1845

Air-Gap?

聯結虛擬與實體世界的方式，是透過OT運營技術(Operational technology)與資訊技術(Information Technology)的整合，而產生了工業4.0



智慧製造業所引進的新興技術，在新與舊的混合使用中，資安風險被無限擴大

雲端運算
Cloud Computing

風險：

雲端用戶之間缺乏隔離，傳輸中數據丟失，數據所有權丟失，缺乏對所有司法管轄規定的遵守，組件之間缺乏整合操作性

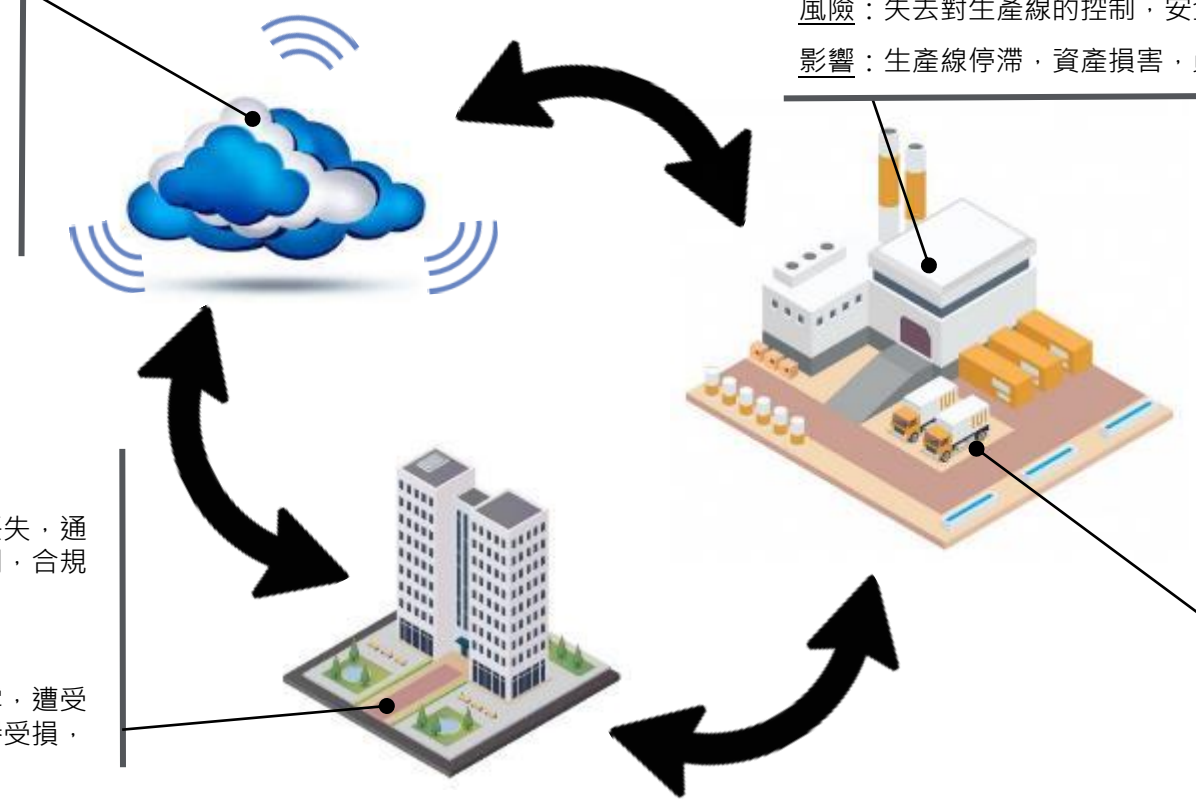
影響：

數據暴露和數據洩露，處罰，服務不可用，數據洩漏

OT運營技術 Operational Technology

風險：失去對生產線的控制，安全系統的損失，環境控制傳感器的損失

影響：生產線停滯，資產損害，員工和環境的健康和安全風險



企業IT Enterprise IT

風險：

未經授權的存取，數據洩露，數據丟失，通信系統丟失，數據和應用服務不可用，合規遵循議題

影響：

日常維運停滯，數據暴露和數據洩露，遭受處罰，服務不可用，數據洩漏，聲譽受損，智慧財產資本流失

工業IT Industrial IT

風險：

物流系統丟失，自動機器人失控

影響：

無法接收原材料，庫存積累，交貨和銷售延遲，無法完成倉庫活動，停止生產線，資產損壞

企業衝擊: 當企業的IT即OT資產與資產被攻陷後，會造成下列領域的衝擊:

財務層面　合約層面　公衛層面　環境層面　合規遵循層面　運營層面　商譽層面

當前工業控制系統環境 對於資安威脅未成熟

針對多起資安事件報告分析 發現亞太區長期受到勒索病毒攻擊且有上升趨勢

80%的企業表示曾遭受資安攻擊，其中47%表示其 工業控制系統(OT/ICS)環境受到了影響。

66%的企業營運生產一週內即可恢復，19%企業表示營運生產中斷超過一週。

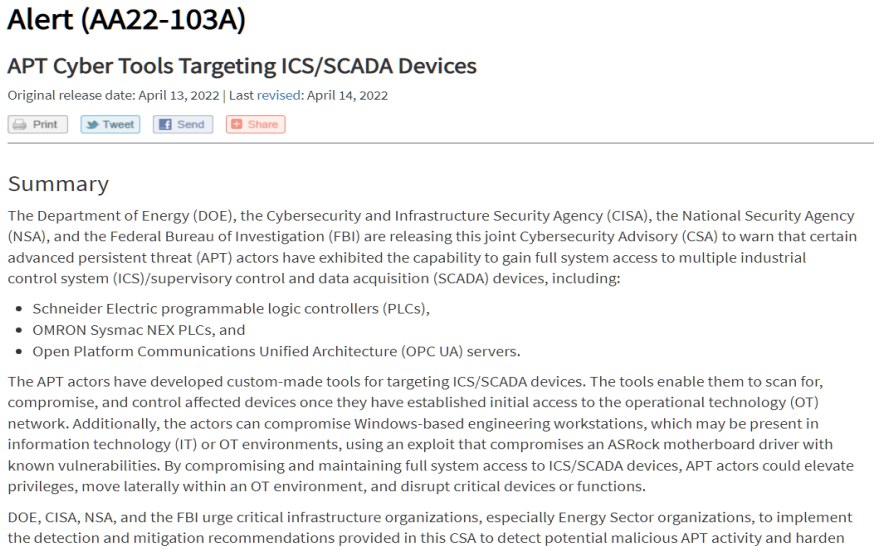
平均從感染到擴散約45分鐘，未適當隔離網路即可大規模式癱瘓企業內部網路。

攻擊主要來源為網際網路，僅少數來自於多媒體裝置；且主要為勒索軟體、間諜或後門程式，以竊取或遠端操控為主。

April 2022

工業控制系統惡意軟體模組化 針對機台設備控制器進行攻擊

美國資安主管機關聯合警告，關鍵基礎設施及製造業提防PLC被Pipedream攻陷



Alert (AA22-103A)

APT Cyber Tools Targeting ICS/SCADA Devices

Original release date: April 13, 2022 | Last revised: April 14, 2022

Print Tweet Send Share

Summary

The Department of Energy (DOE), the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) are releasing this joint Cybersecurity Advisory (CSA) to warn that certain advanced persistent threat (APT) actors have exhibited the capability to gain full system access to multiple industrial control system (ICS)/supervisory control and data acquisition (SCADA) devices, including:

- Schneider Electric programmable logic controllers (PLCs),
- OMRON Sysmac NEX PLCs, and
- Open Platform Communications Unified Architecture (OPC UA) servers.

The APT actors have developed custom-made tools for targeting ICS/SCADA devices. The tools enable them to scan for, compromise, and control affected devices once they have established initial access to the operational technology (OT) network. Additionally, the actors can compromise Windows-based engineering workstations, which may be present in information technology (IT) or OT environments, using an exploit that compromises an ASRock motherboard driver with known vulnerabilities. By compromising and maintaining full system access to ICS/SCADA devices, APT actors could elevate privileges, move laterally within an OT environment, and disrupt critical devices or functions.

DOE, CISA, NSA, and the FBI urge critical infrastructure organizations, especially Energy Sector organizations, to implement the detection and mitigation recommendations provided in this CSA to detect potential malicious APT activity and harden

事件背景

多個美國資安主管機關，包括網路安全暨基礎設施安全局（CISA）、國家安全局（NSA）、聯邦調查局（FBI）與能源部（Department of Energy），於近日聯合發表資安通報，警告駭侵者已有能力利用新型惡意軟體工具，針對液化天然氣和電力設施的產線進行攻擊，大量的工廠與產線都已採用的PLC，一旦PLC遭受攻擊，從停機、停電、化學洩漏、設備損壞甚至爆炸都可能發生。(資料來源：CISA)

系統潛在影響

- 可以利用這些APT模組掃描目標設備，對設備詳細信息進行偵察，將惡意配置/代碼上傳到目標設備，備份或恢復設備內容，以及修改設備參數。

根因分析

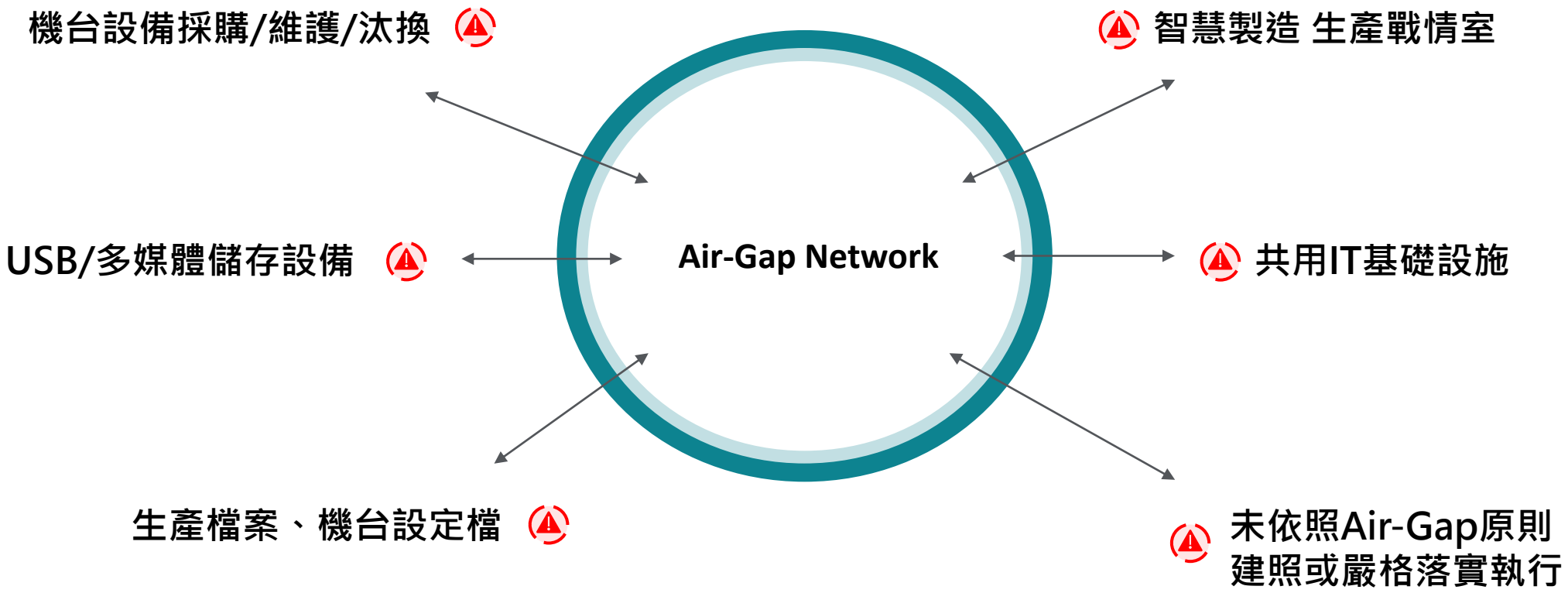
- 駭客製作APT客製化模組，一旦他們在 OT 網絡中建立了初始訪問權限，就可以掃描、破壞和控制 ICS/SCADA 設備。

預防方法

- IT網路及ICS/SCADA 做區隔
- 針對系統用戶套用多重登入驗證（MFA）流程，且務必更改預設密碼
- 帳戶最小權限化
- 有效的離線備份

Air-Gap並非想像安全 - 多數人員認為網路完全隔離但未實地落實檢視

訪談多數企業發現：場域人員認為完全隔離但未考量OT裡的IT設施；IT人員對工控技術認知有限，亦無法覆核確認



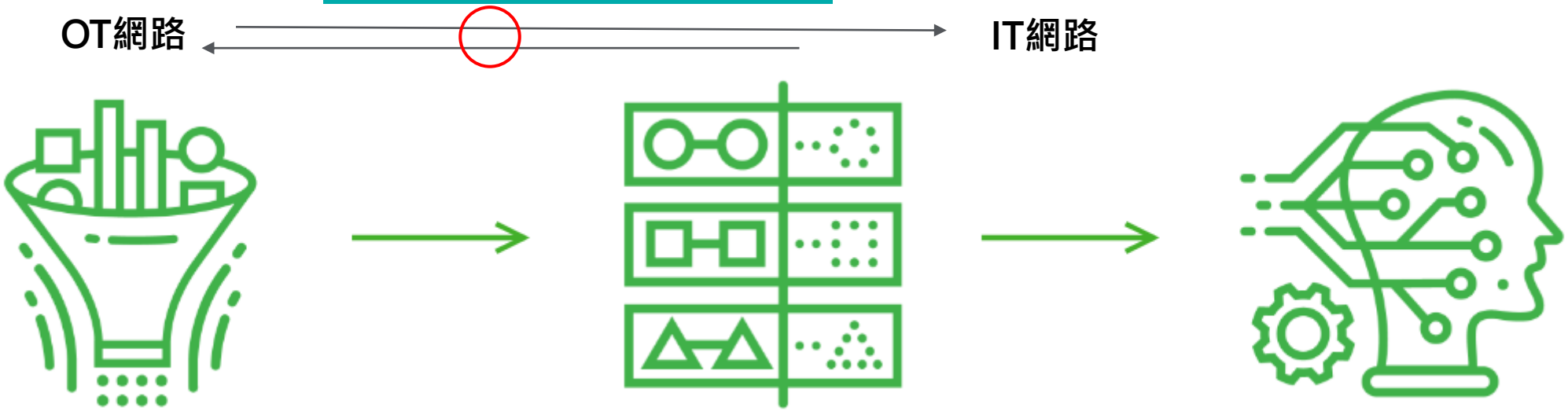
真的Air-Gap嗎?

真的Air-Gap 嗎? (1) – 智慧工廠戰情室 可視化即時監控生產數據

提供各種數據的採集模組，透過通訊整合平台，讓生產資訊達到真正的透明化，提升產能與優化營運管理。相對的也讓OT與IT鋪設一條快速道路，資料可以出來也代表惡意程式有機會進去。

檢視點1：

生產報表數據是否來自機台設備?



通過連接和收集生產數據

分析數據獲得洞察力

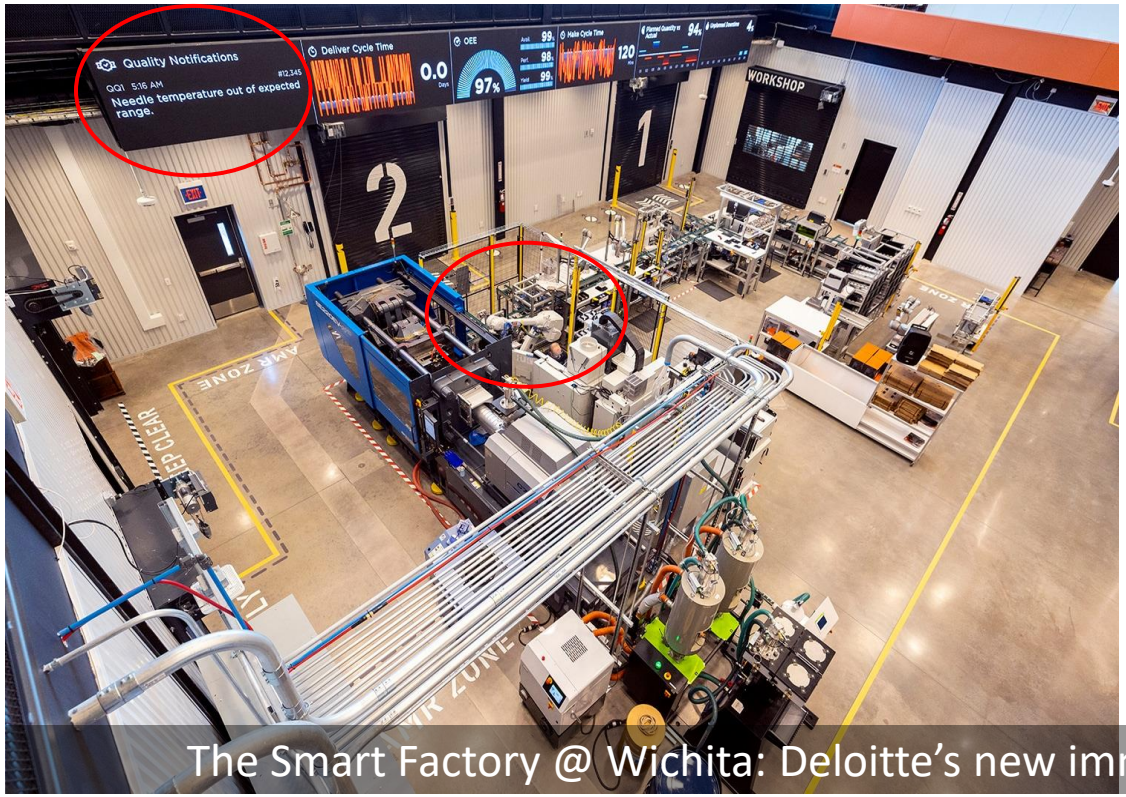
通過AI預測強化生產性能和設備可用性

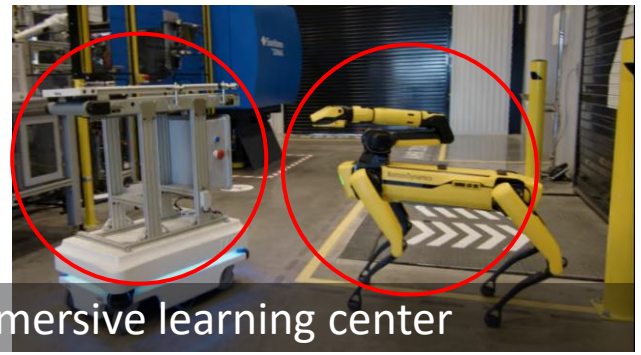
真的Air-Gap 嗎? (2) – 智慧製造未來 新興科技技術導入連接生產設備

機器手臂、無人搬運車(AGV/AMR)、5G通訊、數位分身(Digital Twin)與混合實境(MR)等應用更為便利；相對的也改變了既有封閉的網路，引進更多IT設備及通訊線路以支持此技術。

檢視點2：

這些新興科技資料來源如何處理、儲存，是否可以遠端監控及遙控? 是否放入更多的IT設備? 甚至可以透過手機遠端監控?

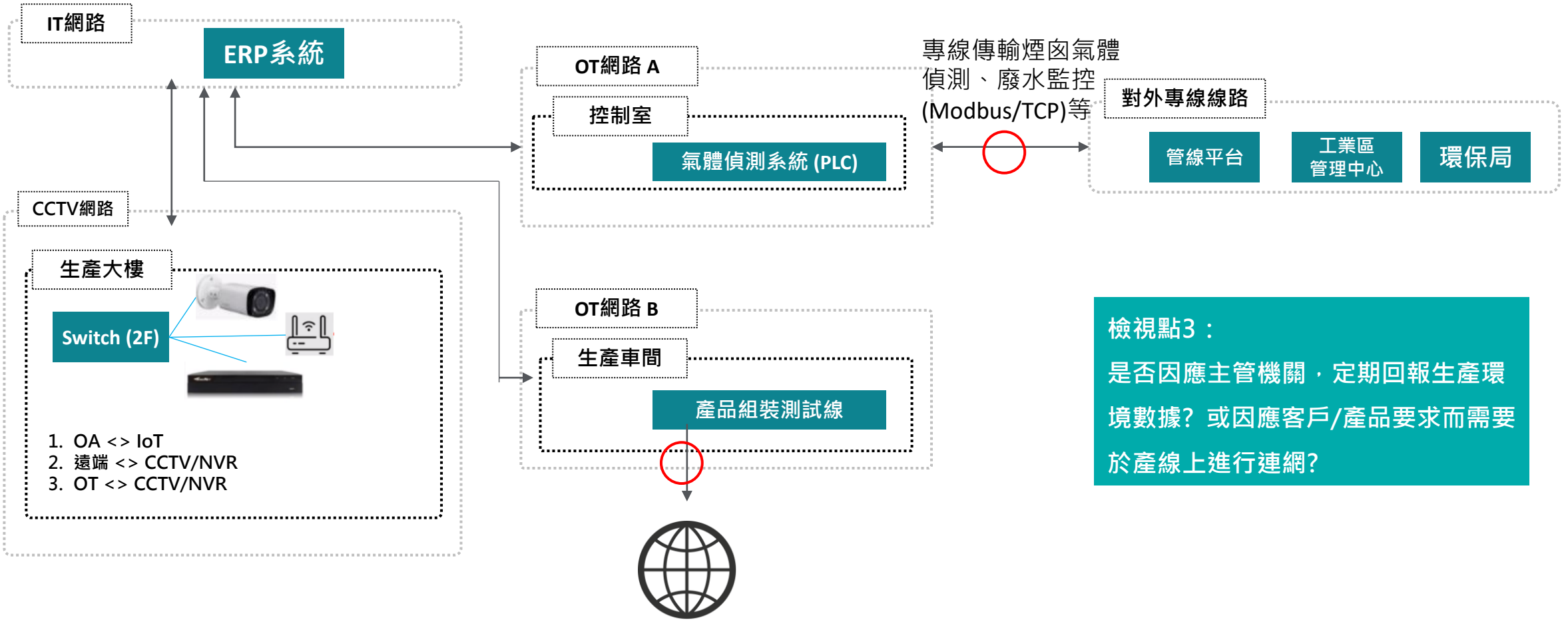




The Smart Factory @ Wichita: Deloitte’s new immersive learning center

真的Air-Gap 嗎? (3) – 因應主管機關/客戶要求 工廠即時通報環境監控資訊

工控場域通常涉及3~4個甚至更多不同承包商各自負責範圍，並非單一單位可全面完全瞭解全貌；期間可能因為相關政策改變要求而增設線路但並非為主要控制系統人員悉知。

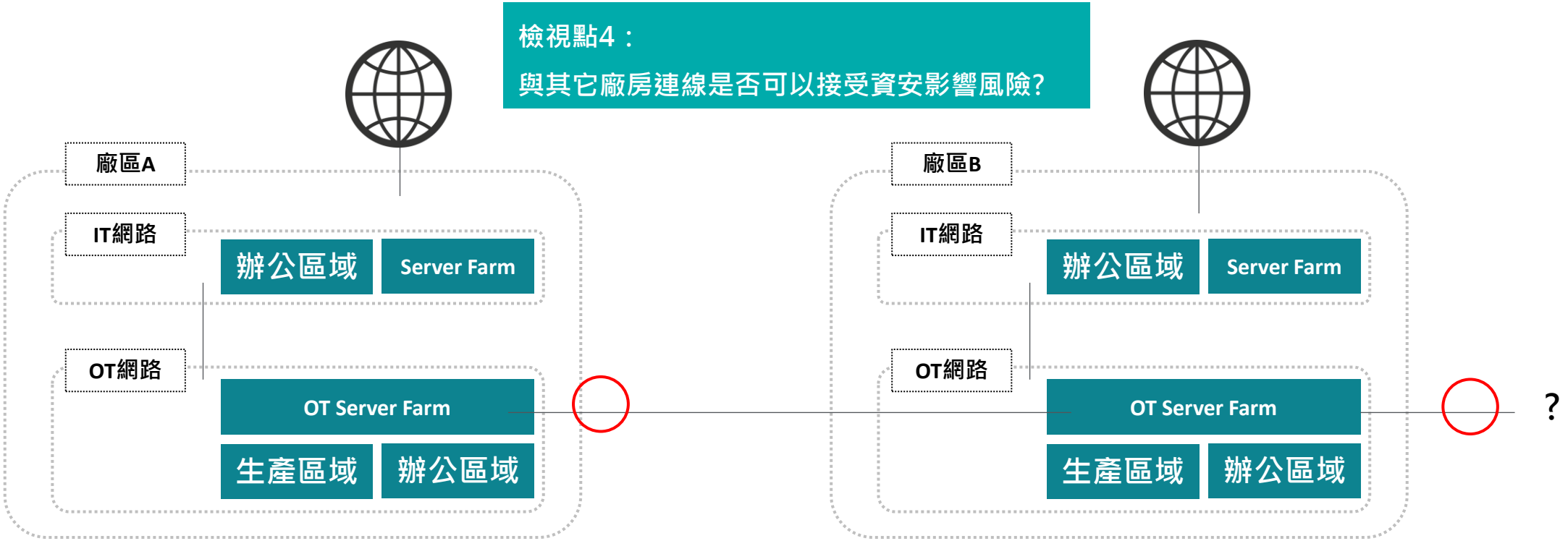


檢視點3：

是否因應主管機關，定期回報生產環境數據? 或因應客戶/產品要求而需要於產線上進行連網?

真的Air-Gap 嗎? (4) – 跨廠區網路視為內網，無須擔心資安威脅

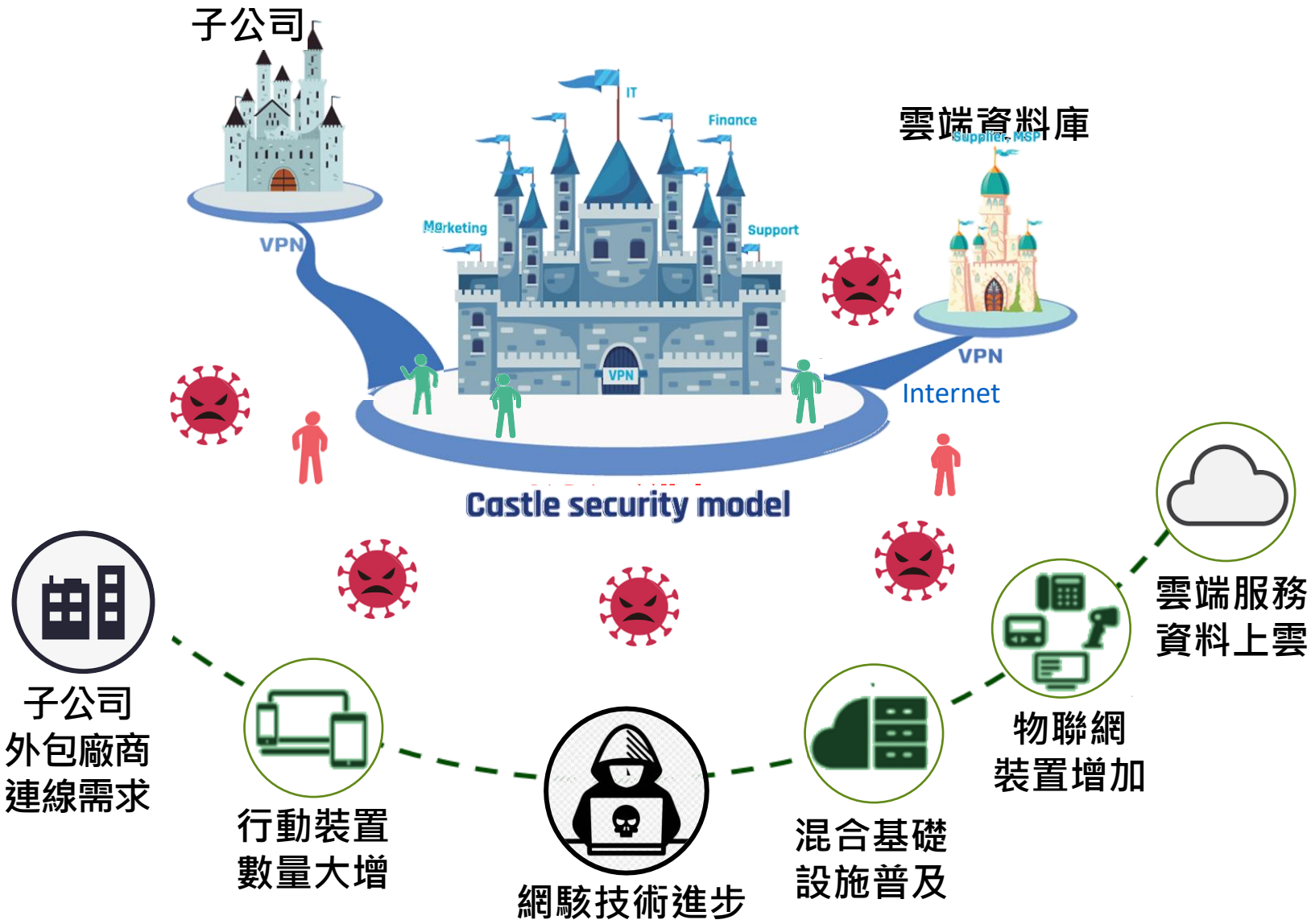
時常生產場域同時具備許多廠房，因為作業方便因此串聯不同大樓，甚至與不同地區工廠串聯。若中間並未有適當防護機制，資安事件發生時可能發生一連串骨牌效應。



內外網隔離

還隔離了什麼?

傳統資安防護模型



內外網隔離

當遇到攻擊時，我們的自然反應就是----隔離

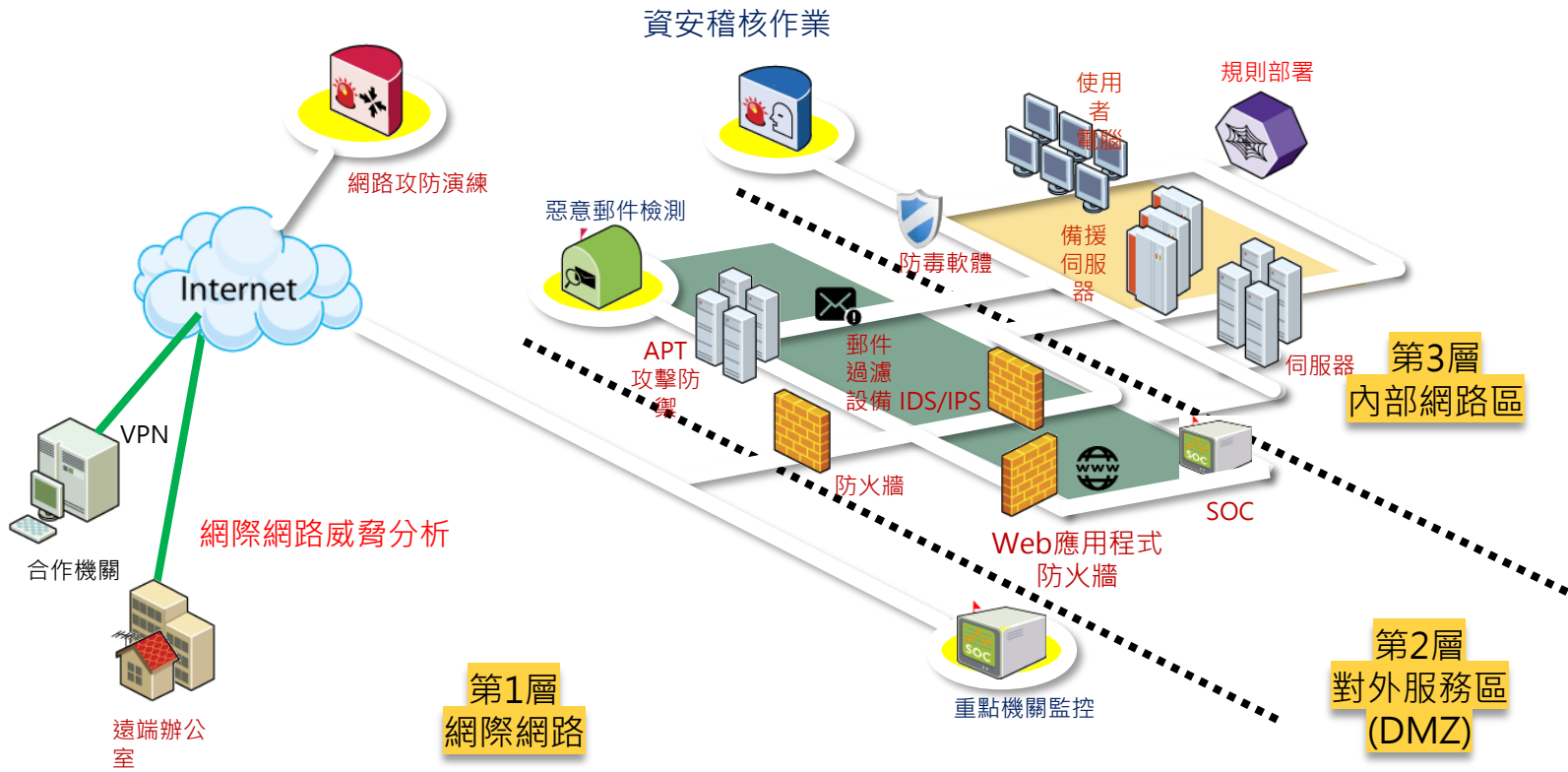
內網 VS 外網

資訊 VS 業務

國內 VS 國外

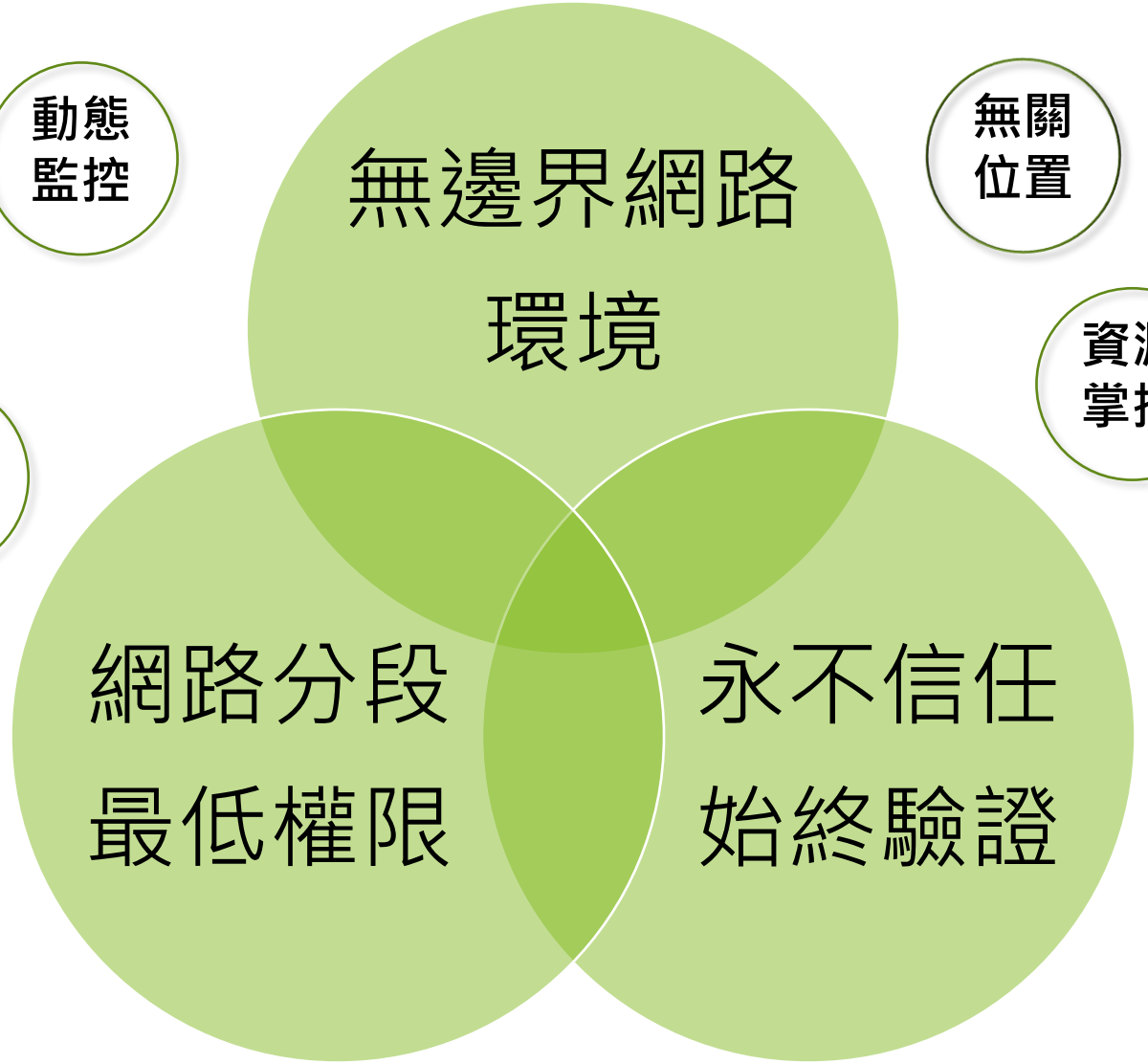
網路長城

網路碎型化



縱深防禦才是基礎，零信任框架才是王道

零信任架構及NIST 7大原則



動態監控
- ✓ 基於身分的信任評估
- ✓ 基於環境的風險判定
- ✓ 基於行為的異常發覺

無關位置
- ✓ 以身分為中心
- ✓ 用戶及設備白名單

資源掌控
- ✓ 資產盤點及網路分割
- ✓ 端點偵測回應(EDR)工具

最少時間
- ✓ 處理所需最少時間
- ✓ 限制敏感文件訪問

身分驗證
- ✓ 多因子身分認證
- ✓ 強密碼策略

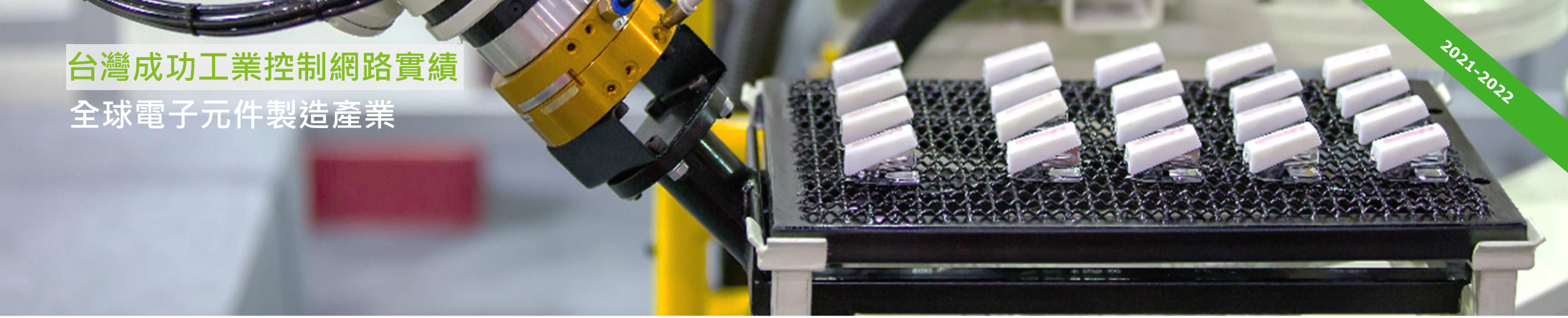
最小需求
- ✓ 業務所需最小訪問權限

訪問規則
- ✓ 依業務制定訪問規則

資料來源：NSB

How to bridge the gap?

工控與資安跨領域整合



台灣成功工業控制網路實績

全球電子元件製造產業

2021-2022

Project description

專案摘要

協助客戶製造產線避免惡意程式影響產線活動，透過ISA/IEC 62443整體標準協助客戶進行產線資安能力強化。從產線設備資產盤點、產線維護流程、產線網路架構、產線設備維護流程及產線網路安全管理委員會(CSMS)進行一系列系統性規劃。

依據資產盤點、架構調整、機台功能安全評估、流程作業改善等階段，協助客戶進行整體規劃並制定一系列作業標準程序，協助客戶在全球生產管理上建立最佳模板，讓全球工廠都有一至化的管理規範並具備一定程度資安防護能力，避免產線因操作不當、資安意識不足或網路攻擊情形，導致產線遭受意外地停擺可能。

How we made an impact

專案效益：

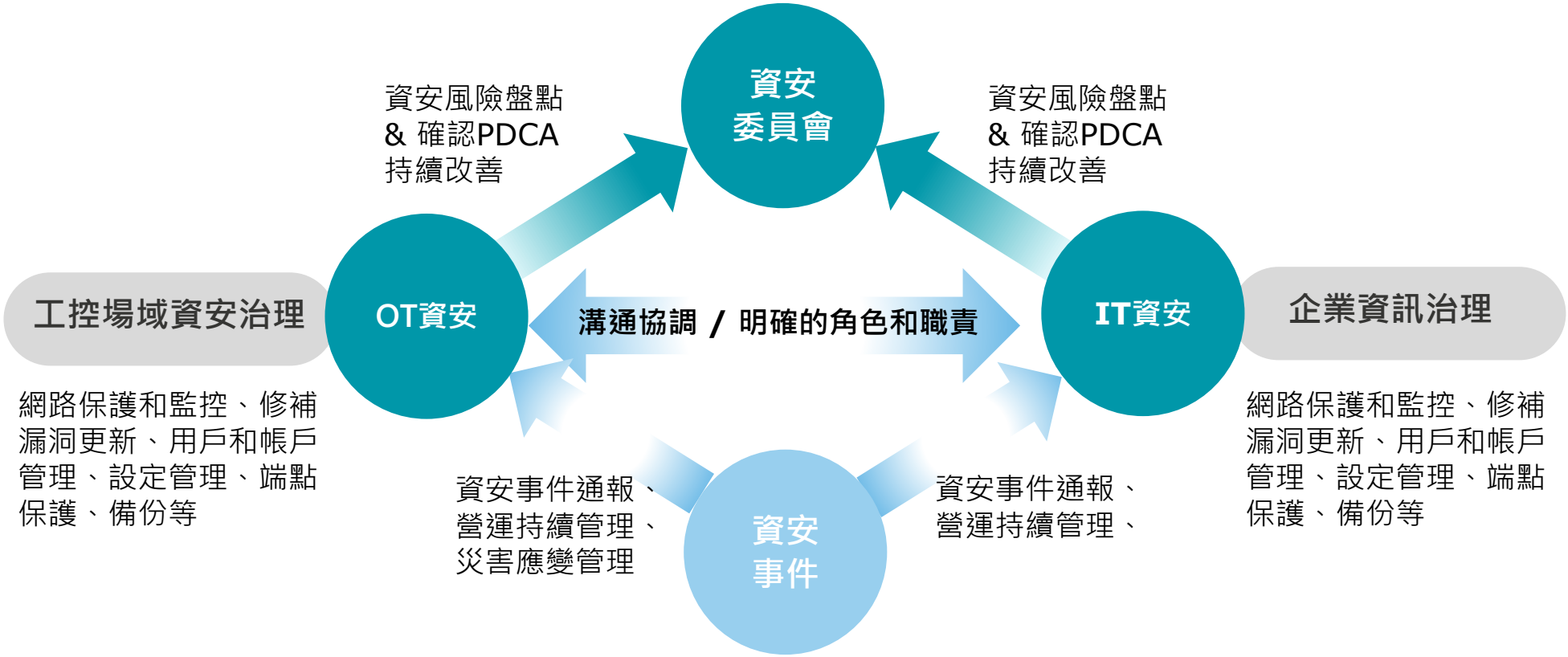
- 整合IT及OT團隊之資安業務
- 成功取得全台灣首個 ISA/IEC 62443-2-4 機台設備維護流程認證
- 成功取得全台灣首個 ISA/IEC 62443-3-3 產線機台設備安全認證
- 產線資產盤點、網路架構調整、機台功能安全評估、機台維護流程作業改善

設備導入規劃：

- 工控資安產品規劃諮詢服務

工控與資安跨領域整合經驗 (1) – 如何整合OT/IT資安管理團隊?

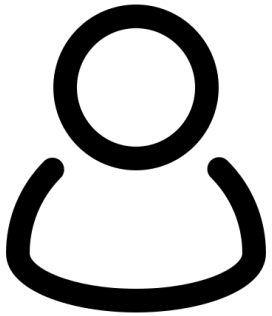
為了實現更順暢、更安全的 IT/OT 融合，應讓雙方了解 IT 和 OT 在意優先順序與傳統工作文化之間的潛在衝突。



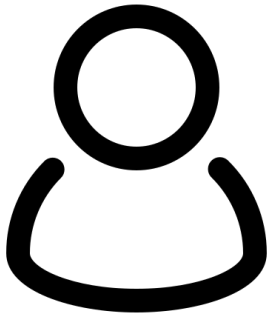
工控與資安跨領域整合經驗 (2) – 誰應更注意並積極參與工控場域資安?

網路安全對於 OT 來說是一個新話題，而自動化人員並不熱衷於 IT 技術，因此正確與OT人員溝通應該始終是重點

場域負責人



場域資安代表



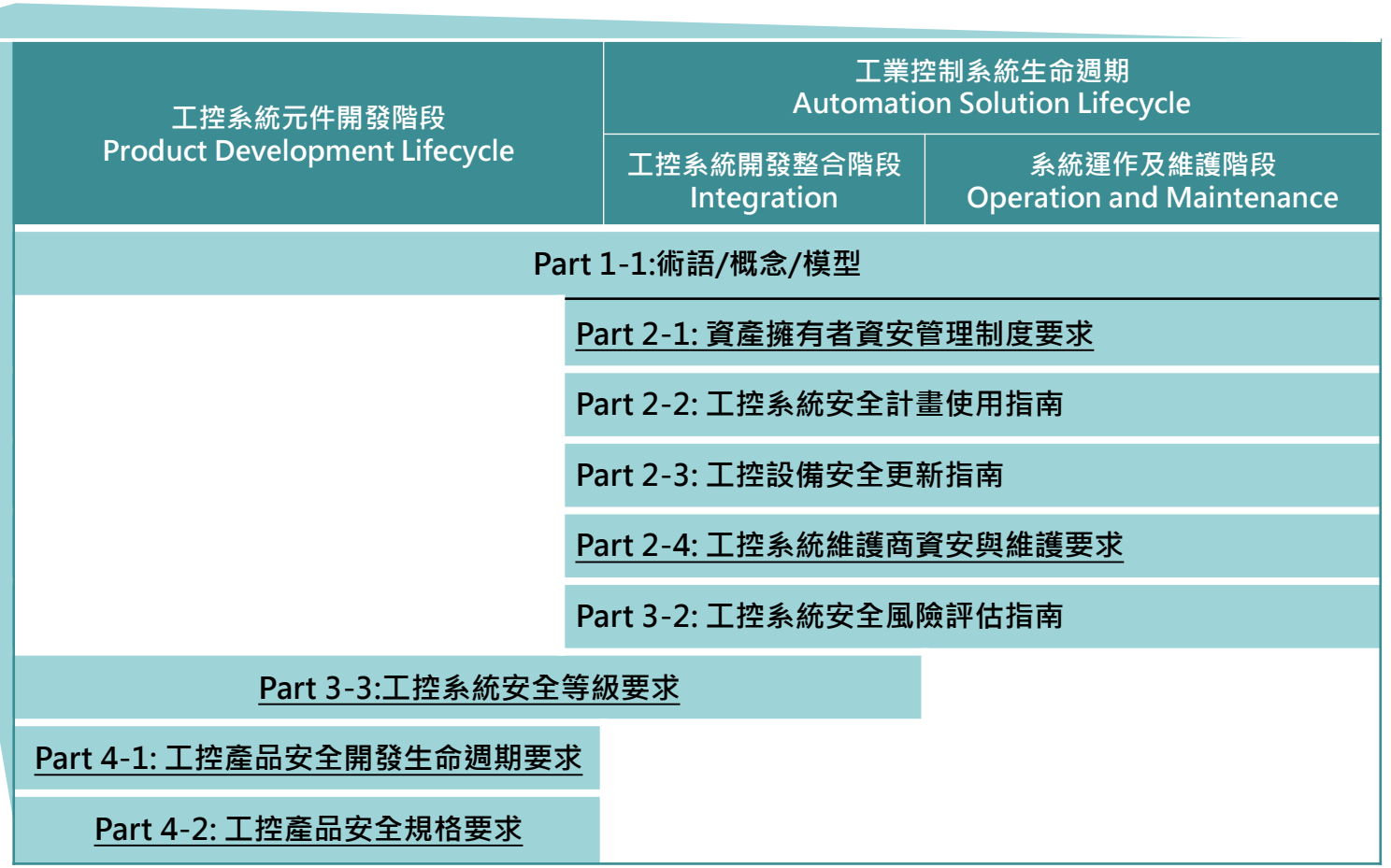
場域IT代表

機台設備工程師
(機台設備商)

工控與資安跨領域整合經驗 (3) – 有哪些工控場域安全標準可以參考遵循?

ISA/IEC 62443為通用自動化標準，各產業因應生產作業特殊性可參閱產業特有標準。

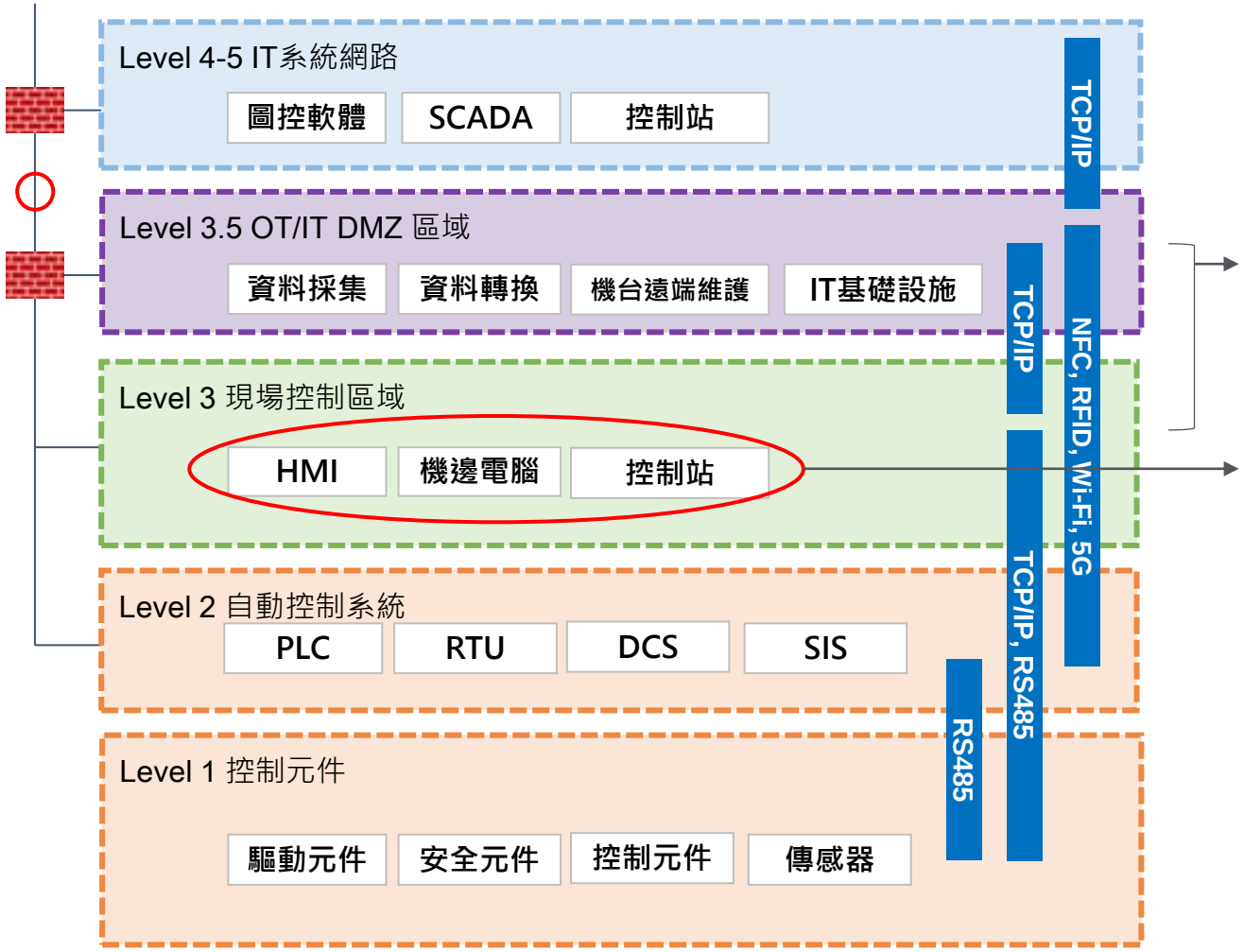
- 通用自動化 General Automation
  - **ISA/IEC 62443, NIST SP 800-82**
- 半導體產業 **Semi-Conductor**
  - **SEMI E187, E169**
- 汽車產業 **Automotive**
  - **ISO/IEC 21434, TISAX, UN/ WP.29**
- 能源自動化 **Power Automation**
  - **IEC 62351 / NERC CIP (US) / IEC 61850 (System) / IEC 1686 (Component) / NIST IR7628 (Smart Grid)**
- 海事自動化 **Marine Automation**
  - **IEC 61162-460**
- 石油和天然氣管道**Oil & Gas Pipeline**
  - **ISA/IEC 62443,**
  - **美國石油標準API 1164**
- 資訊科技 **IT Security System**
  - **ISO/IEC 27000, NIST SP 800-53**



ISA/ISA/IEC 62443 系列標準

工控與資安跨領域整合經驗 (4) – 導入資安產品應注意那些事項?

工控場域資安產品選擇應更注意相容性及機台設備商意見，部署時更應優先考量是否會影響到產線可用性。



網路防護：

1. OT/IT邊界應設置防火牆過濾允許通訊。
2. 不清楚系統指令前，工控內網應優先考量採取被動式偵測機制。

端點防護：

1. 應安裝機台設備商認可之端點防護方案，避免發生無法持續提供維護服務情形。
2. 工控環境除IT病毒外，更具備針對工控通訊協定攻擊惡意程式，選擇具備其偵測功能尤佳。

工控與資安跨領域整合經驗 (5) – 導入SIEM平台碰到的挑戰?

最近的工控資安事件表示，攻擊者的知識和能力與組織的整體工控網路防禦能力之間存在明顯差距，如何有效提前預防至關重要， 透過整合日誌至SIEM平台常碰到相關挑戰。

- 兩個不同的領域，有兩個非常不同的知識來構建使用情境。

- SIEM平台並非設計用於分析 ICS 協議。

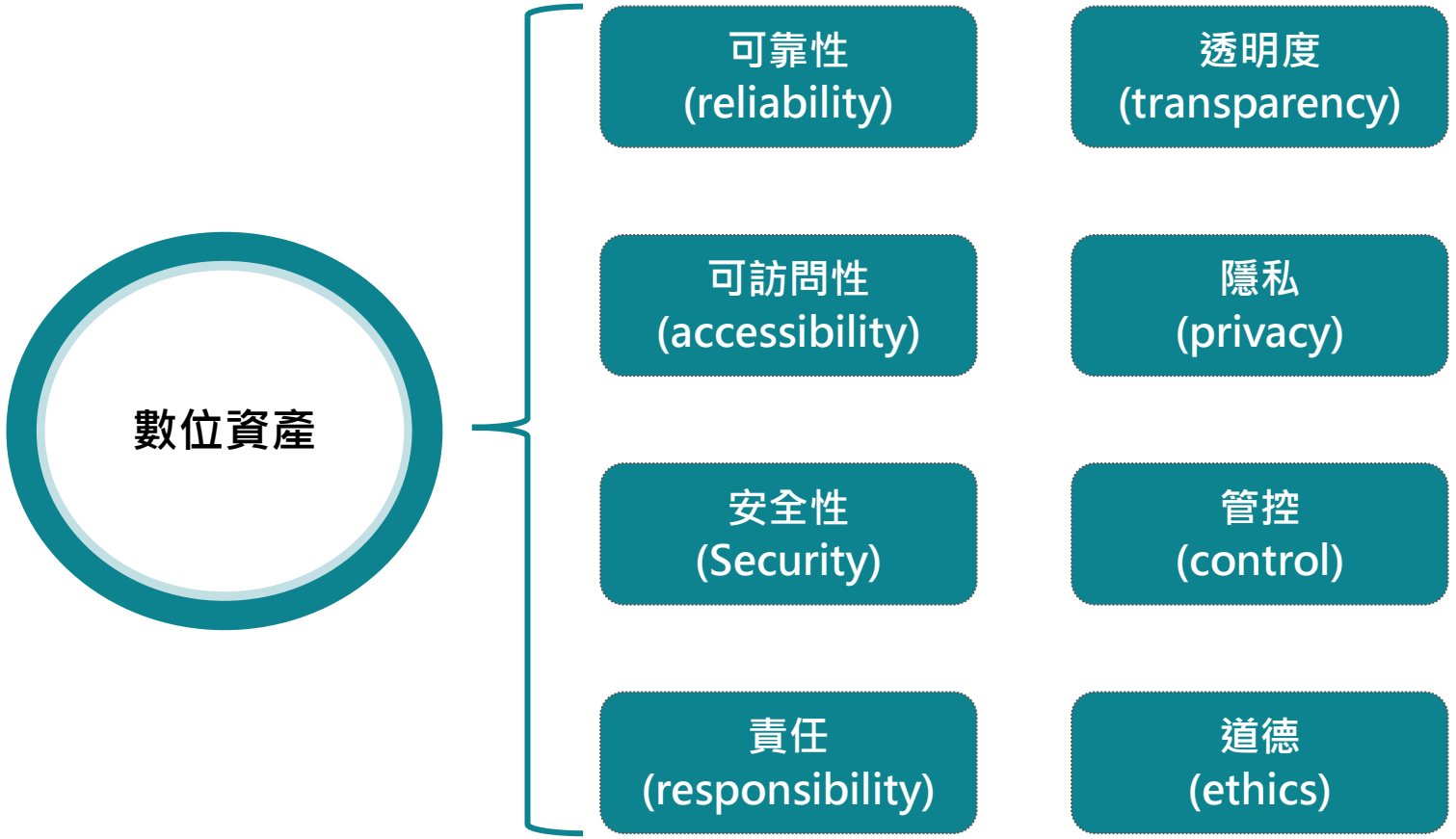
- 為了建立實時監控，需要集中化 SIEM 解決方案，在工控場域裡是極為挑戰。

- 工控場域設備啟用日誌紀錄，可能會產生嚴重的性能和穩定性問題。

How to bridge the gap?

Digital Trust

甚麼是數位信任(Digital Trust)



「不論是客戶、員工、合作夥伴或是其他的利害關係人，皆能夠完全的信任所創建、維護的數位資產，並且該組織必須確保數位資產的保密性、可用性與完整性。」

數位信任生態系 -生態系中相互影響的五大組成要素

包含客戶、員工、合作夥伴或是其他的利害關係人等，彼此間會互相交流的所有角色。

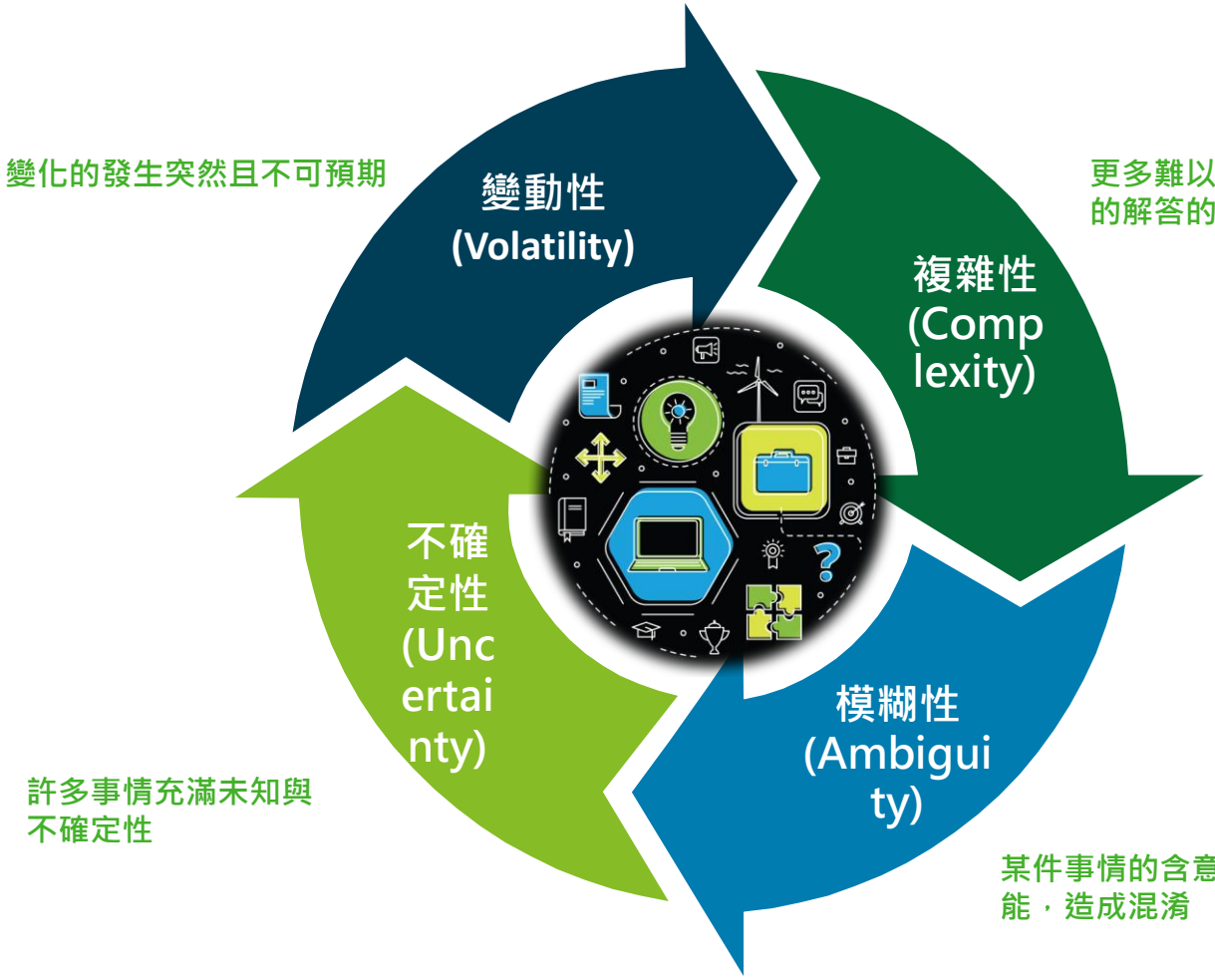
泛指需交換、存取及保護的各項資料，包括商業資訊、技術資料及個資等。

使用者透過各項系統的協作，以利在網路空間存取需要的資料，包含應用程式、網路架構、伺服器及資料庫等。

泛指履行職務，為他人做事，並使他人從中受益的各項活動。

對於各項行為進行評價和斷定的規範標準。

數位信任的未來-持續上升的VUCA因子



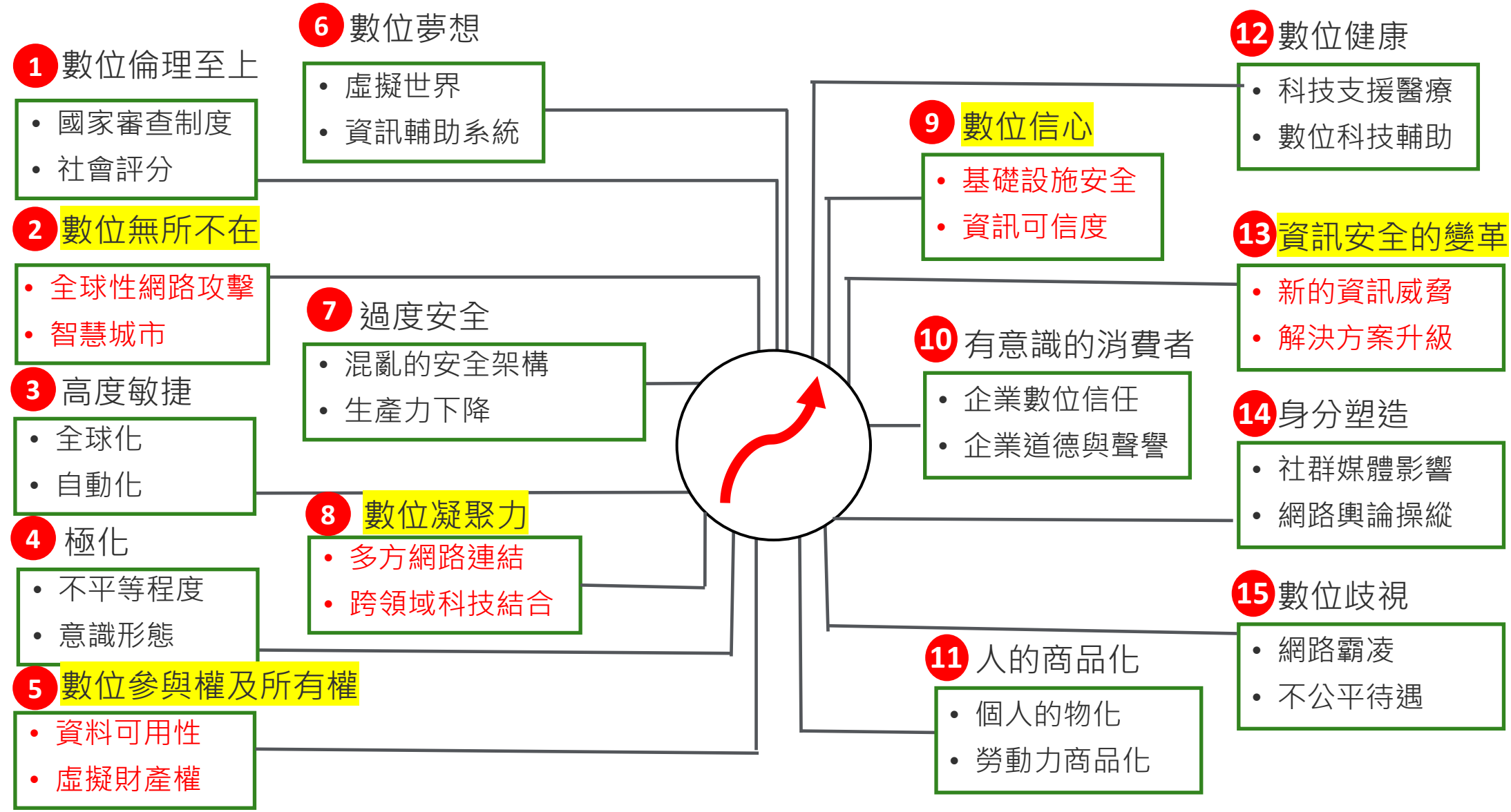
數位信任生態系 – STEEPL框架

現實中存在取多影響數位信任的影響因子，透過基於AI分析方法及傳統研究方法，共找出143個關鍵因子，分類為6大類別並稱為STEEPL框架。

STEEPL Framework

Social 社會的	Technological 科技	Economic 經濟	Environmental 環境	Political 政治的	Legal 法律
• 心理健康 • 數位倫理道德 • 現實冷漠 • 虛假訊息 • 數位追蹤	• 區塊鏈 • AI 人工智慧 • 自動化 • 深度造假 • 生物科技	• 數位監控資本化 • 網路安全創業 • 網路犯罪 • 科技巨頭壟斷	• 綠色能源 • 科技廢棄物 • 都市發展 • 綠色運算能源	• 數據保護監管 • 選舉與投票操縱 • 網路恐怖主義 • 惡意資訊濫用	• 資料保護隱私 • 網路法規全球化 • 反壟斷法監管 • 網路監管準確性

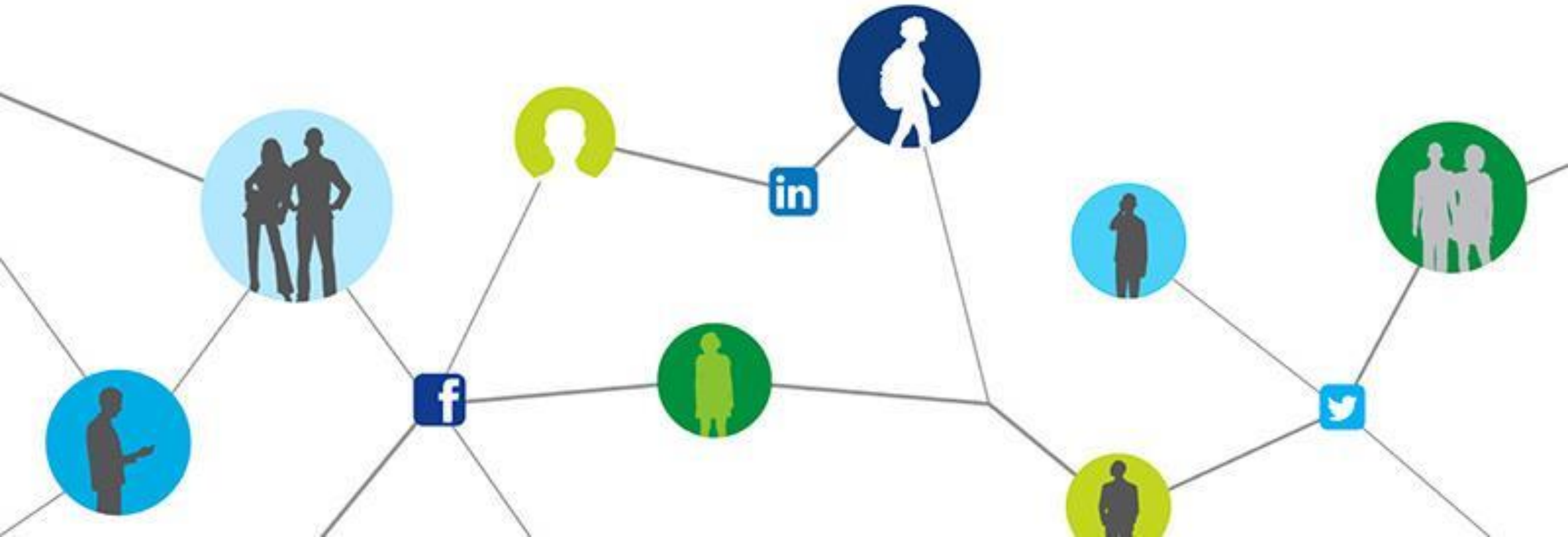
數位信任的未來-基於STEEPL驅動力描繪出的15大相關趨勢



數位信任生態系 – 數位化8大關鍵省思

1. 責任碎片與當擇性：數位化後延伸出新的責任及當責角色
2. 數位永續的必要性：任何數位化決策是否能夠讓系統永續發展
3. 資料至上的管理原則：任何數據使用需以保護個人權利為最高優先
4. 數位世界為世界的一部分： 如何永續管理數位世界
5. 獨立思辨能力：如何辨識數位化帶來海量訊息真偽
6. 解決方法的關鍵演化：解決方案必須隨著不斷發展的商業模式持續改善以跟上數位轉型快速發展
7. 重新思考科技潛力：應該思考如何在資訊科技帶來便利性的同時，保有相對應的安全機制
8. 注重互連的品質：數位連結關注的焦點逐漸從數量轉移至連結性的品質

意見交流



Deloitte.

勤業眾信