張世豪教授 Henry

2000 年

分散式多媒體系統碩士學位　英國利物浦約翰摩斯大學

2009 年

計算與數學科學博士學位　英國利物浦約翰摩斯大學

✓

✓

經歷

- ✓ 朗訊科技
- ✓ 中華電信研究院
- ✓ NCTU 和 NTU 博士後研究員
- ✓ 淡江大學助理教授，副教授
- ✓

研究興趣

- ✓ 無線感測器網路
- ✓ 網路和資訊安全
- ✓ 物聯網

前言

- 通信技術早已融入日常生活的各個層面，如物聯網（ IoT ）、人工智慧（ AI ）、 5G 行動網路等技術，這引發了新一波的數位化革命浪潮。
-
- 這一波的數位化革命使得 OT 與 IT 環境之間的隔閡日漸消失，工業 4.0 與關鍵基礎領域高度仰賴的工業物聯網 (lloT) 的運用造成工業操控技術 OT 以及工業控制系統 (ICS) 遭駭客攻擊風險正急遽上升。
-
- 過去 10 年中發生的許多案例中都發現，使用工業控制系統的國家關鍵基礎設施，以及各產業的自動化生產、製造設備，受到網路攻擊率大增，顯見 OT 或 ICS 系統由於缺乏保護與資安意識，因此比以往都更容易受到攻擊。
-
- 近幾年來，政府與業者們開始正視 ICS 與 SCADA 的安全性，注重關鍵基礎設施在應用此種操作型科技系統（ Operation Technology ， OT ）時的防護。因此，對 OT 及 ICS 系統的基礎架構的熟悉與防禦能力需要進行全面而持續的強化。

單元一 ：工控技術 (OT) 與工業物聯網 (IIoT) 介紹

工控技術 (OT) 介紹

什麼是 OT ？

工業控制系統 (ICS, PLC, DCS)

IT 和 OT 的融合，分析與比較

產業環境的轉變與資安的挑戰

物聯網 (IoT) 與工業物聯網 (IIoT) 介紹

物聯網的過去與未來

工業物聯網的應用情境

對 OT ， IIoT 與關鍵基礎設施的攻擊

臺灣目前遭遇到的營運技術和物聯網資訊安全挑戰

問題討論時間

什麼是 OT ？

- **IT** 是使用電腦系統作儲存、檢索、傳輸、資料共享和操作。

例如：**CRM**、 **ERP**、電子郵件等。

- **OT** 是一種硬體和軟體，通過直接監控或控制實體設備來檢測或導致更改。
- 例如：SCADA、 PLCS、 HMIs 等。
-

什麼是 OT ？

- OT 是一種直接監督與控制實體設備執行情況的軟體與硬體；而這圍繞著許多應用系統，例如與水電供應有關的監控與資料擷取系統，以及能源管理系統（ EMS ），用於煉油、化工處理、火力發電輔助的分散管理系統（ DCS ）
-
- 在火力、核能、風力等發電廠採用的流程控制系統（ PCS ），資料中心環境控制系統有關的建築物自動化系統（ BAS ）與管理系統（ BMS ），核電生產的執行與控管系統（ I&C ），以及用於煉油、化工生產與發電的安全儀表防護系統（ SIS ）。
-
- OT 裝置並非只出現在工廠，或是油水電等關鍵基礎設施場域，各個行業幾乎都有。產業、設施用途的控制與自動化系統，而與其相關的國際安全標準 ISA 99/IEC 62443 ，也採用了 ISA 62443.01.01 的定義，將其界定為足以影響產業流程安全性與可靠度的硬體與軟體。

工業控制系統 Industrial Control Systems (ICS)

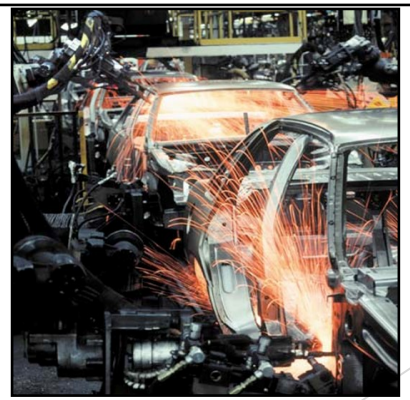
工業控制系統 Industrial Control Systems (ICS)

Supervisory Control And Data Acquisition (SCADA)

Process Control Systems (PCS)

Distributed Control Systems (DCS)

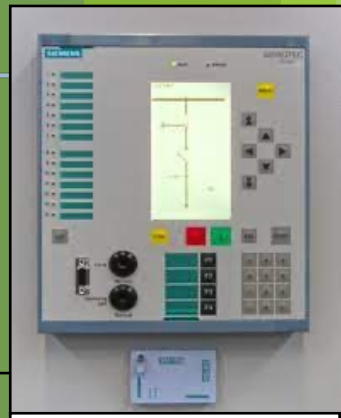
Automation



ICS主流的 ICS 元件

IED
Intelligent Electronic Device

DCS
Distributed Control Systems



RTU
Remote Terminal Units

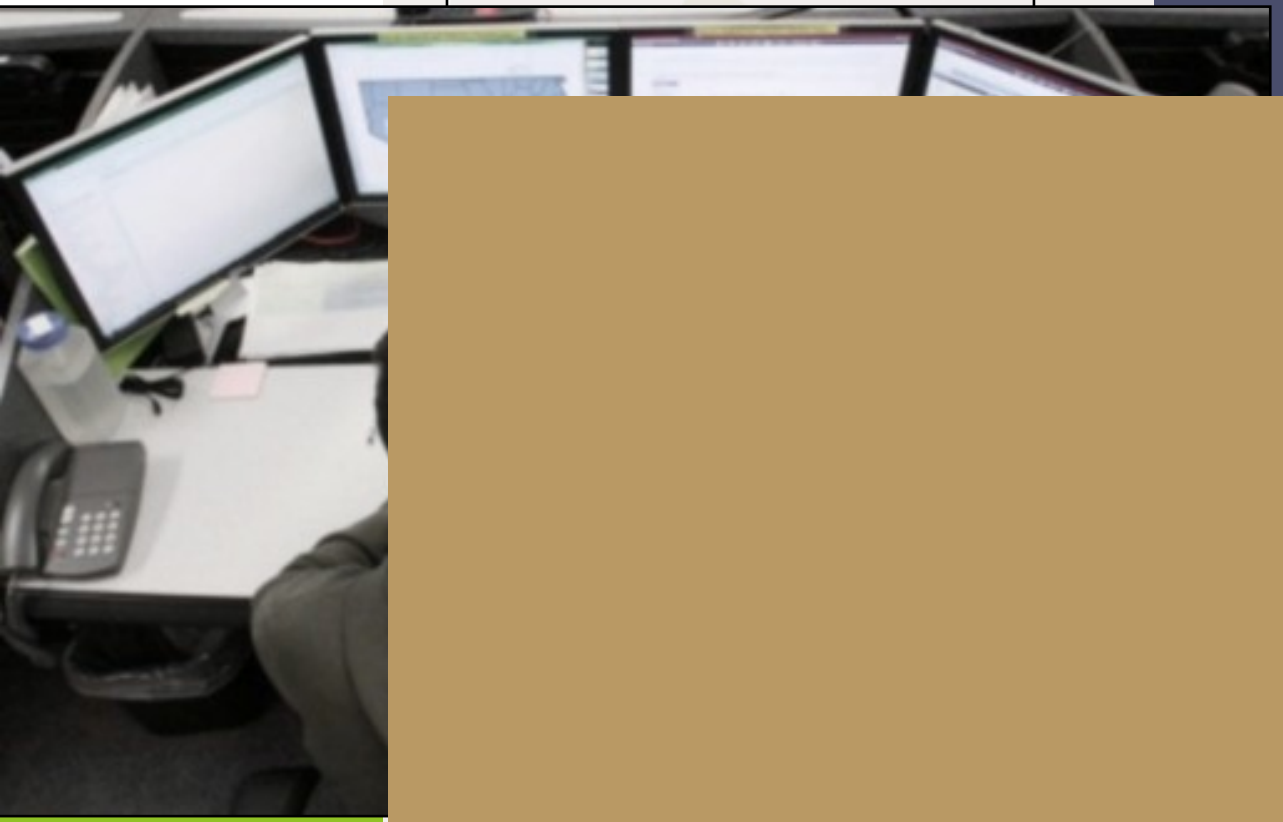
HMI
Human-Machine Interfaces

PLC
Programmable Logic Controllers

SCADA
Supervisory Control and Data Acquisition

主流的 ICS 網路通訊協定

ICS 安全性如何工作？



程和機器的平穩運

制室儀錶板和螢幕上
資訊和數據準確，反
或生產車間的真實情

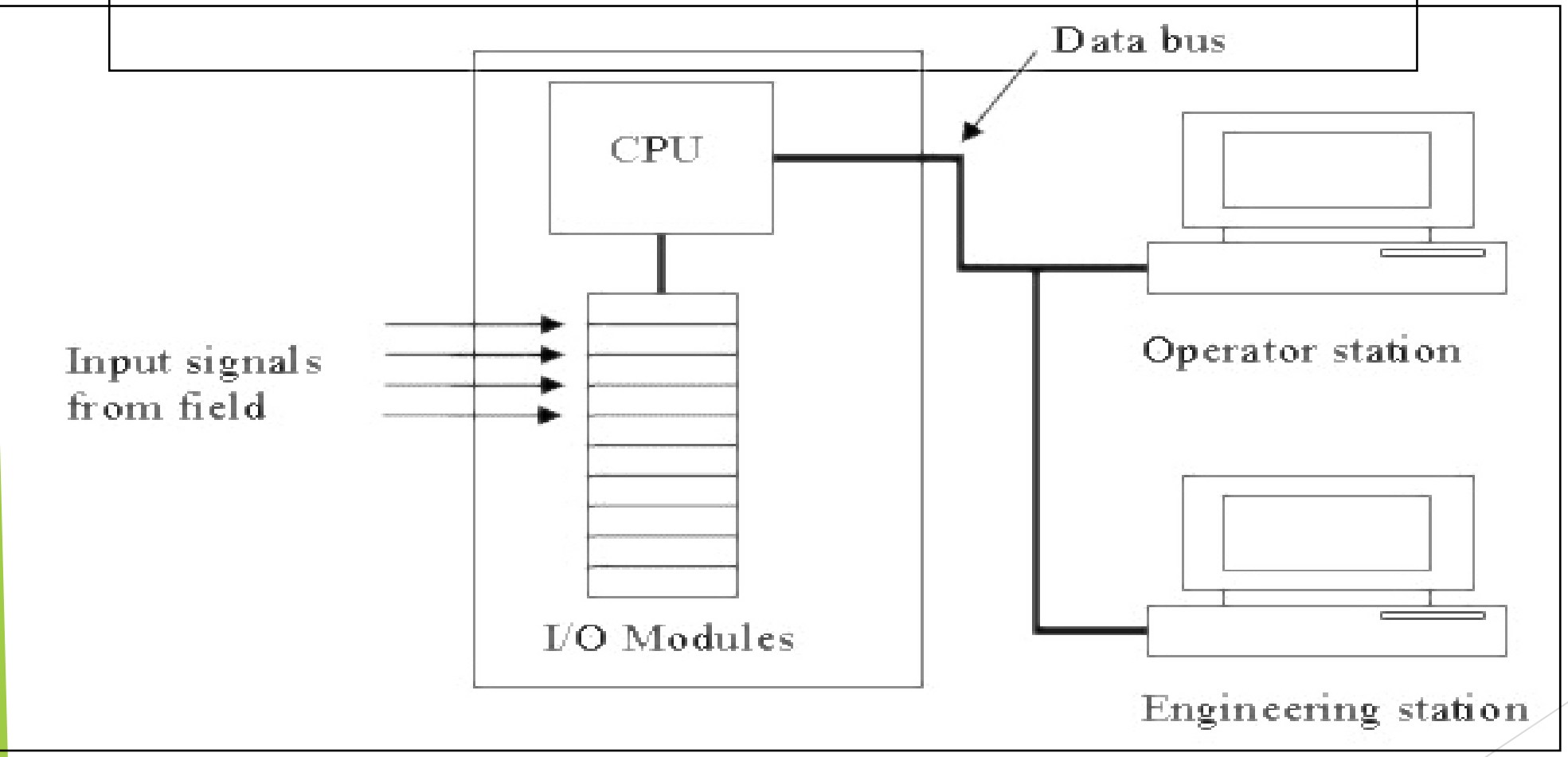
分散式控制系統（DCS)

DCS 是一個特別設計的自動化控制系統，由工廠或控制區域的地理分佈控制元件組成。

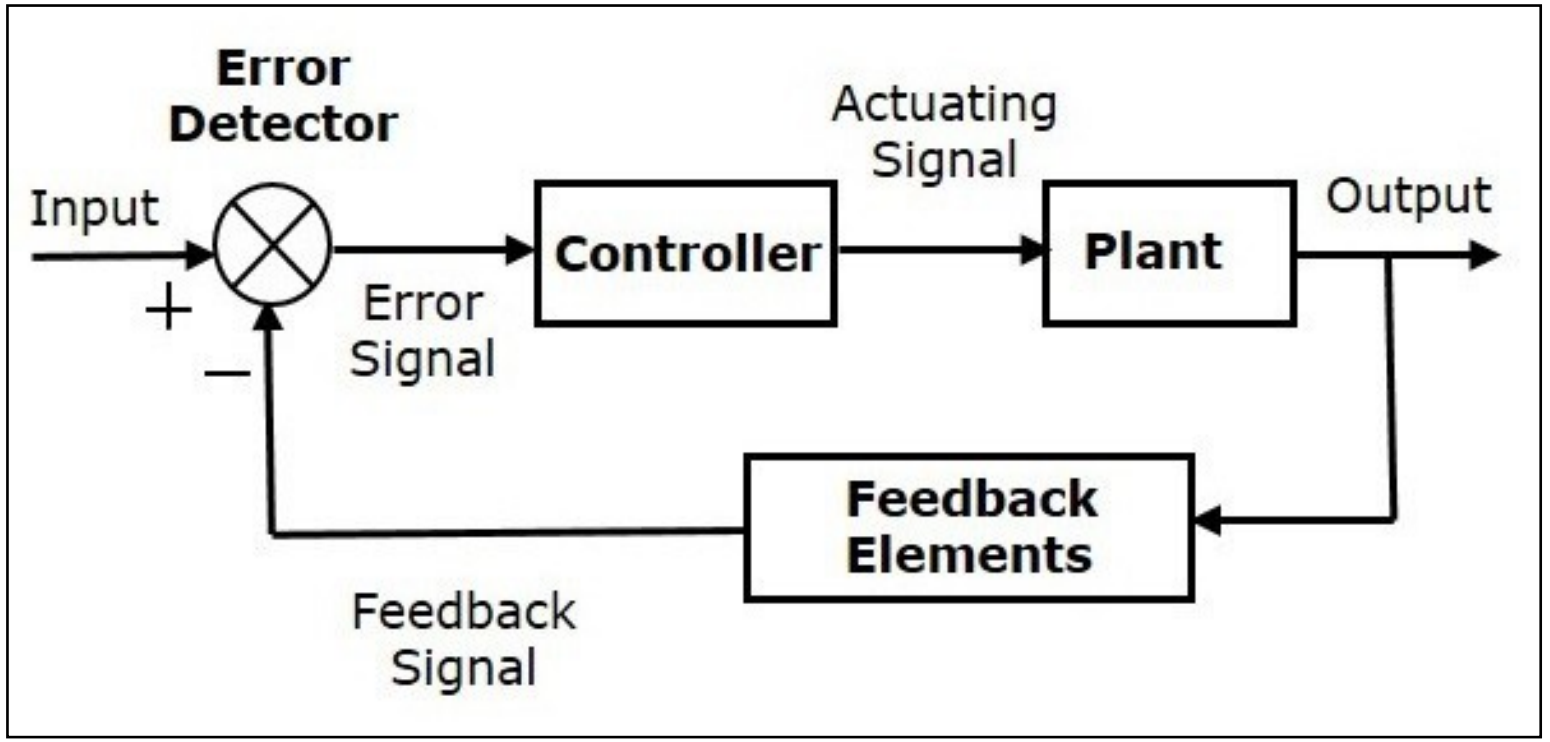
為什麼需要 DCS ？


工廠自動化
Total Plant
Automation.
管理資訊系統
Management
information
system
進階的流程控
制
Advanced
process

DCS 如何運作？


Data bus
CPU
Input signals
from field
I/O Modules
Operator station
Engineering station

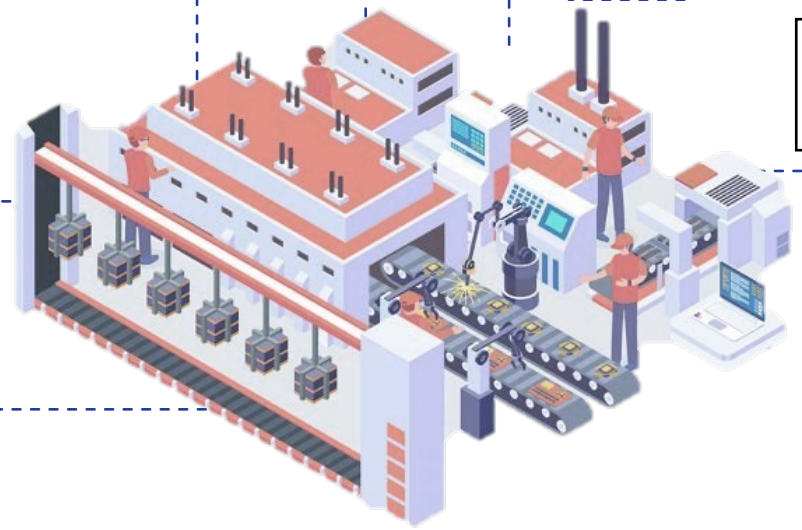
閉路控制系統
Closed Loop Control Systems



直流元件

業務集成

現場設備



輸入 / 輸出模組

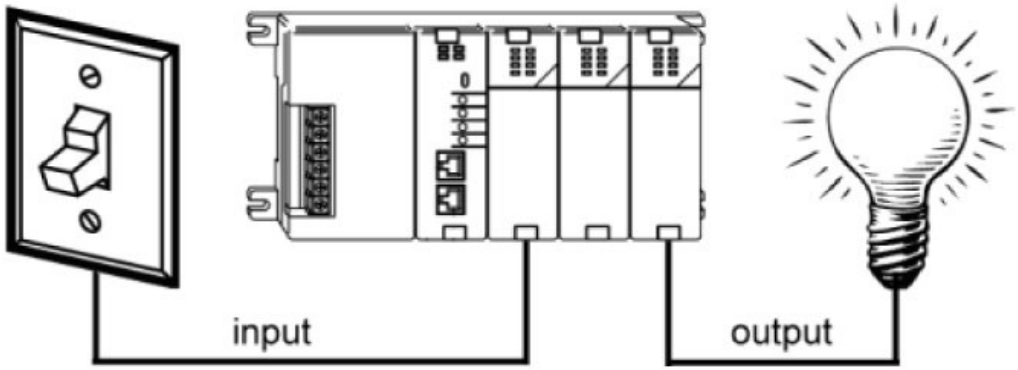
監控

人機介面
（ HMI ）

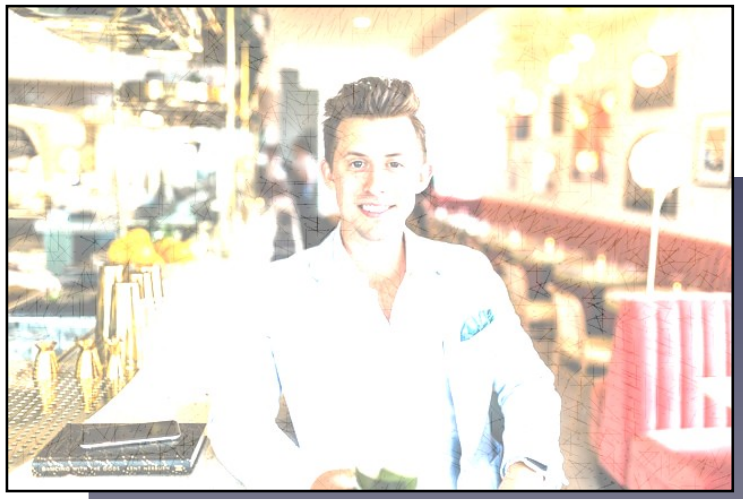
控制器

什麼是 "PLC"？

可程式設計邏輯控制器（**PLC**）或可程式設計控制器是一種工業數位電腦，經過堅固耐用，可控制製造過程，如裝配線或機器人設備，或任何需要高可靠性、易程式設計和過程故障診斷的活動。



Basics of PLC



我

· 梯子圖（ LD ）

清單（ IL ）聲明

結構文字（ ST ）

功能塊圖（ FBD ）

順序函數圖表（ SFC ）

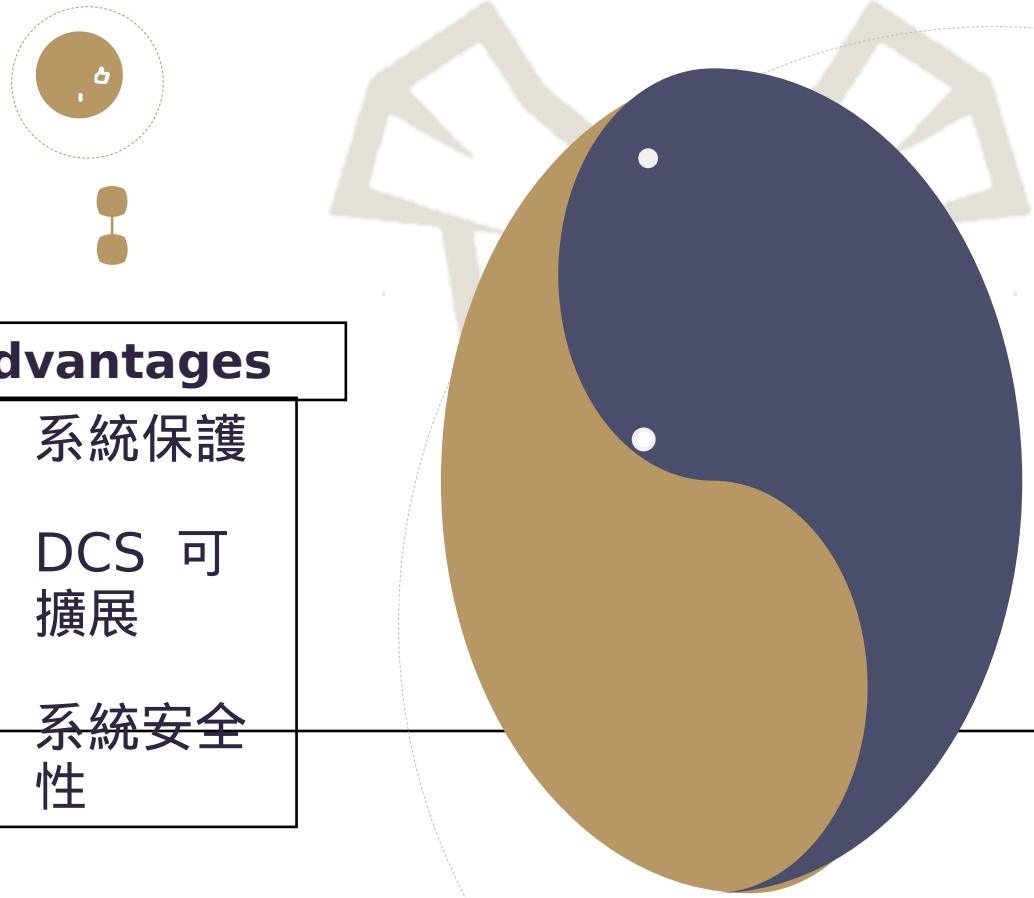
人機介面（HMI）

- 人機介面（HMI）是一種設備或軟體，用於與工廠或生產區域的機器或機器組進行通信。
-

人機介面（HMI）

- HMI 直接通過在監視器上的圖形表示將大量複雜數據轉換為可訪問的資訊，即可將人與機器連接起來。

分散式控制系統（DCS)



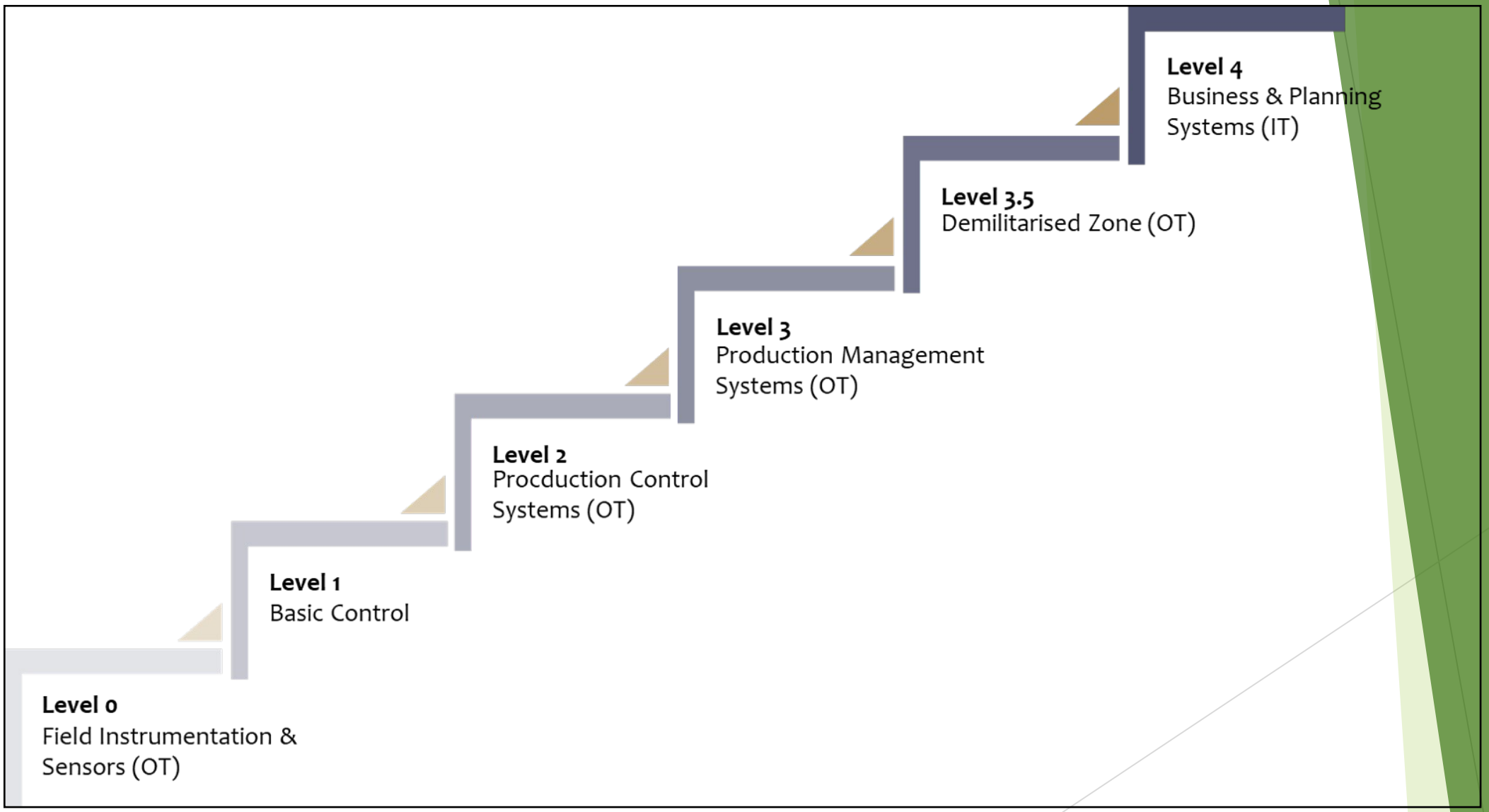
Advantages

- 系統保護
- DCS 可擴展
- 系統安全性

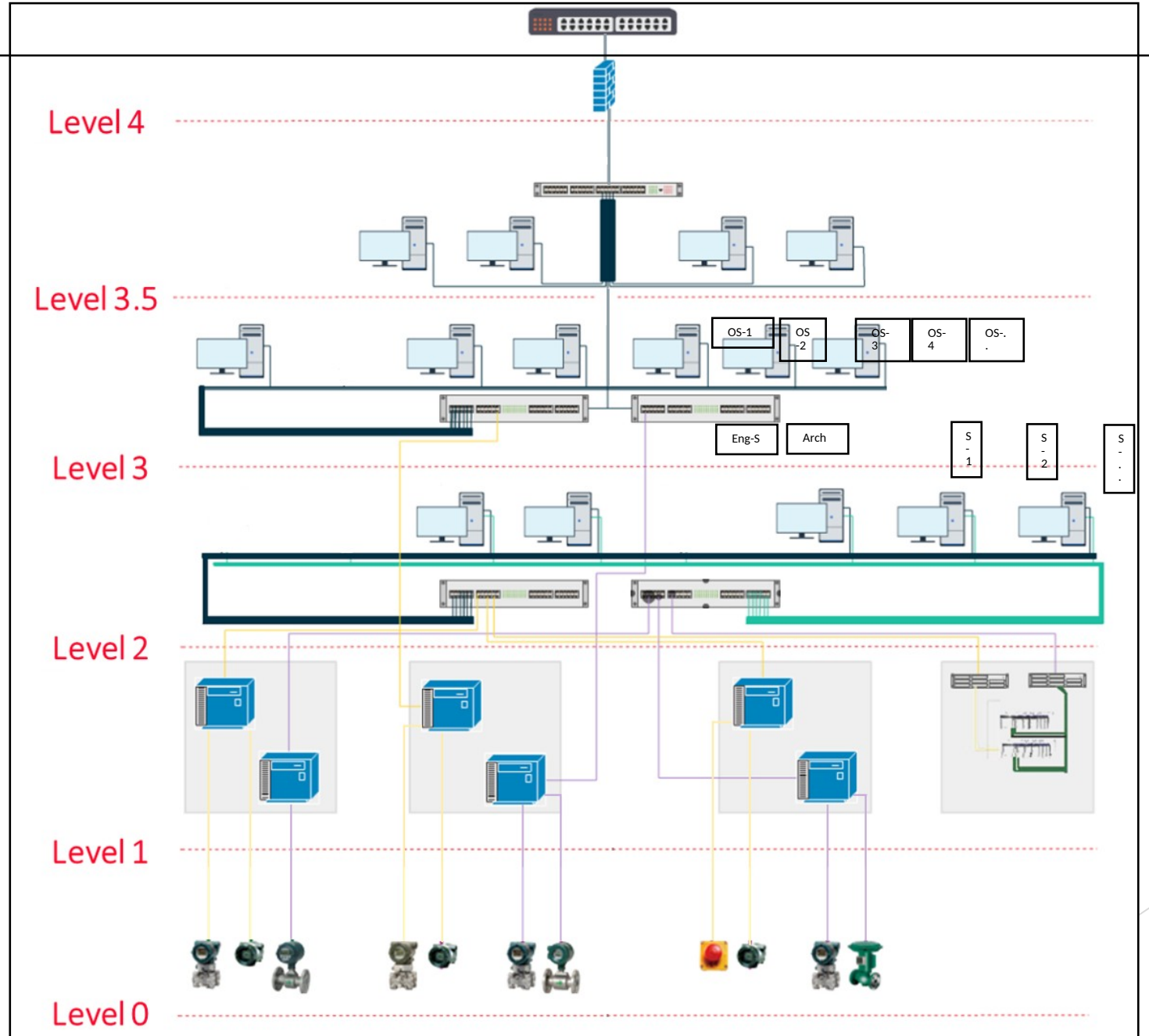
Disadvantages

- 操作員在處理時要保持警惕和小心。
- 一個控制器的故障會影響多個迴圈。

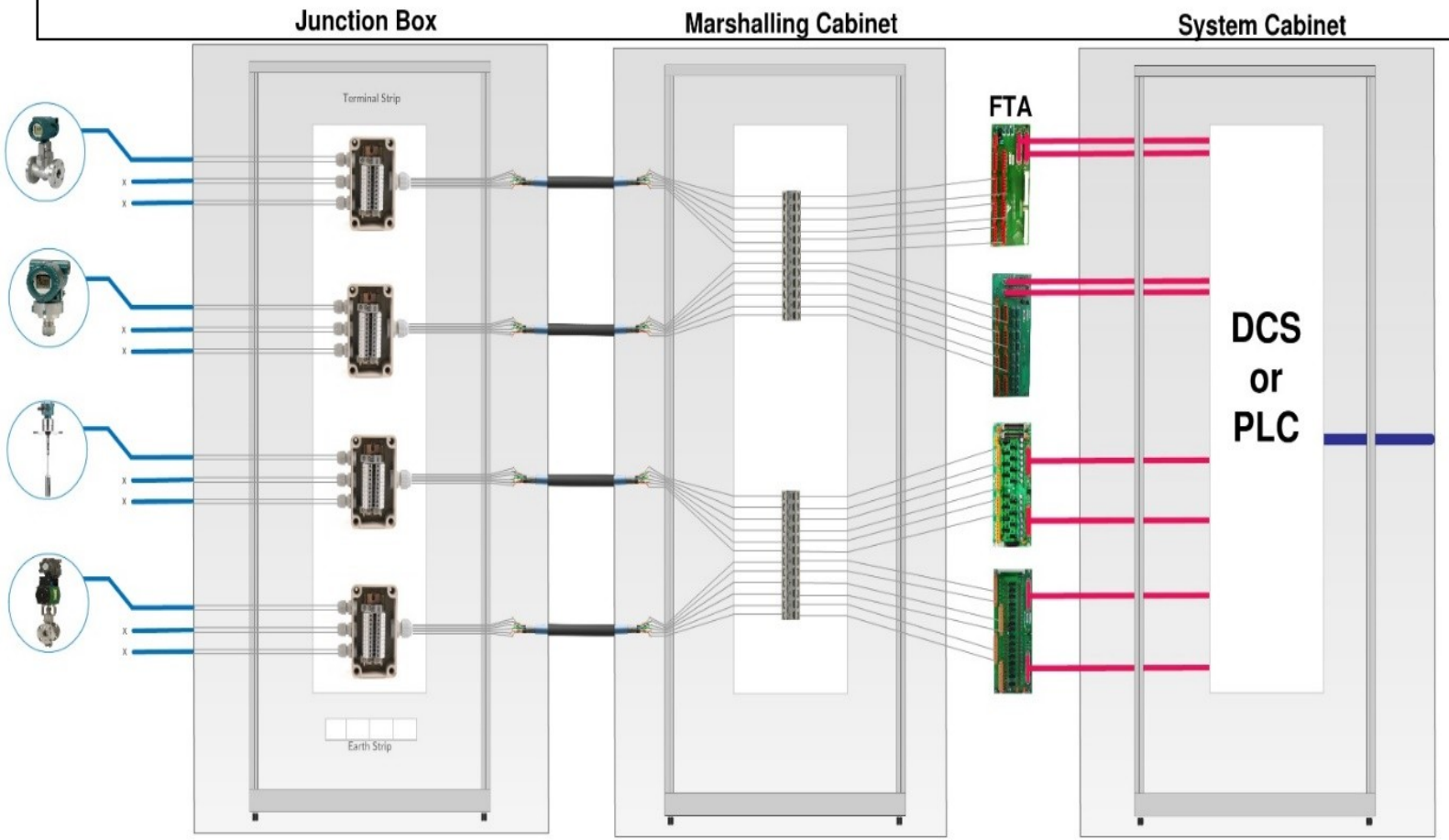
分散式控制系統階段（ DCS Level ）



分散式控制系統架構 DCS Architecture



分散式控制系統架構 DCS Architecture



Field/Branch Cables

HomeRun/Main Cables

FTA Cables

Data Communication Cables

儀器信號來自感測工廠場域到分散控制系統

IT x OT

有處理資訊需求之產業

關鍵基礎設施、製造、機械、醫療.....

產 業

IT(Information Technology)

主要用於管理和處理資訊所採用的技術總稱，可包含軟體、硬體及應用等三個層次

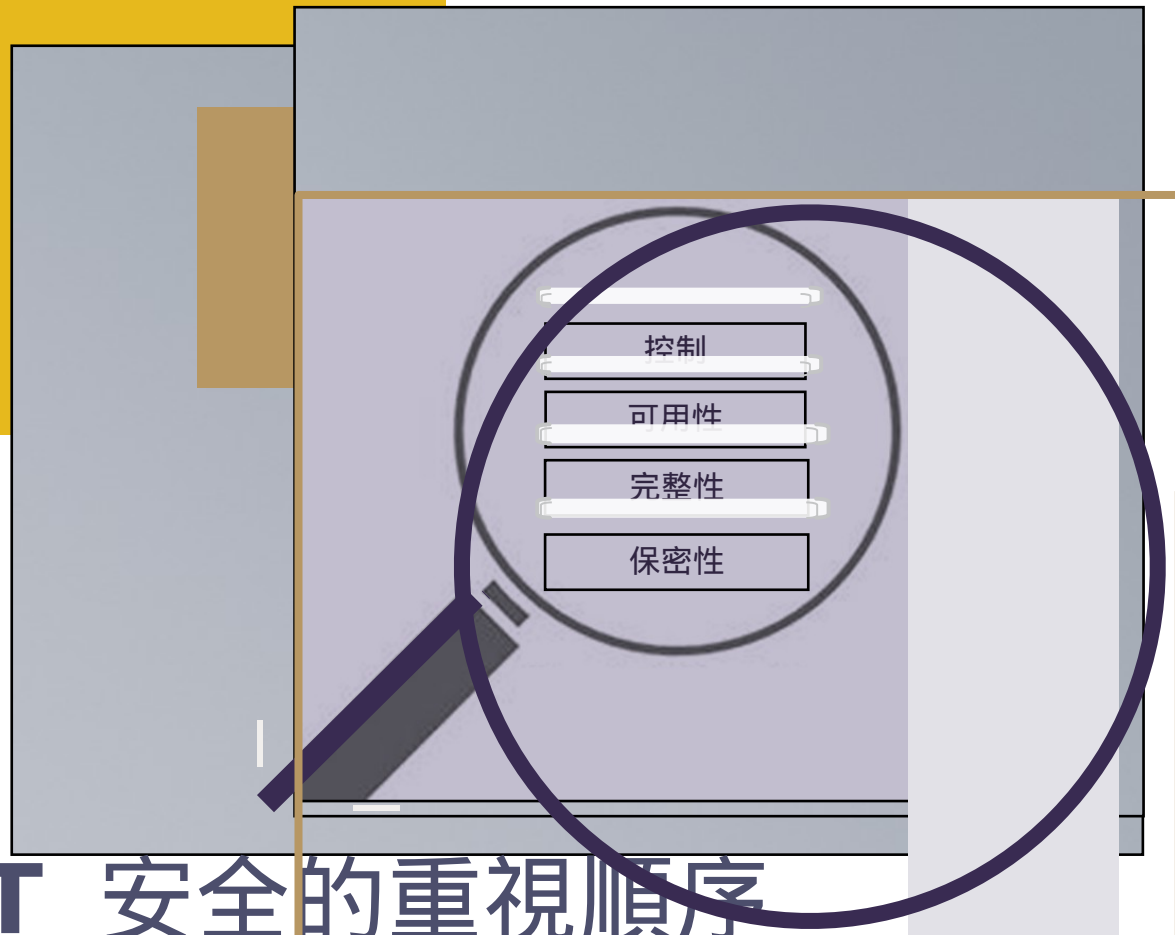
OT(Operation Technology)

泛指可對實體設備進行監測、控制及操作的軟體及硬體

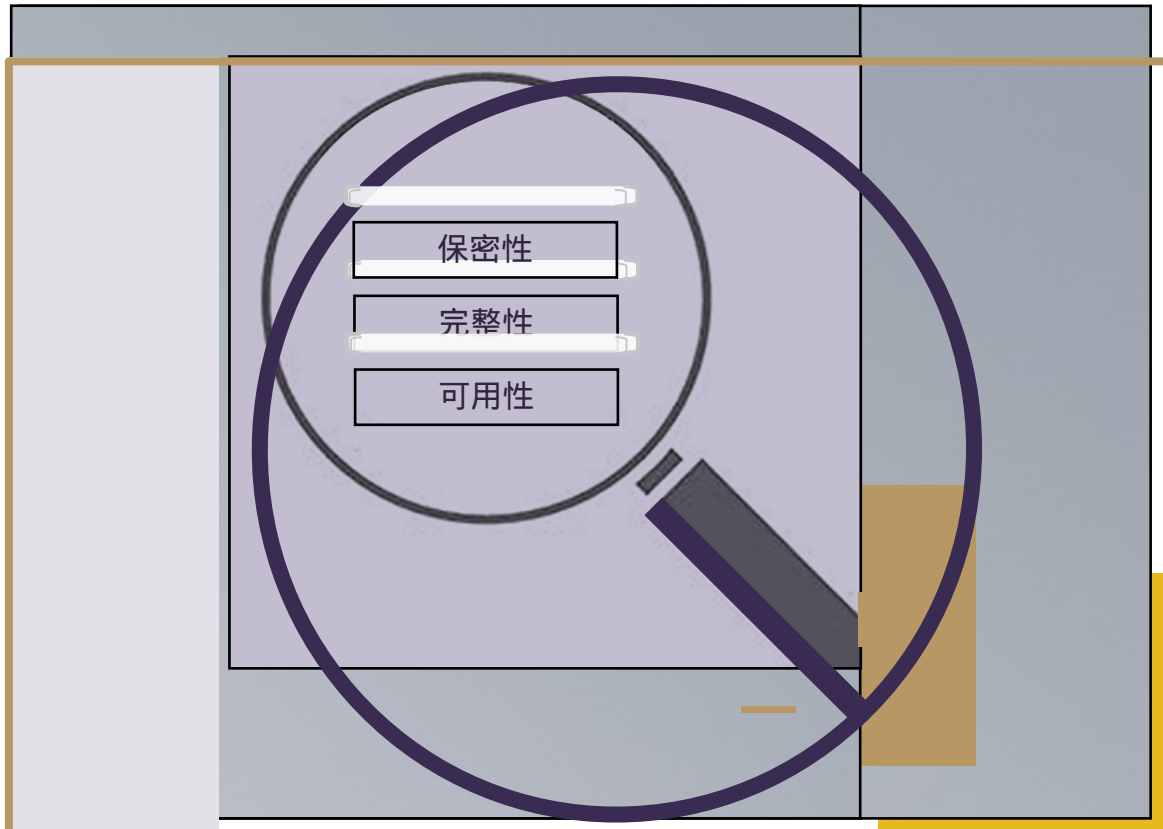
應用

應用場景

OT 安全的重視順序



IT 安全的重視順序



IT / OT 比較表

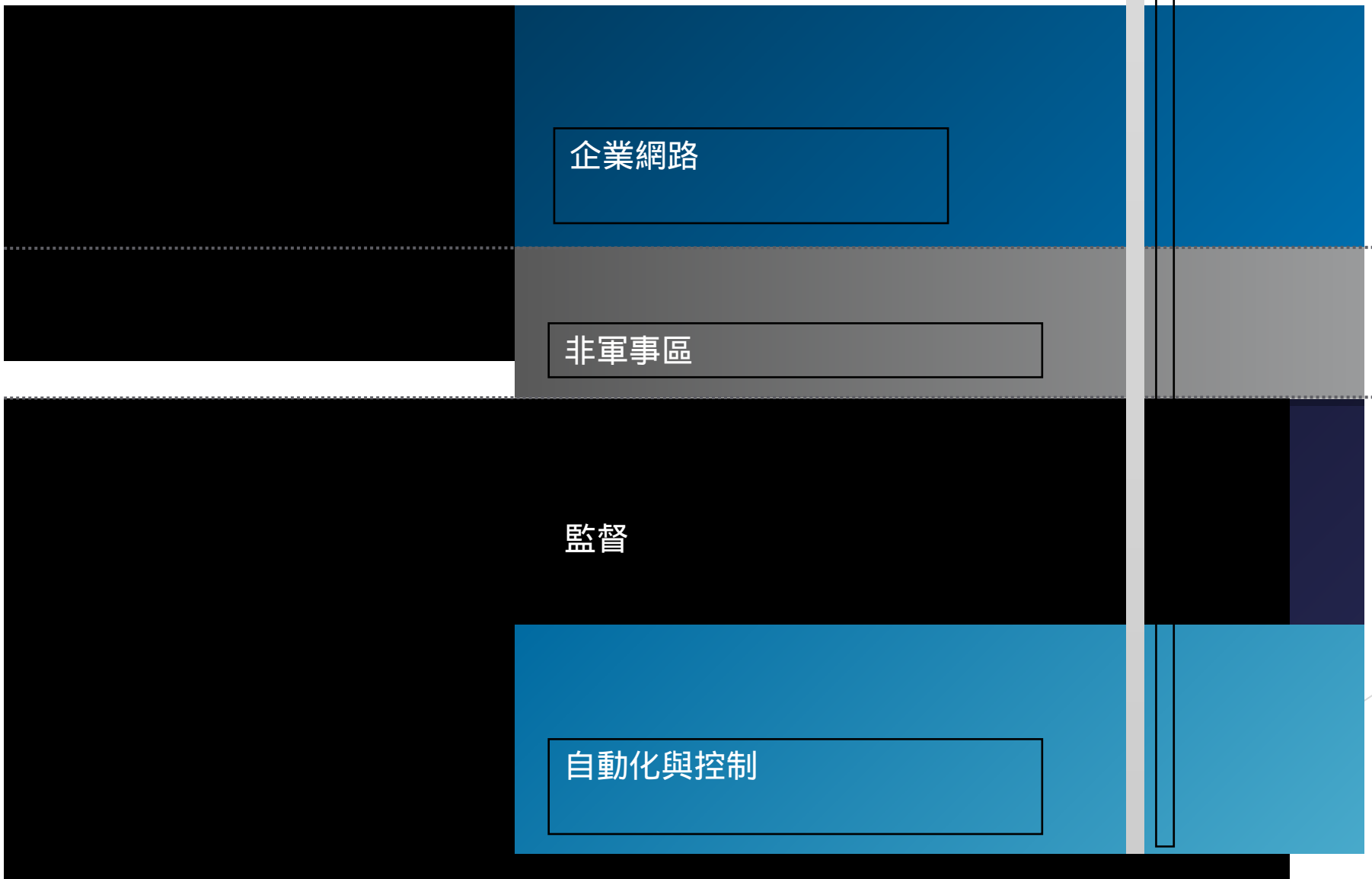
	IT	OT
使用範圍	• 以業務為導向	• 以工業為導向
資料存取	• 與外界相連	• 非常有限定的相連
生命週期	• 更短的生命週期（3-5年）。	• 更長的生命週期（15-20年）
作業系統	• 標準作業系統	• 專有的系統系統
任務	• 以業務為中心	• 以機器自動化為中心
環境	• 可控制、固定且穩定	• OT 忍受惡劣的天氣條件

IT 和 OT 本質上的不同

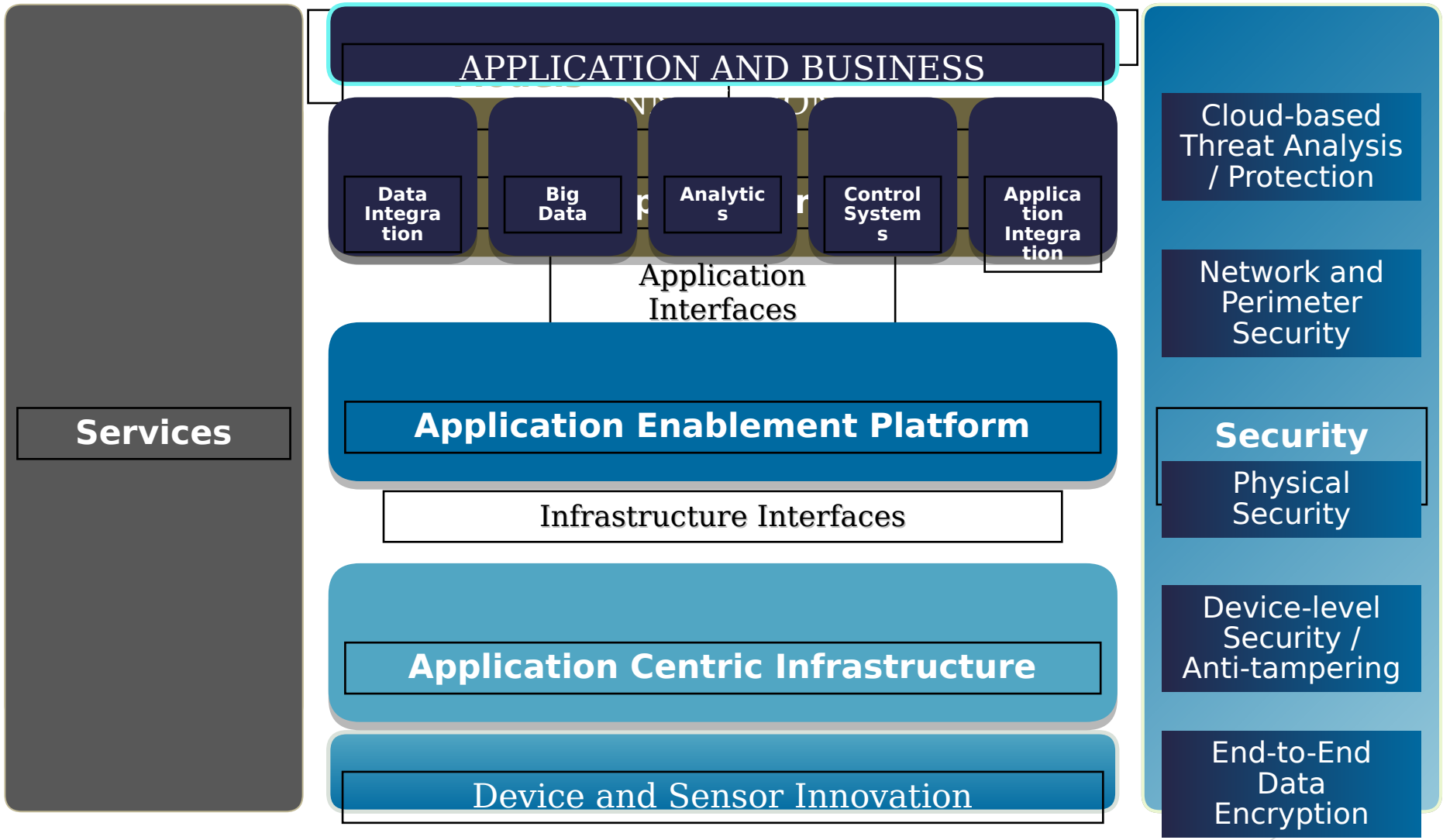
- IT
  - 連接：" 從任意到任何 "
  - 網路姿態：保密性、完整性、可用性（ CIA ）
  - 安全解決方案：網路安全；數據保護
  - 應對攻擊：隔離 / 關閉以減輕

- OT
  - 連接：層次分明
  - 網路態勢：可用性、完整性、保密性（ AIC ）
  - 安全解決方案：物理訪問控制；
  - 安全對攻擊的反應：不停的操作 / 任務關鍵 + 永不停止，即使被破壞

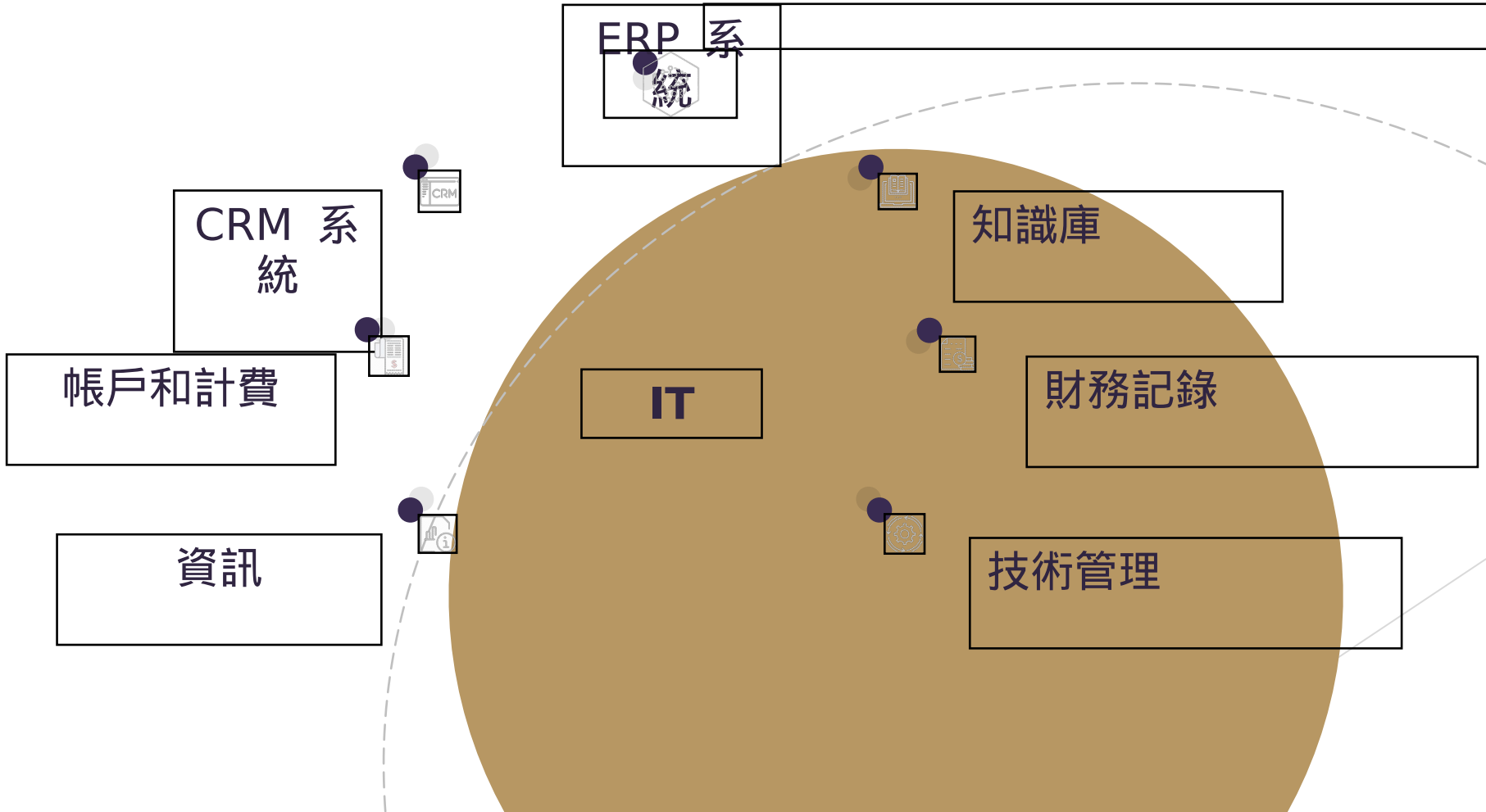
IT/OT 融合安全模型



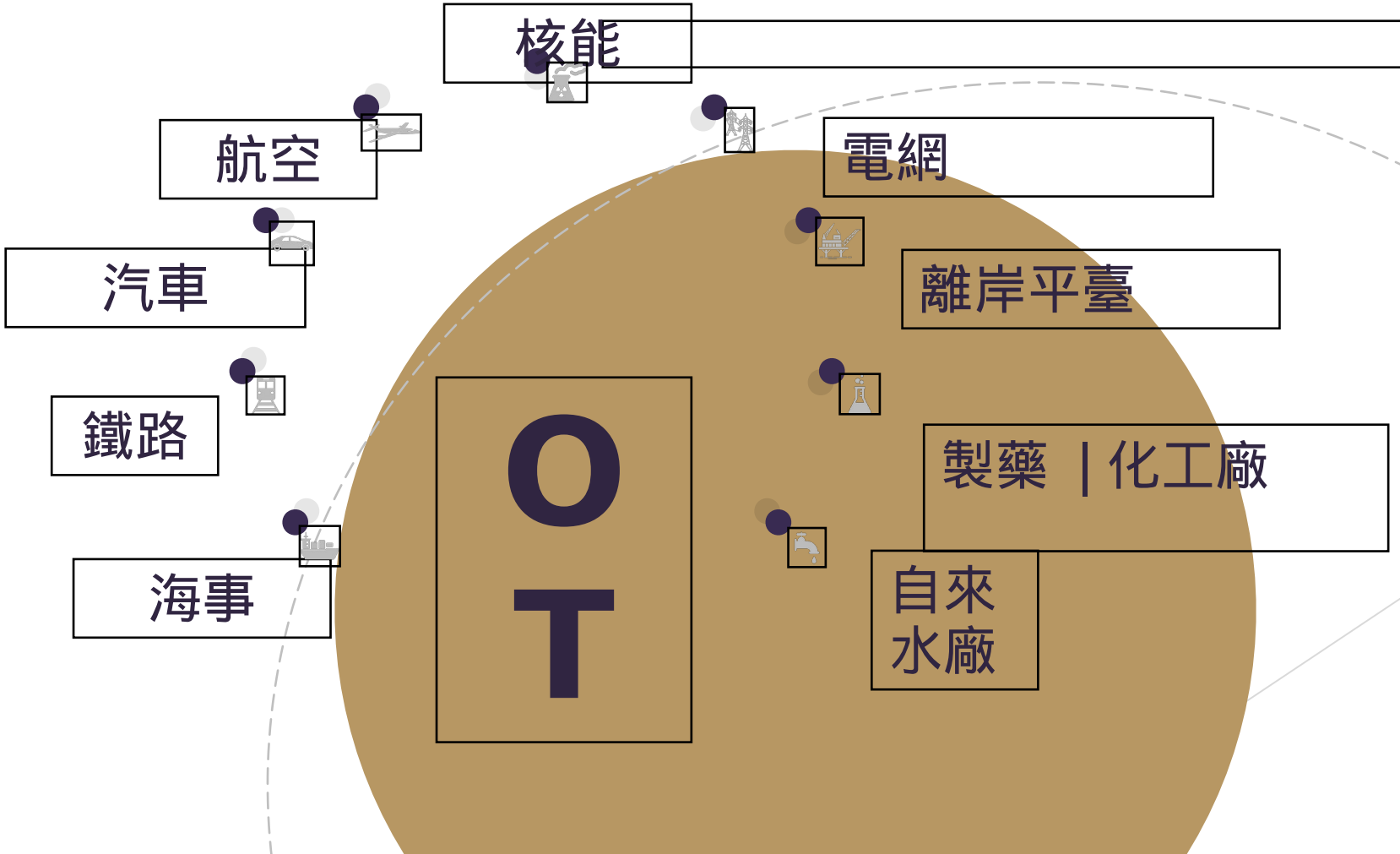
安全物聯網架構：IT 加 OT！



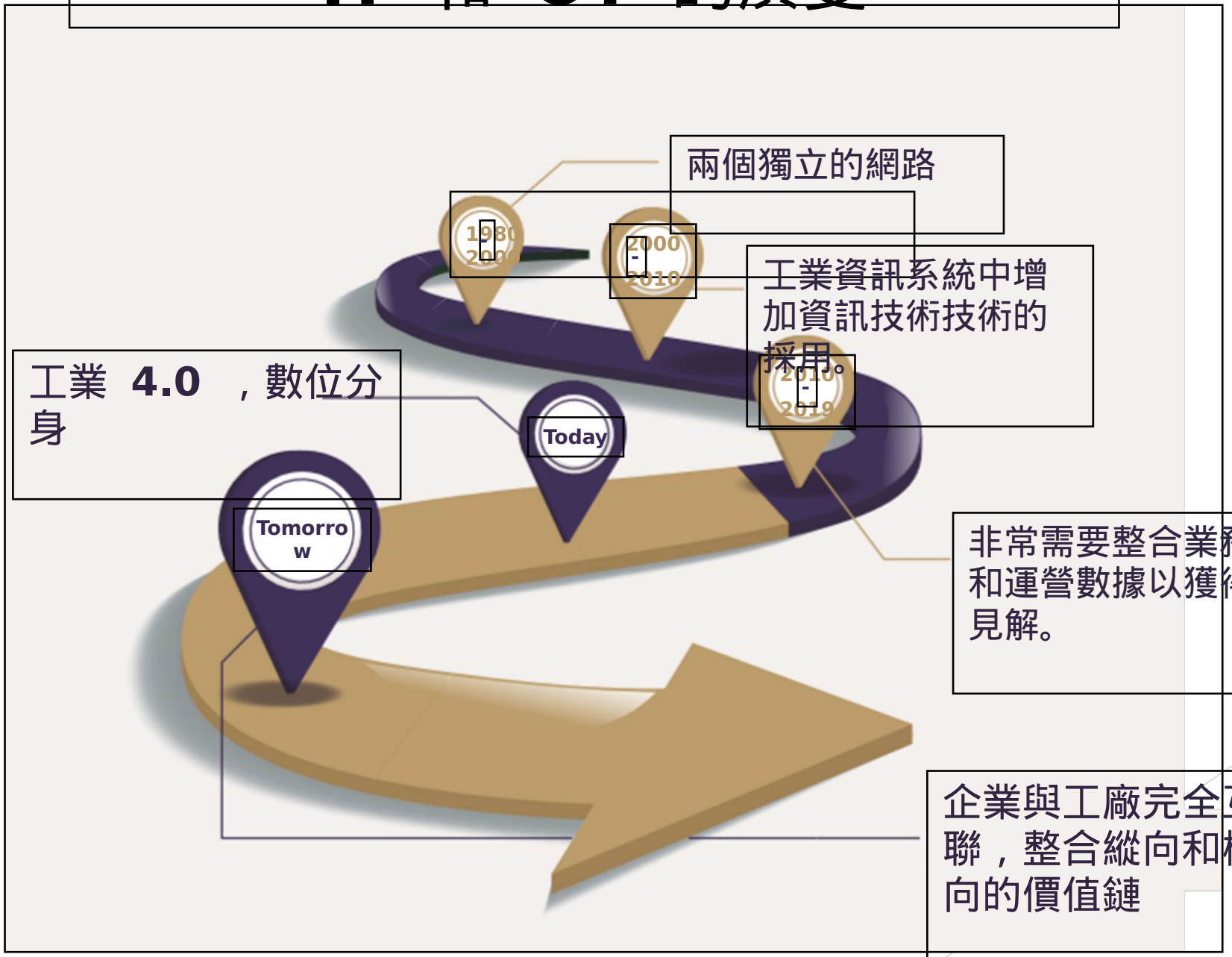
虛擬資產



實物資產



IT 和 OT 的演變


兩個獨立的網路
2000
-
2010
工業資訊系統中增加資訊技術技術的採用。
2010
-
2019
工業 4.0 ，數位分身
Today
Tomorrow
非常需要整合業務和運營數據以獲得見解。
企業與工廠完全互聯，整合縱向和橫向的價值鏈

產業環境轉變 – OT與IT融合

能源

民生資源

醫療

ERP系統

行政PC

叫號系統

機械設備

超音波儀

投藥設備

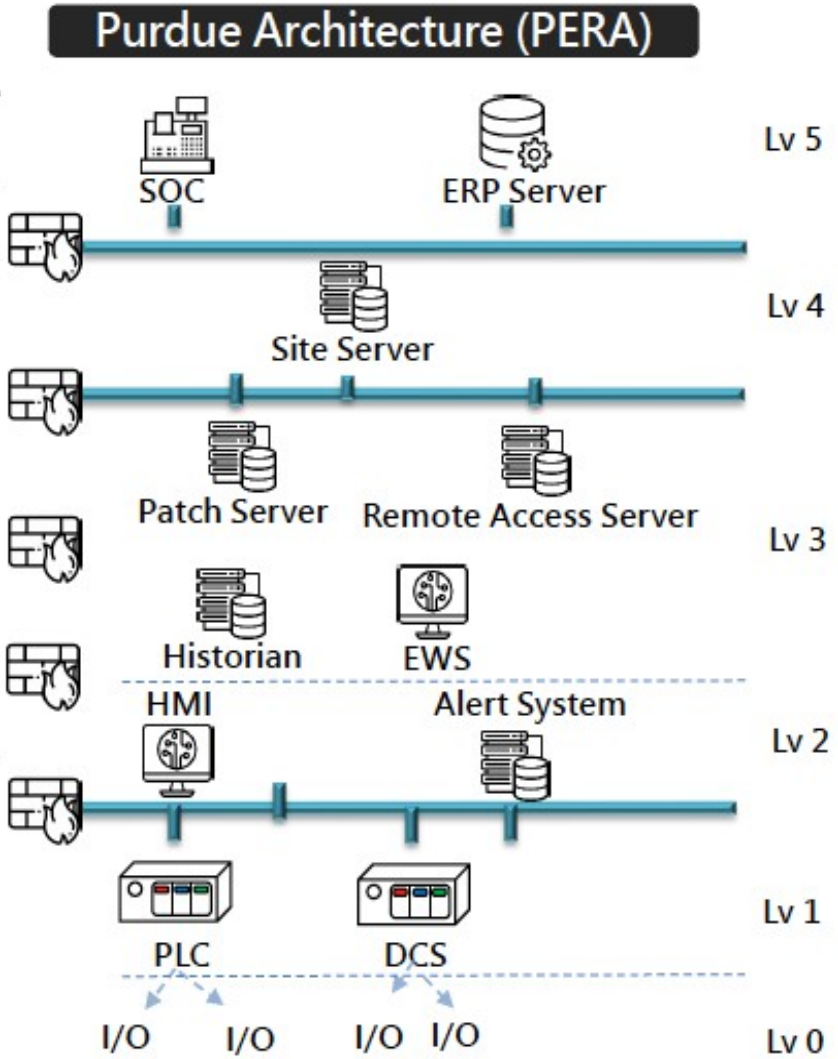
CT攝影儀器

控制設備

核磁共振儀器

IT

OT



ICS 元件識別的漏洞分佈

其他

工業視訊監控系統

工業 PC 和伺服器

PLCs

網路設備

軟體工程

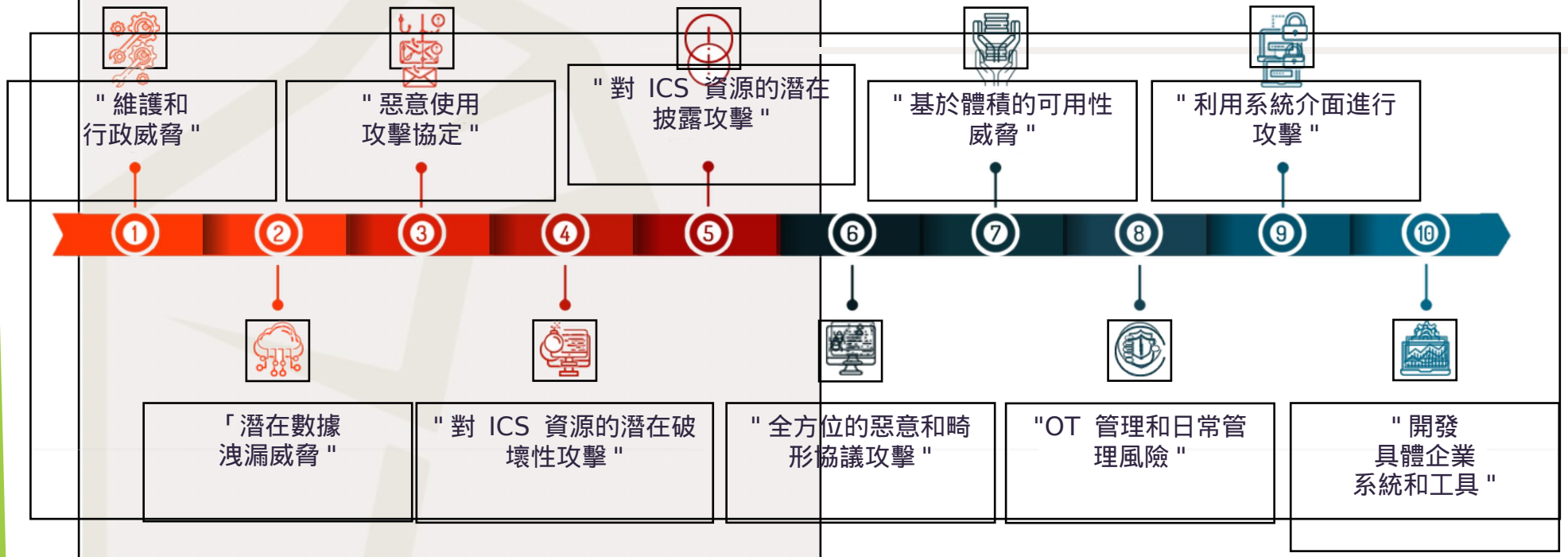
HMI/SCADA

工業網路安全認證

GICSP

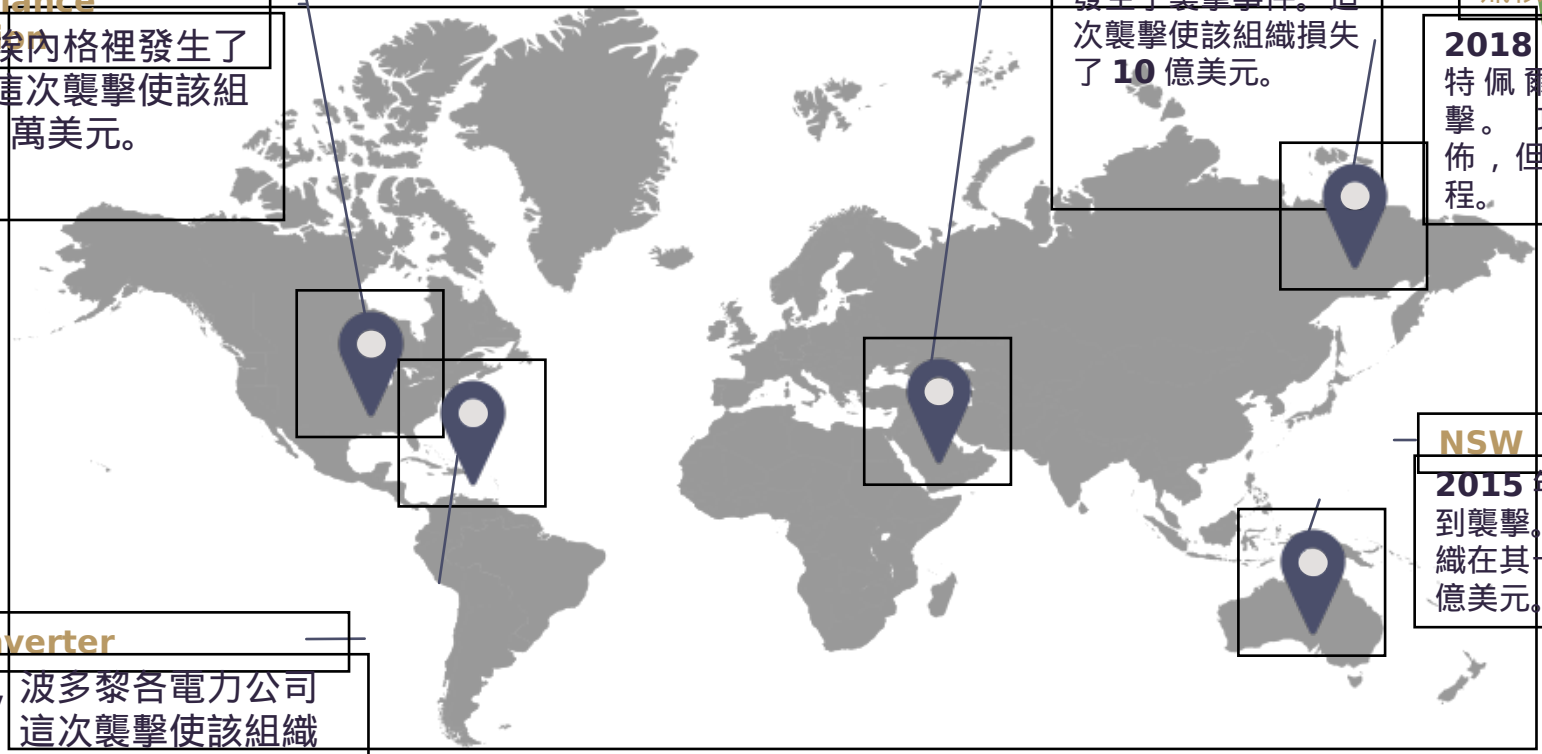
Global Industrial Cyber Security Professional

十大運營技術安全威脅



Source: Bayshore networks

近年來針對運營技術攻擊重大事件



Compliance Violation

2019 年，杜克埃內格裡發生了一起襲擊事件。這次襲擊使該組織損失了 **1 000** 萬美元。

Optical Converter

2012 年，波多黎各電力公司遭到襲擊。這次襲擊使該組織損失了 **1** 億美元。

沙蒙

2012 年，沙特阿美發生了襲擊事件。這次襲擊使該組織損失了 **10** 億美元。

氚核

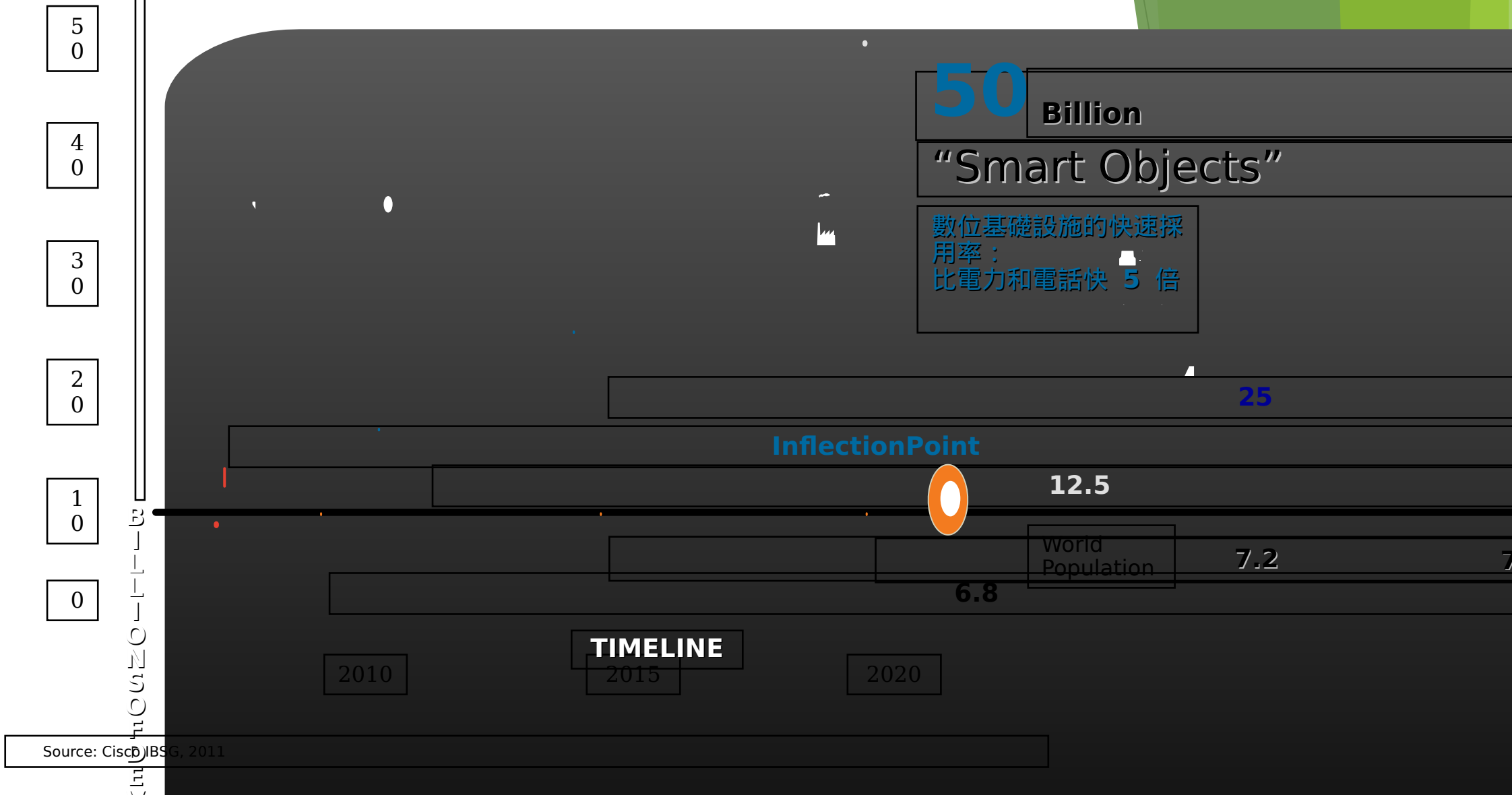
2018 年，俄羅斯在沙特佩爾托切姆發動襲擊。攻擊成本尚未公佈，但它包括業務、流程。

NSW

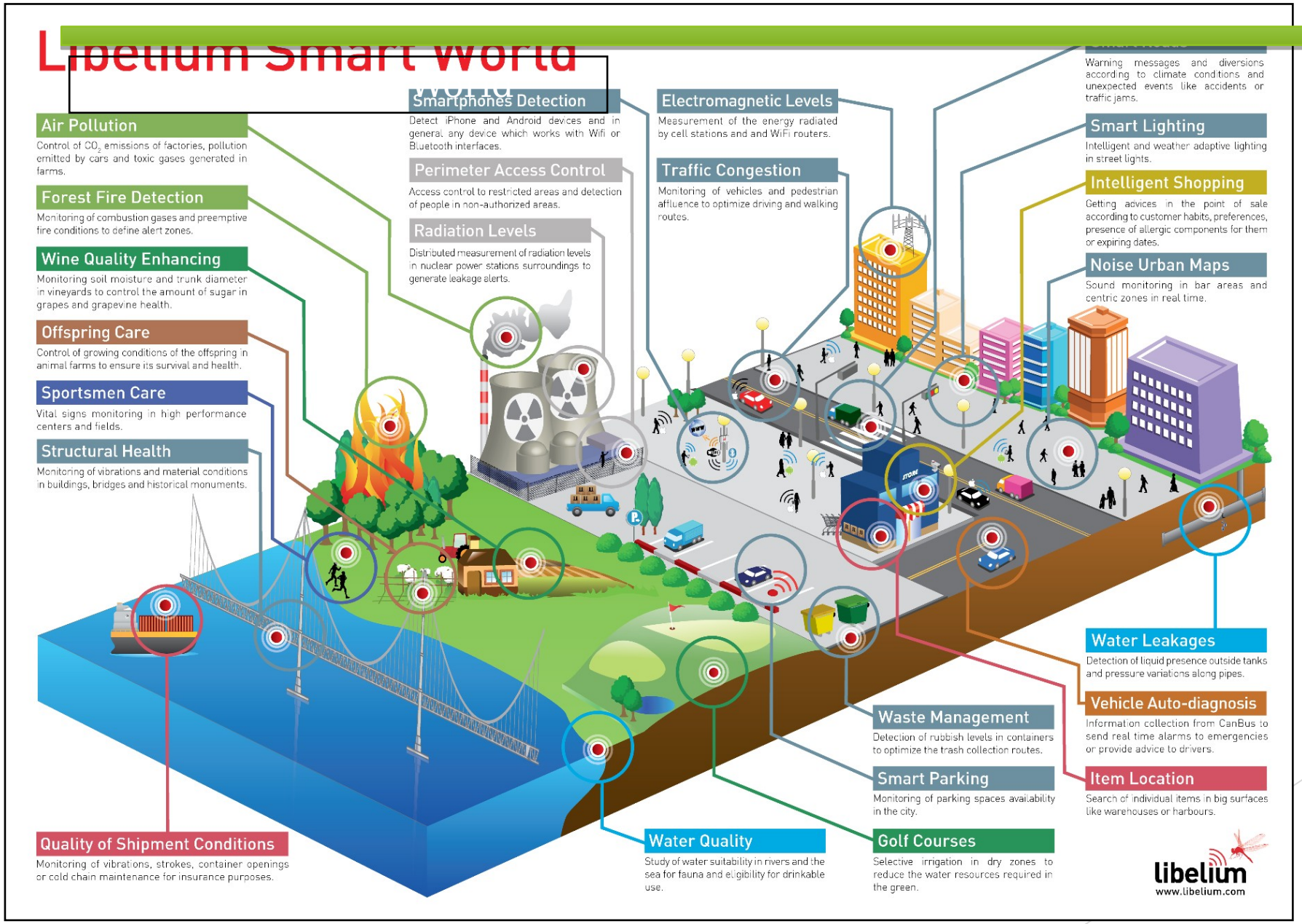
2015 年，澳大利亞政府遭到襲擊。這次襲擊導致該組織在其一個專案上損失了 **12** 億美元。

物聯網與（IoT）與 工業物聯網（IIoT）

物聯網 ： 過去與未來


50
40
30
20
10
0
Billion
50
“Smart Objects”
數位基礎設施的快速採用率：
比電力和電話快 5 倍
25
InflectionPoint
12.5
World Population
7.2
6.8
TIMELINE
2010
2015
2020
Source: Cisco IBSG, 2011

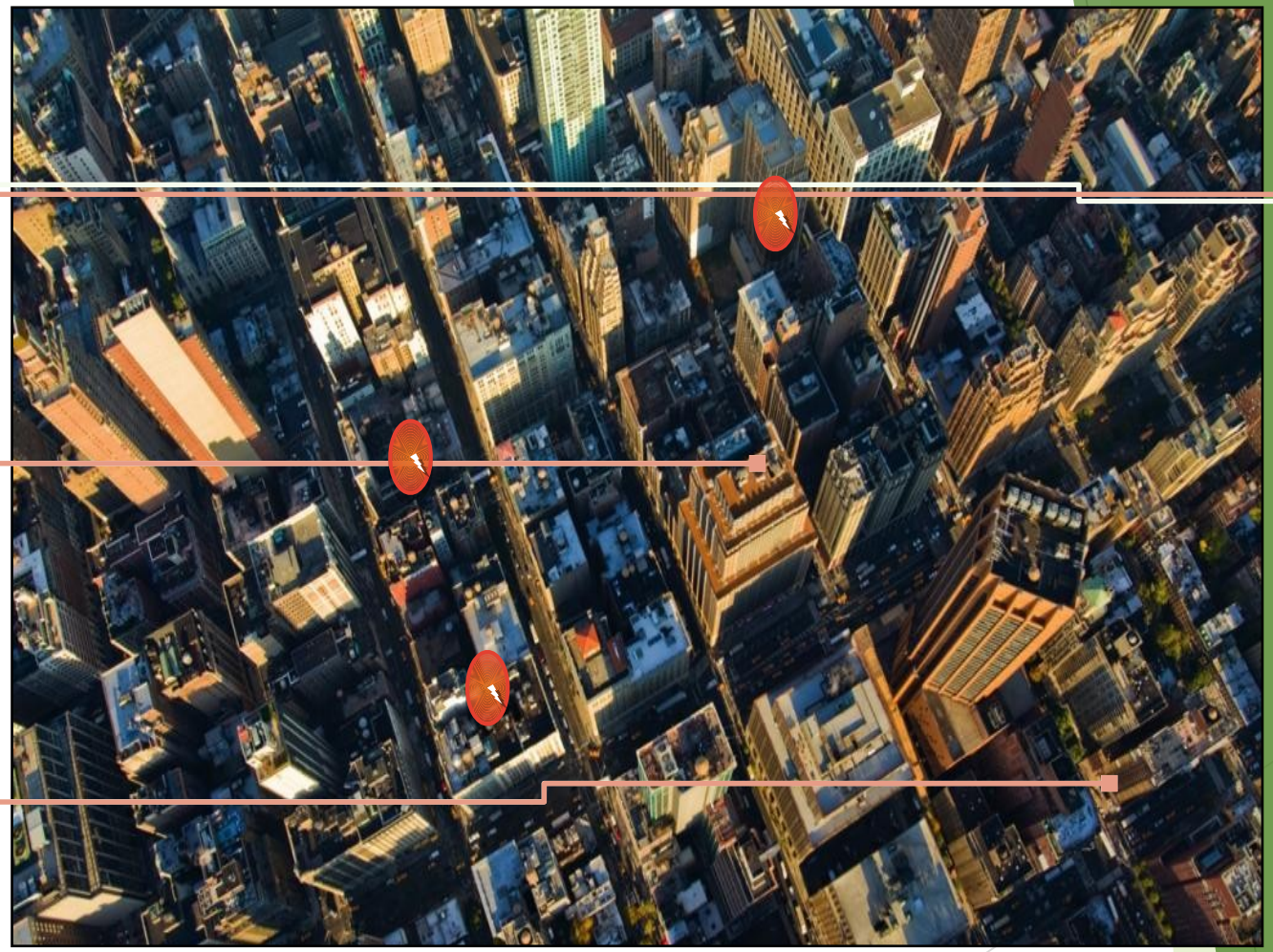
物聯網：過去與未來


Libelium Smart World
Air Pollution
Control of CO_2 emissions of factories, pollution emitted by cars and toxic gases generated in farms.
Forest Fire Detection
Monitoring of combustion gases and preemptive fire conditions to define alert zones.
Wine Quality Enhancing
Monitoring soil moisture and trunk diameter in vineyards to control the amount of sugar in grapes and grapevine health.
Offspring Care
Control of growing conditions of the offspring in animal farms to ensure its survival and health.
Sportsmen Care
Vital signs monitoring in high performance centers and fields.
Structural Health
Monitoring of vibrations and material conditions in buildings, bridges and historical monuments.
Quality of Shipment Conditions
Monitoring of vibrations, strokes, container openings or cold chain maintenance for insurance purposes.
Smartphones Detection
Detect iPhone and Android devices and in general any device which works with Wifi or Bluetooth interfaces.
Perimeter Access Control
Access control to restricted areas and detection of people in non-authorized areas.
Radiation Levels
Distributed measurement of radiation levels in nuclear power stations surroundings to generate leakage alerts.
Electromagnetic Levels
Measurement of the energy radiated by cell stations and and WiFi routers.
Traffic Congestion
Monitoring of vehicles and pedestrian affluence to optimize driving and walking routes.
Water Quality
Study of water suitability in rivers and the sea for fauna and eligibility for drinkable use.
Waste Management
Detection of rubbish levels in containers to optimize the trash collection routes.
Smart Parking
Monitoring of parking spaces availability in the city.
Golf Courses
Selective irrigation in dry zones to reduce the water resources required in the green.
Warning messages and diversions according to climate conditions and unexpected events like accidents or traffic jams.
Smart Lighting
Intelligent and weather adaptive lighting in street lights.
Intelligent Shopping
Getting advices in the point of sale according to customer habits, preferences, presence of allergic components for them or expiring dates.
Noise Urban Maps
Sound monitoring in bar areas and centric zones in real time.
Water Leakages
Detection of liquid presence outside tanks and pressure variations along pipes.
Vehicle Auto-diagnosis
Information collection from CanBus to send real time alarms to emergencies or provide advice to drivers.
Item Location
Search of individual items in big surfaces like warehouses or harbours.
libelium
www.libelium.com

智慧城市

連接交通信號
- 減少擁堵
-
- 改進緊急服務回應時間
- 降低燃油使用量

停車場和照明
- 提高效率
- 節省電力和成本
- 新的收入機會



城市服務
- 高效服務交付
- 增加收入
- 增強環境監測能力

安全、財務和環境效益

智慧交通

乘客安全
- 站內和車載安全

關鍵事件的可見性

路線優化
- 增強的客戶服務

提高效率
避免碰撞
節省燃油

關鍵感測
- 將「數據」轉換為「可控制智慧」

主動維護
避免事故

節約成本，提高安全性，提供卓越的服務

智慧車輛

無線路由器
- 線上娛樂

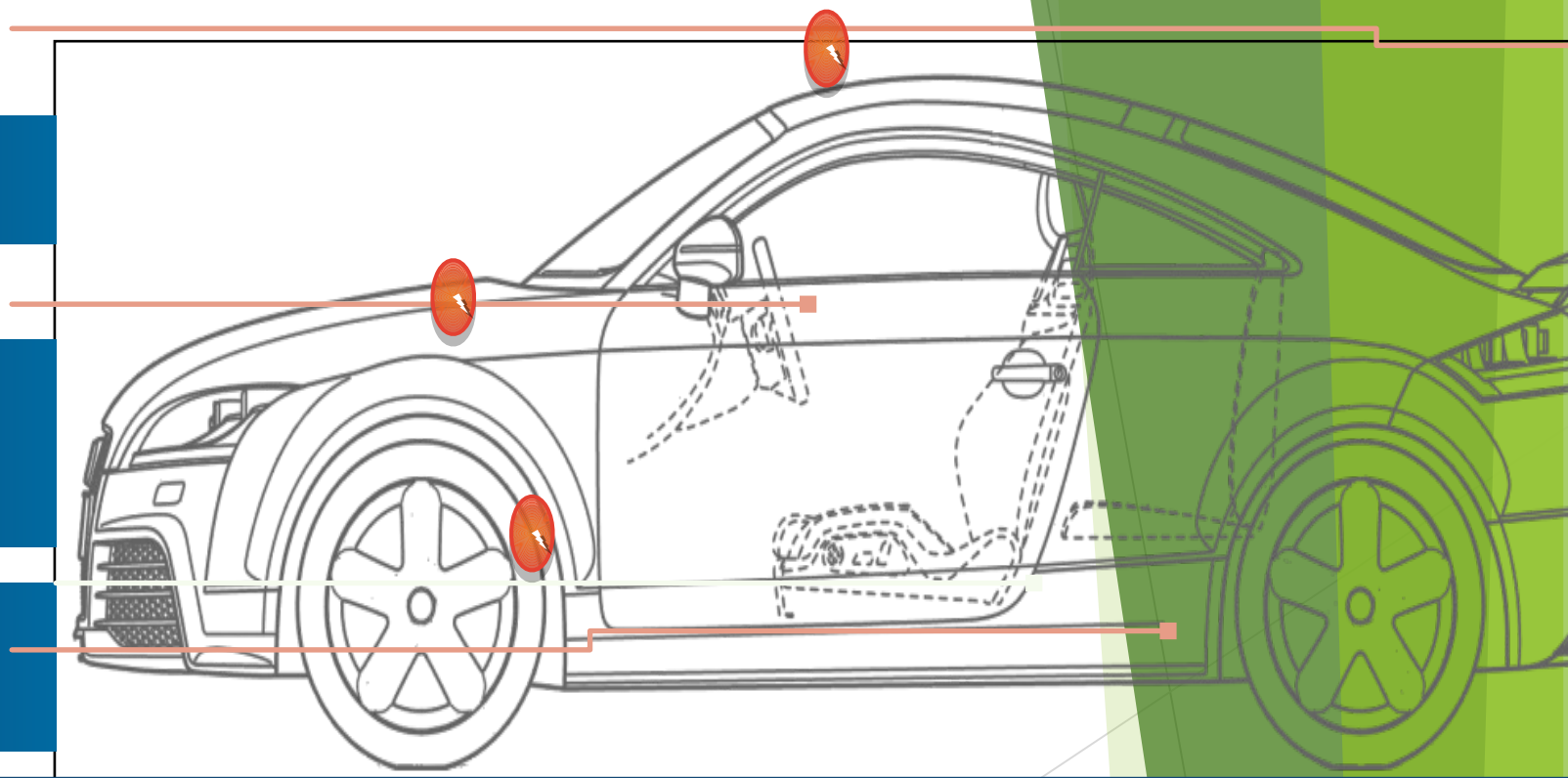
資料映射、動態重路由、安全和資安

連接感測器
- 將「數據」轉換為「可操作智慧」

啟用主動維護
避免碰撞
燃油效率

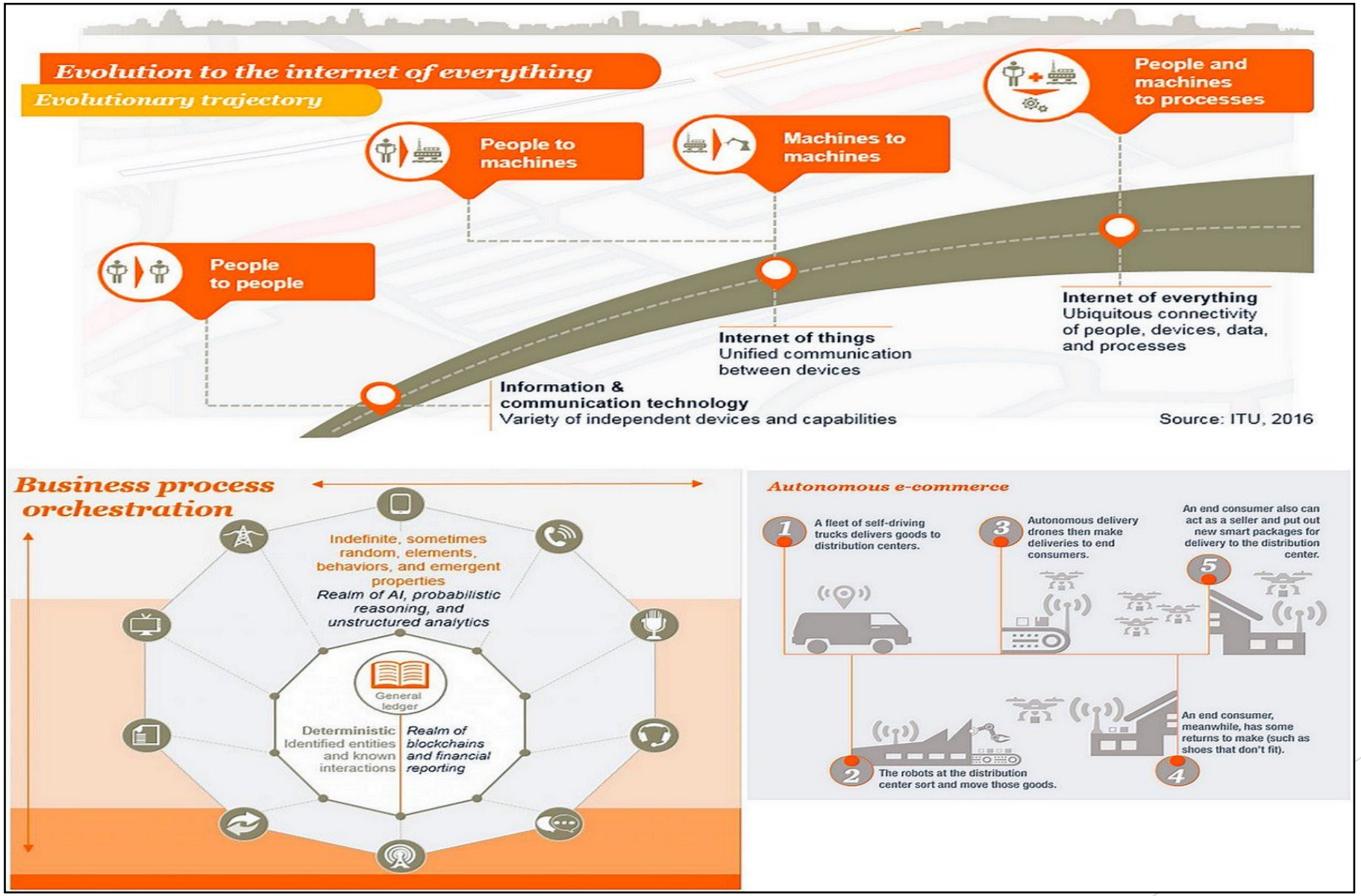
城市連接
- 減少擁堵

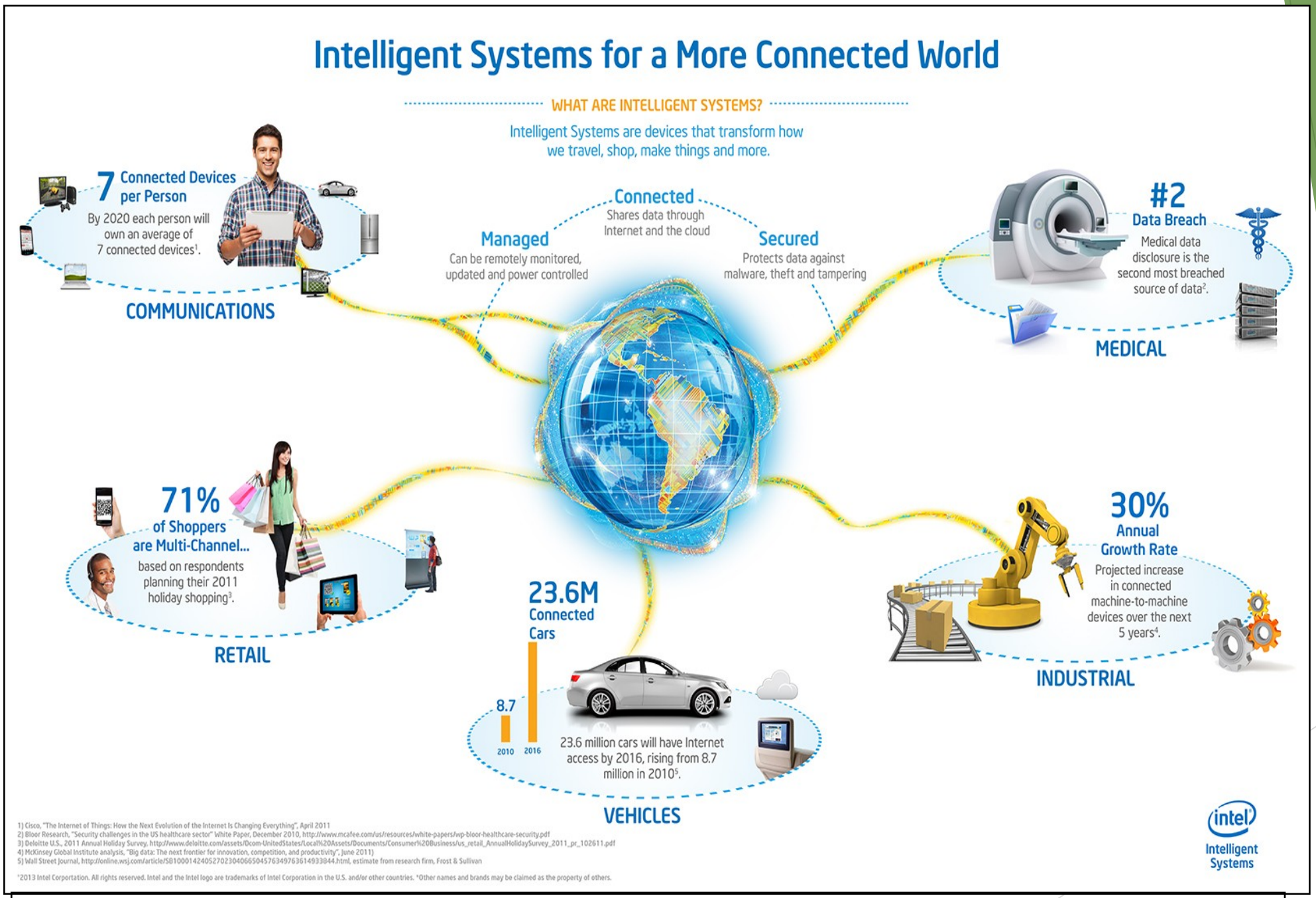
提高效率
安全（避險）



可操作的智慧，增強的舒適性，前所未有的便利性

萬物互聯　Internet of Everything





Source: http://blog.trentonsystems.com/internet-of-things-crosses-business-personal-boundaries/

工業物聯網（IIoT）

工業物聯網（Industrial Internet of Things）簡稱 **IIoT**，是應用在工業上的物聯網，是互聯的感測器、儀表以及其他設備和電腦的工業應用程式以網路相連所成的系統，其中包括了製造以及能源管理。網路連線可以進行資料蒐集、交換以及分析，有助於提昇生產力以及效率，也有其他的經濟效益 [1]。 IIoT 是由分散式控制系統（DCS）演進而成，利用雲端運算完善和優化過程控制，達到較高程度的自動化。

IoT_Video_1:
https://www.youtube.com/watch?v=wMnf3ybe_nw&feature=youtu.be

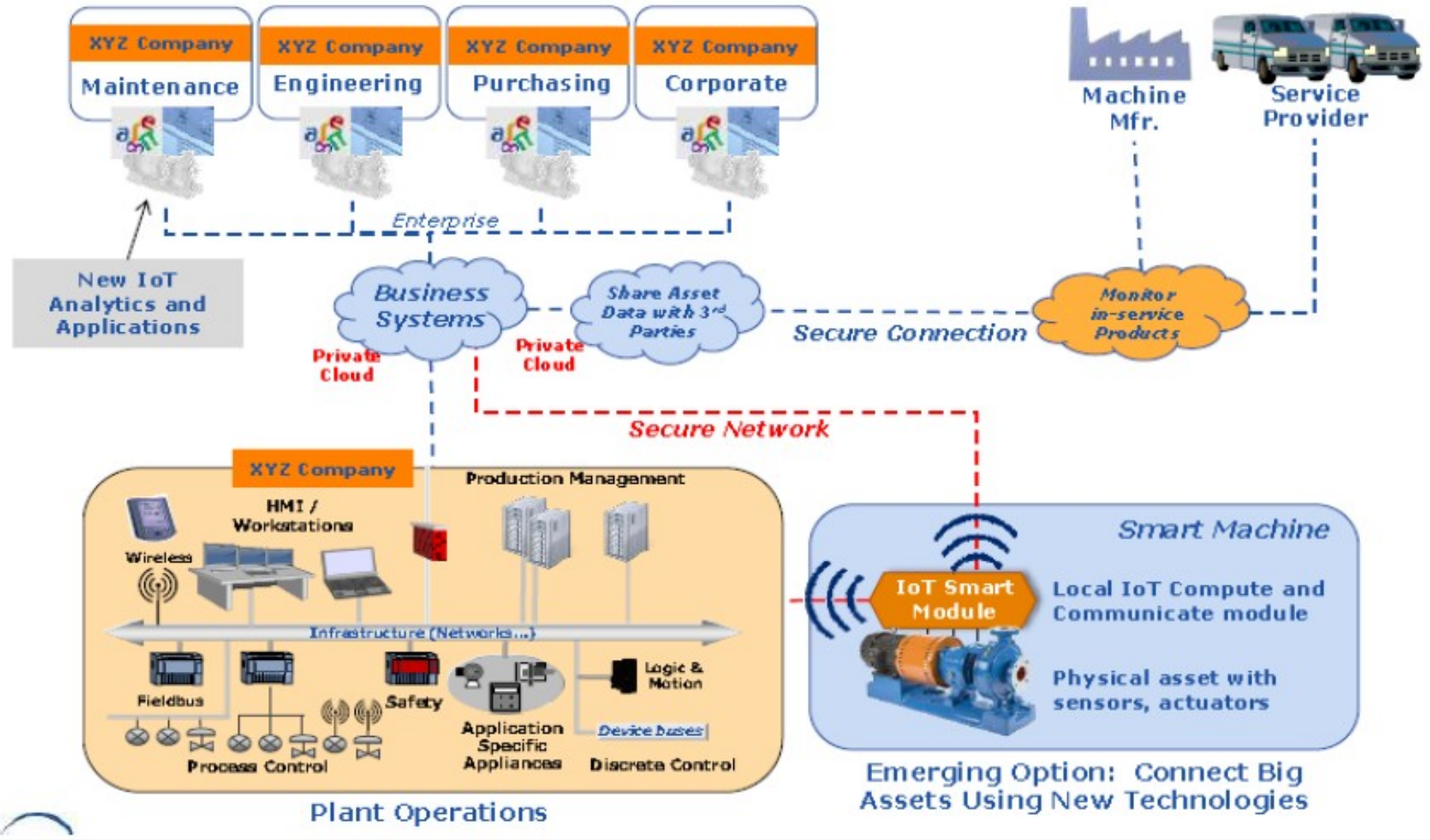
工業物聯網（IIoT）

- 工業物聯網（IIoT）系統可以用數位化技術的分層模組架構來評估 ：
- 「設備層」（ device layer ）是指實體的元件：虛實整合系統、感測器或是機器。
- 「網路層」（ network layer ）包括實體的網路總線、雲端計算以及通訊計協定，這些可以整合資料，傳遞到「服務層」。
- 「服務層」（ service layer ）是許多處理資料的應用程式，並且將資料整合成為資訊，可以顯示在操作者的儀錶板上。
- 「內容層」（Content layer）是使用者介面設備（螢幕、平板電腦、智慧眼鏡等）

IIoT的分層模組架構

內容層	使用者介面設備（螢幕、平板電腦、智能眼鏡等）
服務層	分析資料，並且轉換為資訊的應用程式及軟體
網路層	通訊協定、wifi、雲端運算
設備層	像是網宇實體系統、感測器或是機器等硬體

以物聯網架構 實現工業4.0應用情境



臺灣目前遭遇到的營運技術和物聯網資訊安全挑戰

OT 和 IIoT 與關鍵基礎設施的關係

- 攻擊型態趨於多元，駭客透過**供應鏈缺口**，進而滲透至企業或機關內部，加強內部資訊安全管理問題刻不容緩，安全防護亦需涵蓋VPN網路

調查局首度揭露國內政府委外廠商成資安破口的現況，近期至少10個公家單位與4家資訊服務供應商遇害

調查局歸納近來偵辦數起國內政府機關遭駭案件，在今日（19日）發出警示，兩重規委外資訊服務供應商遭中國駭客組織攻擊的現況，近期已有市政府、水資源局等至少10個單位，以及4家以上資訊服務供應商遇害。

文/ | 2020-08-19 發表

調查局資安工作站副主任吳庚說明中國駭客如何從臺灣政府委外的資訊服務供應商下手，侵入多

Fintech獨角獸Dave發生750萬用戶資訊外洩事件，起因竟是過去合作的服務中介廠商遭駭客入侵

Dave.com前服務供應商Waydev遭駭，間接導致Dave.com的用戶資料流入駭客

政府 | 委外 | 外包 | 供應鏈攻擊

英國政府外包商被駭，洩露10萬員工個資

Interserve公司的人事系統資料庫遭入侵，除了波及自家員工個資，其客戶包含英國國防單位、地鐵局及醫院單位，也陷

中國駭客組織對我國資訊供應鏈發動攻擊

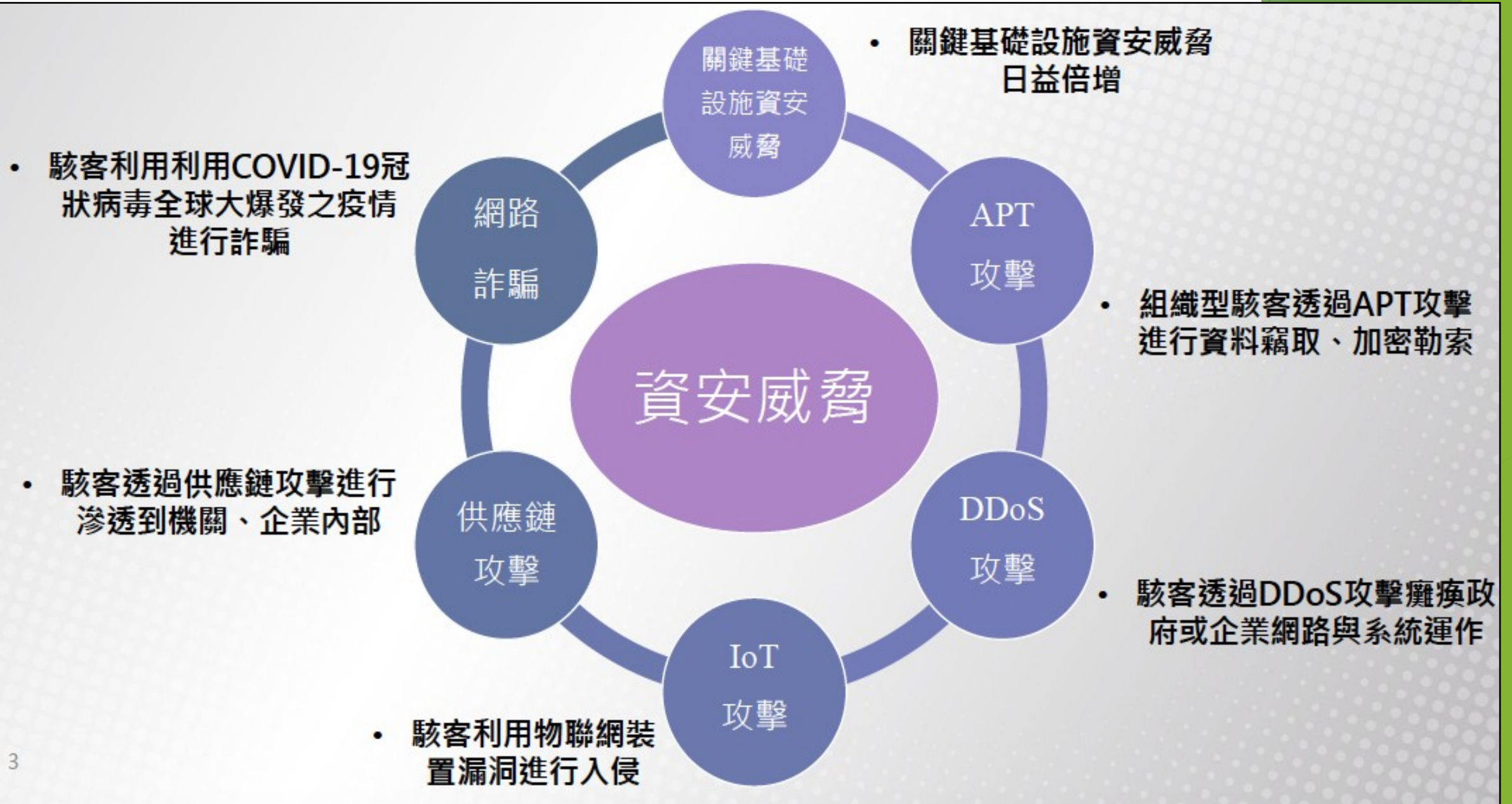
發布日期：1602-undefined-undefined 11:03:20undefined 更新日期：1602-undefined-undefined 08:54:01undefined 公共事務室

調查局近來偵辦數起我政府機關遭駭案件，調查過程中發現中國駭客組織Blacktech與Taidoor，已長期滲透國內政府機關及其資訊服務供應商，尤其是承接政府標案之資訊服務供應商，因其負責政府機關重要資訊系統之開發及維運，故成為駭客主要攻擊目標，作為跳板攻擊政府機關，試圖竊取機敏資訊及民眾個人資料，為全面清查中國駭客組織利用供應鏈在臺灣網路攻擊活動及遏止我國政府機關持續受駭，調查局成立專案小組積極偵辦，

調查發現，中國駭客組織深知政府機關為求便利，常提供遠端連線桌面、VPN登入等機制，提供委外資訊服務廠商進行遠端操作與維運，由於國內廠商大多缺乏資安意識與吝於投入資安防護設備，亦未配置資安人員，故形成資安破

法務部調查局

OT 和 IIoT 與關鍵基礎設施的關係



- 關鍵基礎設施資安威脅日益倍增
- 駭客利用利用COVID-19冠狀病毒全球大爆發之疫情進行詐騙
- 組織型駭客透過APT攻擊進行資料竊取、加密勒索
- 駭客透過供應鏈攻擊進行滲透到機關、企業內部
- 駭客透過DDoS攻擊癱瘓政府或企業網路與系統運作
- 駭客利用物聯網裝置漏洞進行入侵

國內外層出不窮的 OT 與 IIoT 攻擊

- 在萬物聯網、大數據與 AI 等技術的潮流下，智慧製造、智慧醫療已成臺灣政府積極推動的政策，以促進為國內產業智慧化轉型升級，升級部份主要包含製造業、醫療業、關鍵基礎設施、精密機械等產業。
-
- 操作技術 (OT) 則是在這波產業升級下的關鍵核心技術，指針對如製造業、醫療業、關鍵基礎設施、精密機械的實體設備進行監測、控制及操作的軟硬體，不論是智慧製造業抑或公共基礎設施做為整體流程控制用，這樣的環境通常都會有一套系統監控與數據蒐集的工業控制系統 (ICS) 包含在內。
-
- 但這些已開始發生變化！ 連網環境日益普及，形成了物聯網及工業物聯網，而使得兩個世界的系統出現了彼此連接的可能性。工業控制系統從單機走向互聯， 從封閉走向開放。然而，這樣的開放卻也帶來過去所不曾出現的安全性弱點，和 IT 系統一樣， OT 受到惡意軟體的嚴重威脅。

國內外層出不窮的 OT 與 IIoT 攻擊

- 在 2018 年台積電爆發機臺中毒事件後，而在 2019 年 3 月，全球最大鋁業之一的挪威公司 Norsk Hydro ，發生 IT 網路遭到勒索軟體 LockerGoga 攻擊，波及製造環境的事件，導致該公司在歐美地區部分自動化生產線關閉，而根據該公司第一季財報顯示，此事件帶來的損失至少超過 3500 萬美元；
-
- 而在 2019 年 1 月，法國工程諮詢公司 Altran Technologies ，也遭受 LockerGoga 攻擊，同年的 6 月、 7 月，飛機零組件供應商 Asco 公司，以及約翰尼斯堡的 City Power 公司，也都遭勒索軟體感染。因此據 Verizon 發佈的最新資料洩露調查報告顯示，僅就製造業而言，過去一年中就有 200 多次間諜型安全攻擊，以及 700 多次經濟型攻擊。
-
- 證據顯示：企業組織面臨的惡意軟體、資安威脅及釣魚郵件攻擊數量迅速攀升，工控環境仍面臨真實發生的資安威脅，其中勒索軟體來勢洶洶！

惡意程式攻擊列表

TABLE 2-2 Attack Replication Vectors

Vector	Description
IP scan and attack	Infected system scans random or local range of IP addresses and targets any of several vulnerabilities known to hackers or left over from previous exploits such as Code Red, Back Orifice, or PoizonBox
Web browsing	If the infected system has write access to any Web pages, it makes all Web content files (.html, .asp, .cgi, and others) infectious, so that users who browse to those pages become infected
Virus	Each infected machine infects certain common executable or script files on all computers to which it can write with virus code that can cause infection
Shares	Using vulnerabilities in file systems and the way many organizations configure them, it copies the viral component to all locations it can reach
Mass mail	By sending e-mail infections to addresses found in the infected system's address book, copies of the infection are sent to many users whose mail-reading programs automatically run the program and infect other systems
Simple Network Management Protocol (SNMP)	In early 2002, the SNMP vulnerabilities known to many in the IT industry were brought to the attention of the multi-vector attack community. SNMP buffer overflow and weak community string attacks are expected by the end of 2002

攻擊描述 ：IP Spoofing

- IP Spoofing 主要用將來源的 IP address 假造修改
-

為什麼駭客要修改來源的 IP Address 呢？ 有幾個主要原因

- 讓受害者誤以為溝通訊息的對象
- 讓受害者更難追查攻擊的來源
- 透過這個方式發動 DDOS 攻擊

透過假造大量的 IP address 傳送 TCP 3-way handshake 訊號
讓受害者電腦忙於 3-way handshake 造成電腦癱瘓

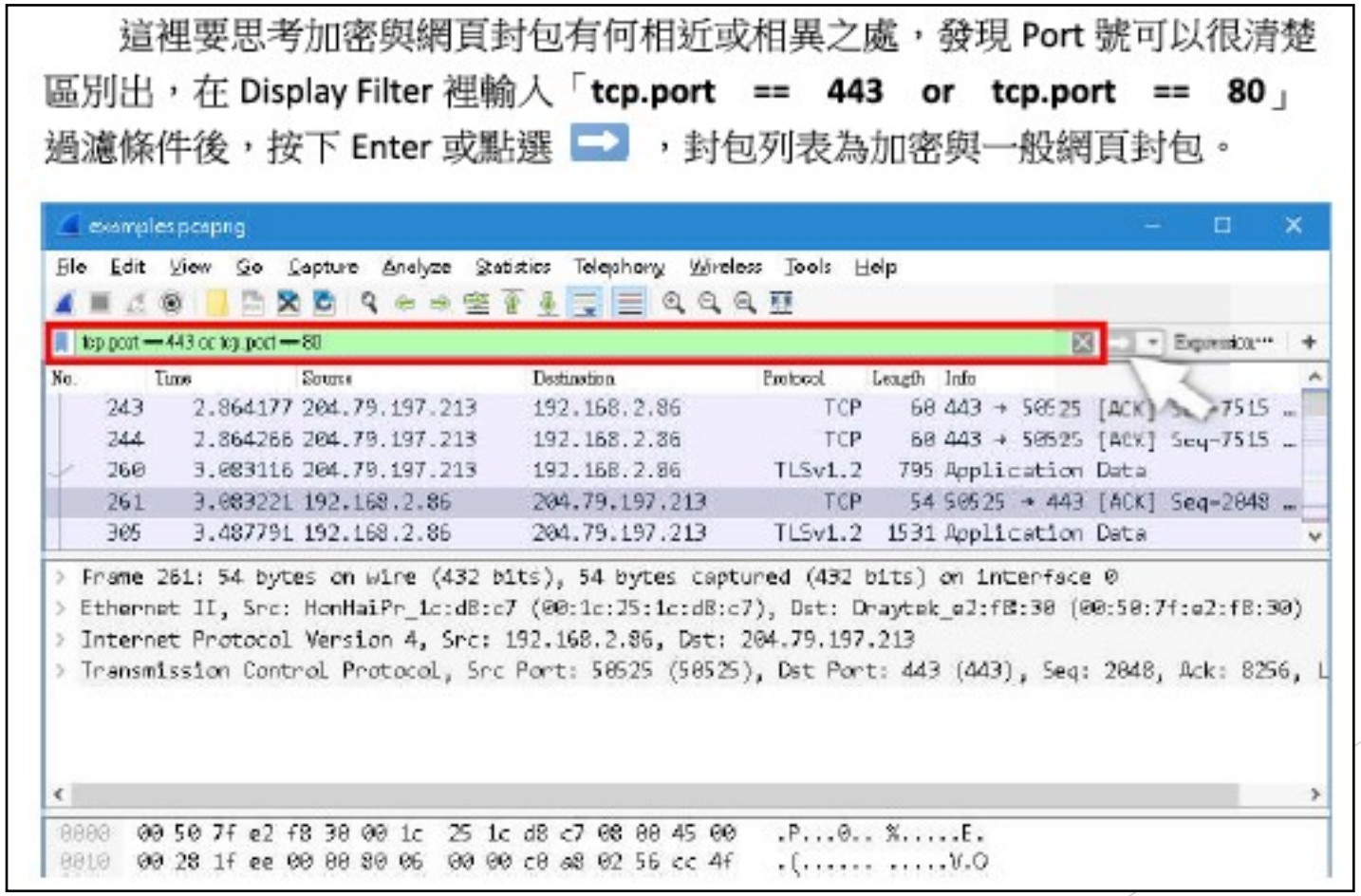
IP Spoofing 測試範例（請同學們在 https://nmap.org/download.html)

Nmap 指令可以透過 nmap 假造來源 ip address (192.168.1.4)
對於受害者電腦（192.168.1.6）做掃描

```
nmap -e eth0 -S  192.168.1.4    192.168.1.6
```

攻擊描述 ：Sniffing

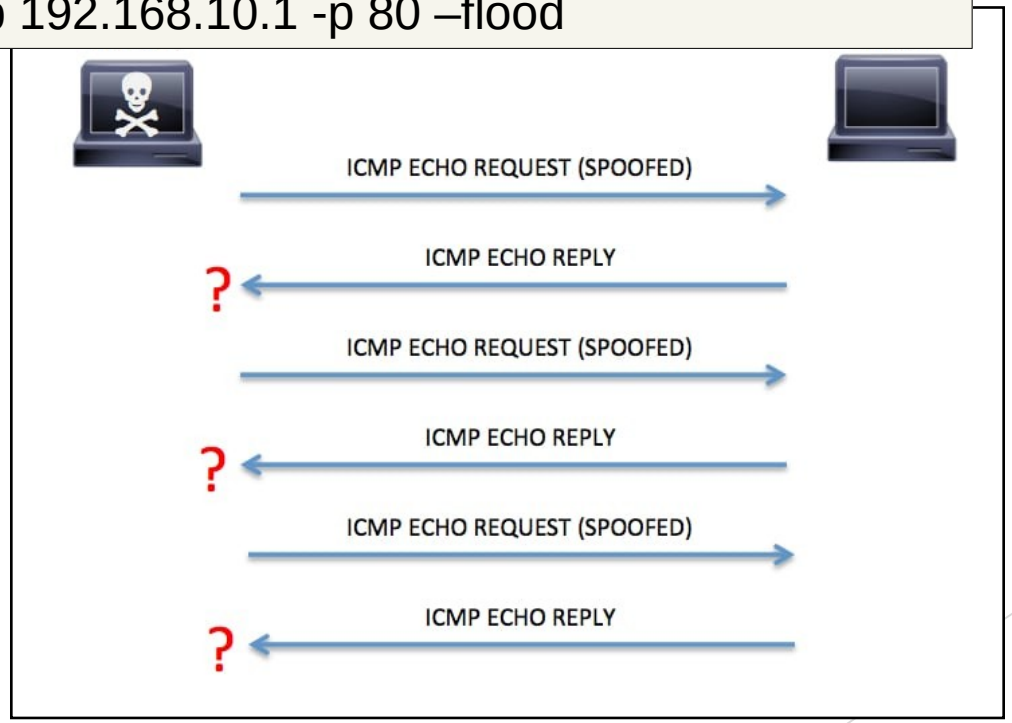
- 透過網路封包的擷取，獲得相關隱私資訊
- 常使用的工具為 WireShark
- 請同學們下載 Wireshark ，並做下列練習



攻擊描述 ：ICMP Flooding

為大家介紹一個駭客級的測試工具「 hping 」，同學們可自行下載
原始網站： http://www.hping.org/
範例： 透過大量發送 ICMP 給受害者電腦，讓受害者電腦過於忙碌造成電腦癱瘓

```
hping www.abc.net.tw -1 -i u100000 -a 100.100.100.100
hping3 –icmp 192.168.10.1 -p 80 –flood
```



Q & A