# 對應 IEC 62443 工控資安之解決方案與操作實務

吳建東/捷而思

# 製造業數位轉型

- 智慧製造
  - 廠內：生產線的問題、產線流程不佳、3D圖像AI辨識、品質不佳之瑕疵判定、處理加工AI預警
  - 供應鏈：斷料、來料檢測 (智慧檢測平台) 、供需預測

- 資安的問題
  - 辦公室 IT
  - 工廠 OT

# 製造業的資安要求

## 1.安全治理和合規性

- 供應鏈廠商網路安全控制評估調查表、修補已發現的漏洞、維持有效的安全管理計畫。

## 2.工作人員安全

- 禁止未通過核可的任何供應鏈廠商進行系統和資料的存取，且員工須每年度完成資訊安全培訓。

## 3.資產管理

- 供應商必須僅允許供應鏈廠商代表從已經過批准的設備，存取系統資料。

## 4.掌握資訊，處理和保護

- 實施控制措施，以確保只有那些需要的供應鏈廠商代表才能存取系統資料。
- 供應鏈廠商必須使用強大的安全演算法，確保在閒置和傳輸中對資料進行加密保護。

## 5.變更管理

- 供應鏈廠商須為新資訊系統升級和版本建立接受和確認過程，以確保在供應鏈過程中不會引入漏洞，並且必須在開發過程中和發布之前對這些過程進行適當的測試。

# 製造業的資安要求

## 6. 身份驗證和存取管理

- 供應鏈廠商必須提供身份驗證和存取控制，以保護系統資料，包括用於防止未經授權存取系統資料的身份驗證方法。
- 供應鏈廠商必須確保對處理資料的供應鏈廠商系統的管理或遠端存取符合行業最佳實施，例如多因素身份驗證和虛擬專用網路。

## 7. 實體和環境安全

- 在安全存取控制的地區，被保護在實體安全控制措施，以防止未經授權的實體存取。

## 8. 安全操作

- 須定期稽核供應鏈廠商網路和系統，以確保符合安全配置要求，必須定期掃描供應鏈廠商的整個網路，系統和應用程式中的漏洞。

## 9. 安全事件回應

- 供應鏈廠商發現任何資料洩露或涉及或可能影響系統和資料的惡意入侵，供應鏈廠商必須立即通知。

## 10.業務連續性/災難復原

- 須實施並維護書面的業務連續性和災難復原計畫。

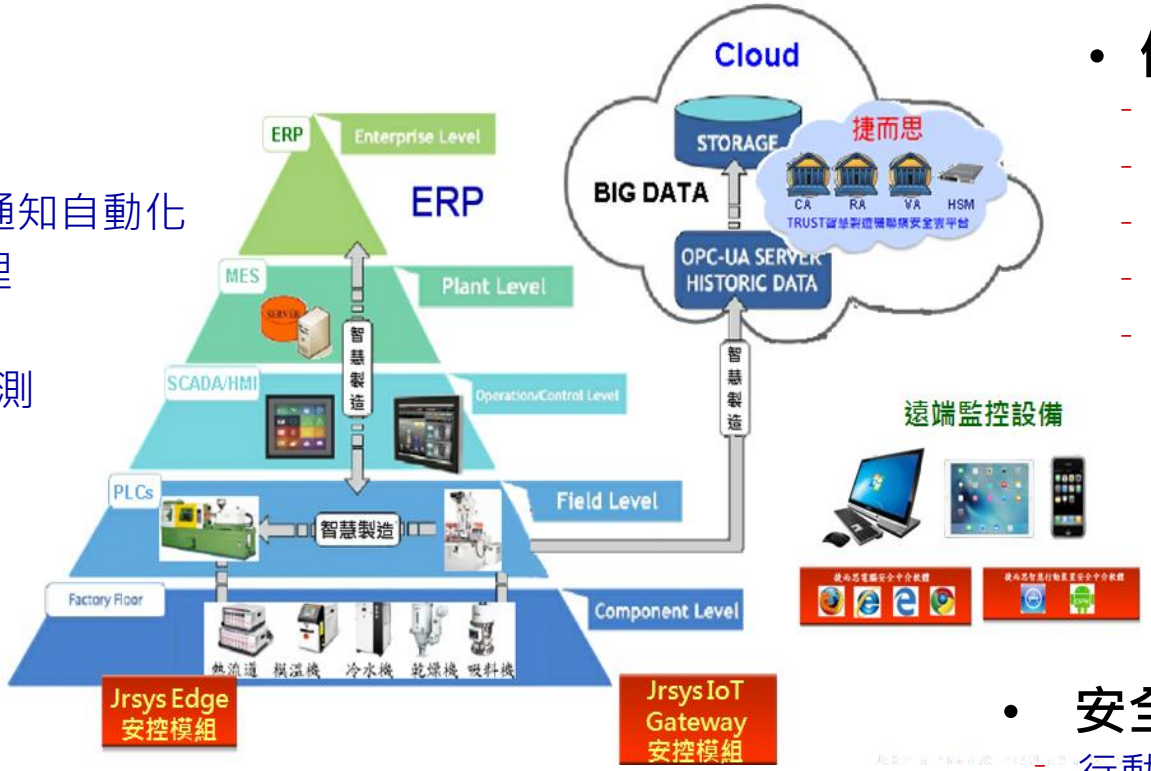
# 企業資安改善計劃

1. 分析公司現況及資安風險，列出必須改善的項目
2. 建立公司資安政策、組織 (IT：ISO 27001, OT ： IEC 62443-2-1)
3. 根據資安風險列舉改善措施
4. 規劃 IT/OT 資安解決方案
5. 分期逐步達成資安防禦之基礎建設

# 智慧生產製造資訊整合資安

## 資安現況診斷、顧問輔導及資安解決方案導入

- **產線資安**
  - 報工、排程、物料通知自動化
  - 供應商員工異動管理
  - 機台生產資料
  - AoI人工智慧光學檢測
  - 設備健康度

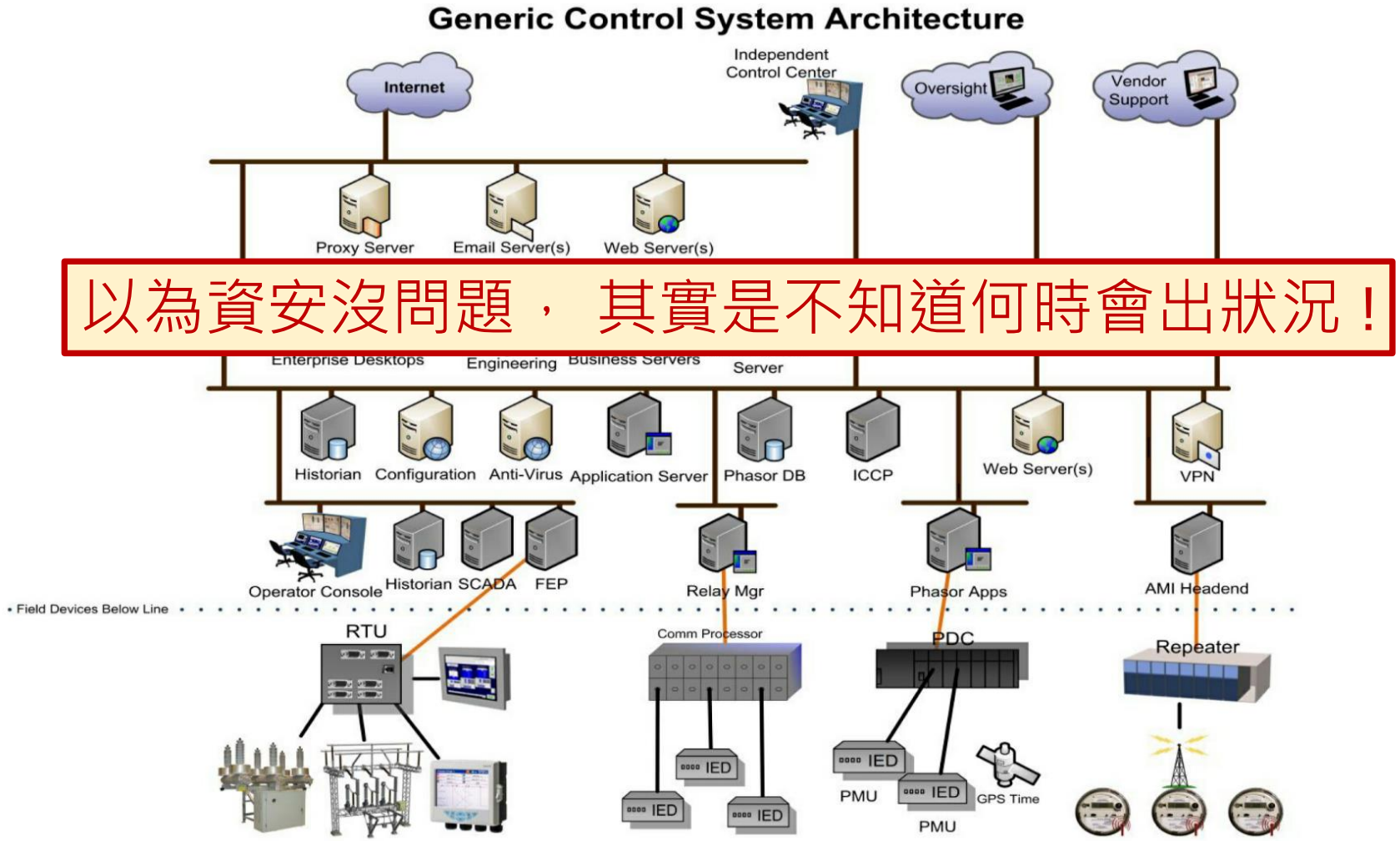



- **供應鏈資安**
  - 供應鏈管理
  - 協力廠的PQC
  - 往來文件管理
  - HMI及遠端登入控管
  - 供應商員工異動管理

- **安全的身份認證**
  - 行動認證
  - 遠端登入控管
  - 員工、供應商權限控管

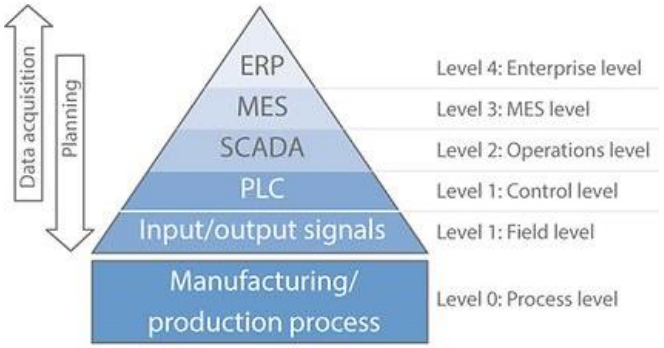
廠內：生產線的問題、產線流程不佳、3D圖像AI辨識、品質不佳之瑕疵判定、處理加工AI預警
供應鏈：斷料、來料檢測 (智慧檢測平台) 、供需預測

# 公司導入產業資安前之現況

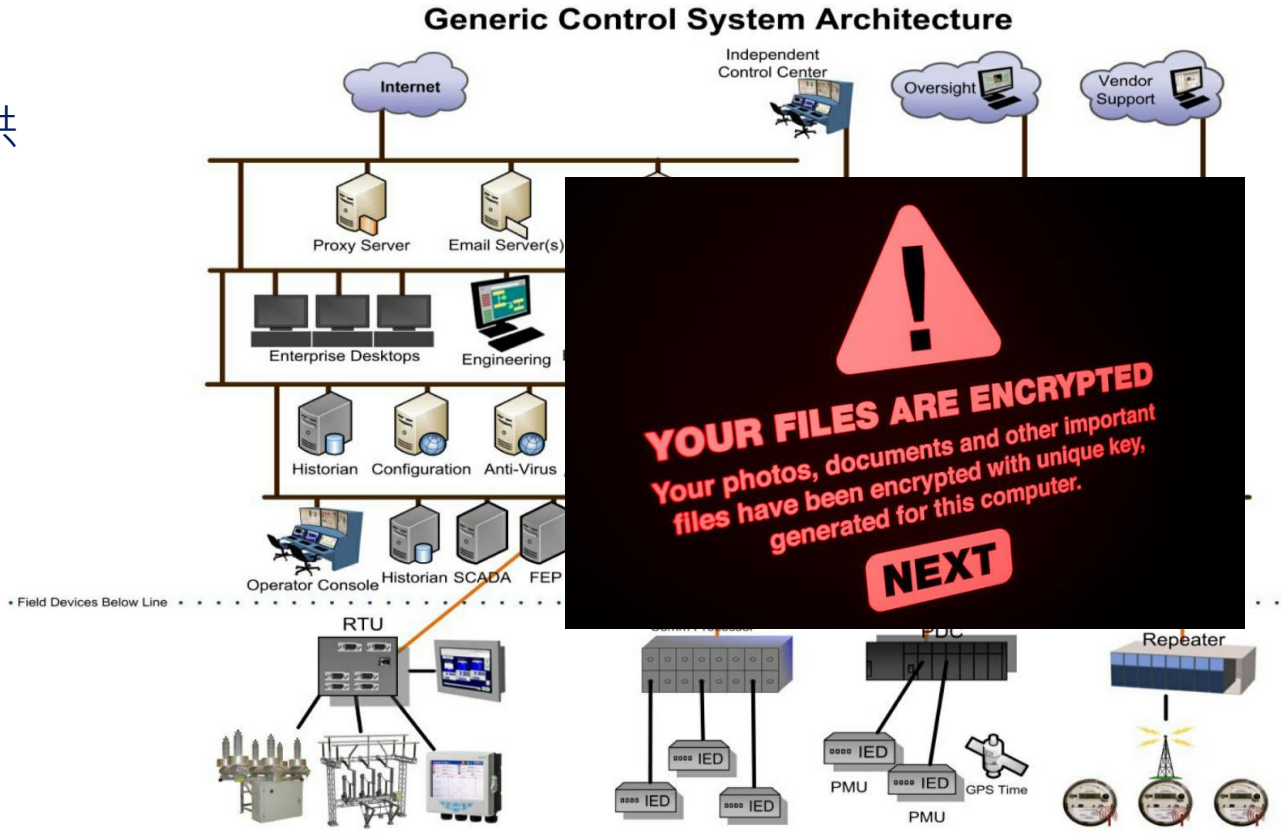


# 公司導入產業資安前之現況

- 我們有防火牆、防毒軟體
- 都在內網不對外，很安全
- 都是一、二十年的老員工及供應商，不會有問題
- 資料沒被偷走，都還在!




ANSI/ISA 95



# 可能的風險

風險一：國外及因疫情居家上班員工使用RDP服務，目前之資安防禦層級不足，易受攻擊

風險二：未進行資安漏洞掃描或系統快篩，不知是否有風險

風險三：釣魚郵件社交攻擊，匯款至錯誤帳號

風險四：端點安全防護不足，易中毒及被入侵

風險五：備份不完整，亦不知系統還原是否能成功

風險六：帳號登入、網路行為，沒有日誌紀錄保存及分析機制

風險七：沒有建立 資安監控中心、AI快篩等資安監控機制

風險八：機台沒有設密碼或密碼都一樣

風險九：機台參數、資料保護與備援

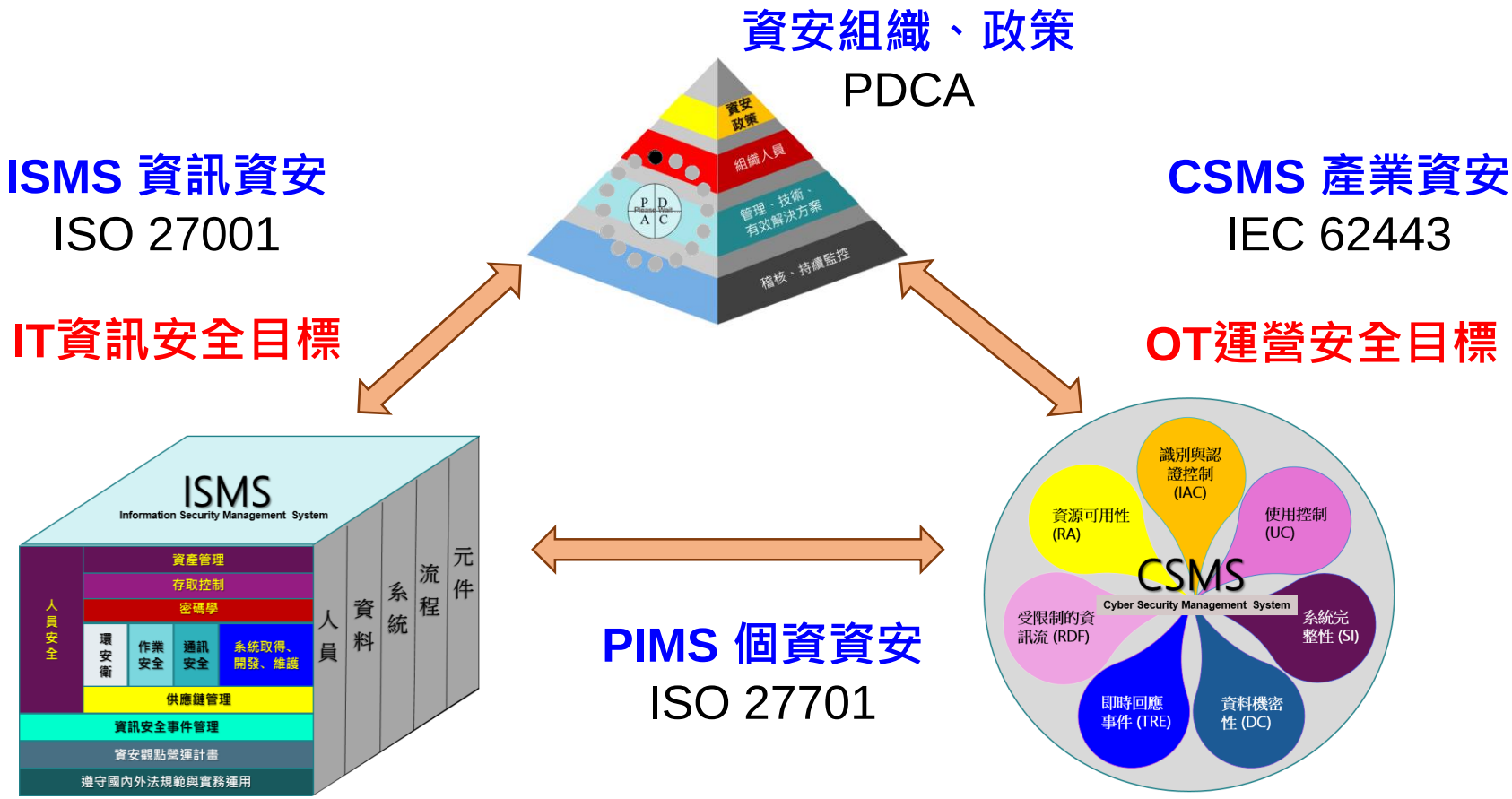
風險十：機台AIoT應用之資安保護

# 安全等級 Security Level Capability

- 七項基本要求
  - FR1 –識別和認證控制
  - FR2 –使用控制
  - FR3 –系統完整性
  - FR4 –資訊保密
  - FR5 –限制資料流
  - FR6 –及時回應事件
  - FR7 –資源可用性

# 企業營運管理資安全貌

企業應同時對資訊 IT (Information Technology) 、整體產業自動化運營 OT(Operational Technology) 及相關的個資保護之資安防護進行整體性的規劃。



# IT 資安：ISO 27001 控制目標及措施

- 行動裝置及遠距工作
- 密碼式控制措施之監管
- 存取控制
- 機密性或保密協議
- 保護應用服務交易
- 供應鏈資訊安全
- 智慧財產權及安全文件
- 個人可識別資訊之隱私及保護

# OT 資安：IEC 62443-2-1控制目標及措施

- 制定遠端登入和連接政策
- 對所有遠程用戶使用適當等級的身份驗證方式
- 用戶身份驗證與授權
- 暫停或移除不需要的賬戶
- 更改預設密碼
- 系統管理及設定應用程式必須使用強認證方法
- 對存取IACS 設備建立適當的邏輯和物理權限管理
- 用角色來控制對資訊或系統的存取
- 對關鍵的 IACS 採用多種授權方法

# 工業自動化資安 IEC 62443

## 一般(General)

工業自動化資安合規相關之術語、說明、矩陣、資安生命週期管理及應用實例

## 政策與程序(Policy and Procedure)

- 62443-2-1 資產擁有者之資安計劃要求
- 62443-2-2 工業自動化之資安成熟等級
- 62443-2-3 工業自動化之修補更新管理
- 62443-2-4 IACS供應商之資安計劃要求
- 62443-2-5 資產擁有者之資安執行指引

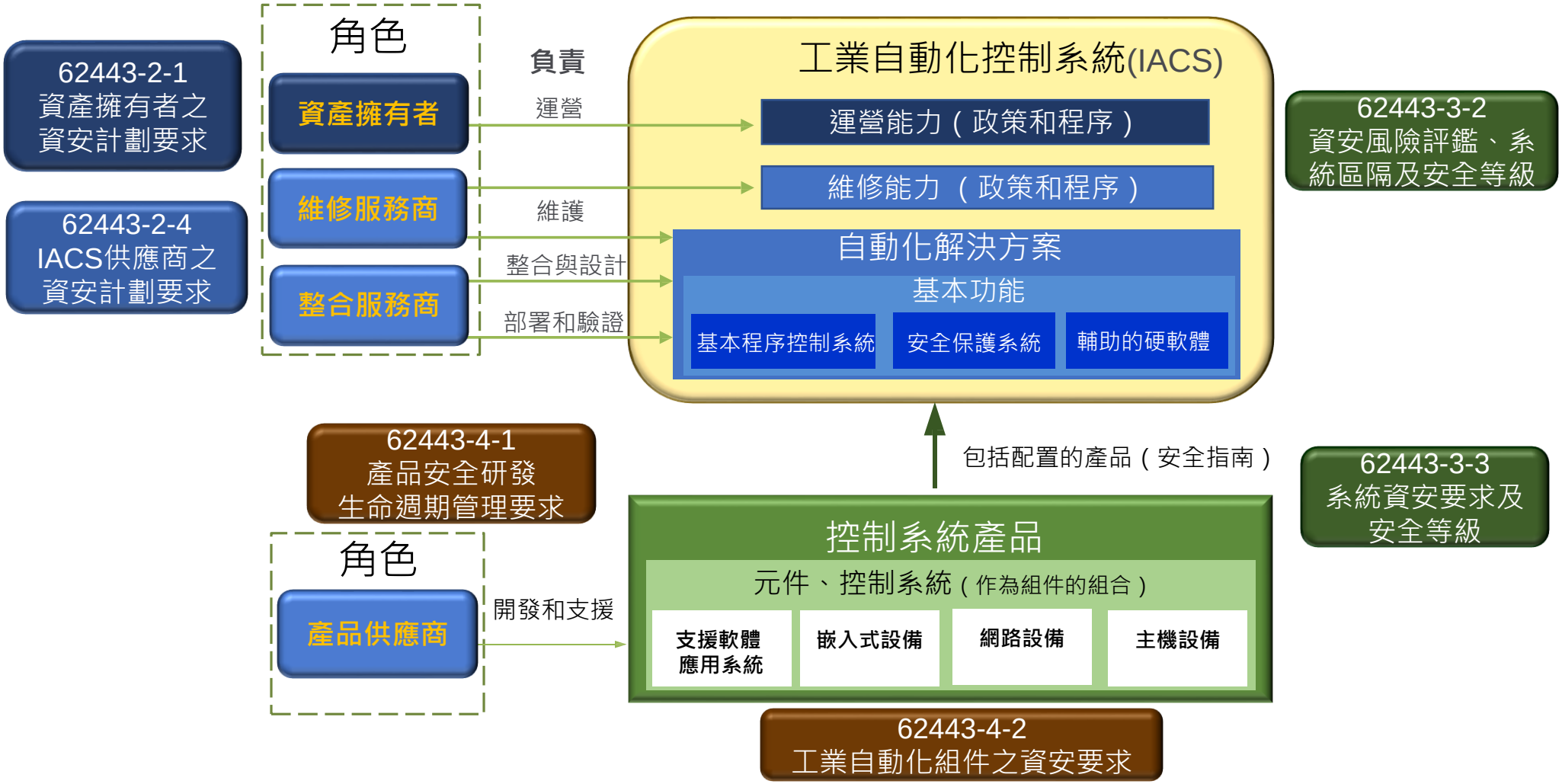
## 系統(System)

- 62443-3-1 IACS資安技術
- 62443-3-2 資安風險評鑑、系統區隔及安全等級
- 62443-3-3 系統資安要求及安全等級

## 設備組件(Component)

- 62443-4-1 產品安全研發生命週期管理要求
- 62443-4-2 工業自動化組件之資安要求

# IEC 62443 工控資安



# 針對風險列舉改善措施

風險一：國外及居家上班RDP使用雙因子認證及授權

風險二：進行資安漏洞掃描系統快篩找出風險

風險三：建置防APT攻擊郵件系統

風險四：建置端點防護系統

風險五：建立安全的備份機制，並定期演練

風險六：完整的日誌紀錄保存及分析機制

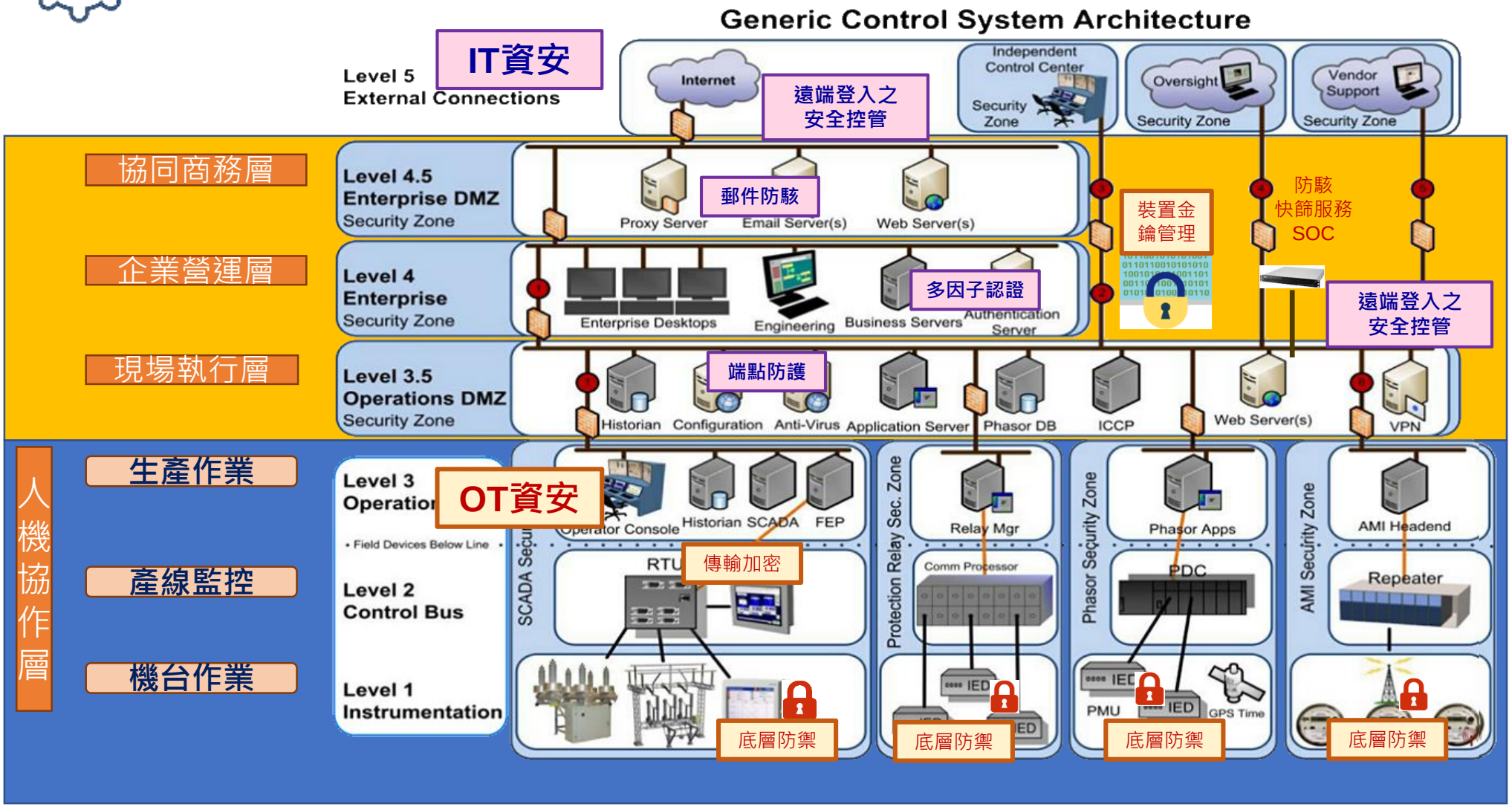
風險七：資安監控中心委外

風險八：機台使用工控PAM，採拋棄式密碼方式管理

風險九：完善機台參數、資料保護與備援之機制

風險十：機台AIoT應用之資安保護

# 公司導入產業資安後之規劃



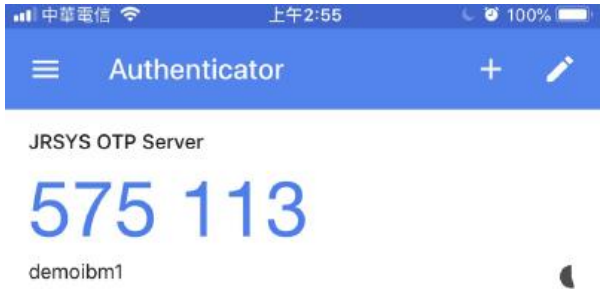
# 供應鏈資安

- VPN/RDP 只有帳號/密碼是危險的
- 公司不易管控所有員工及供應商人員的資安素質
- 公司信任合作的忠實伙伴，但可能因其新進的員工或被駭客入侵而攻擊我們，造成重大損失
- 公司的員工離職刪除 AD帳號就進不來了，但供應商員工離職，帳密移交給交接人員，但公司不會知道也不會變更，供應商離職員工也可能再非法登入
- 台灣公司長期被駭客入侵，造成貨款匯至駭客戶頭，傷害公司及上下游關係的事件曾出不窮，損失千萬至億元

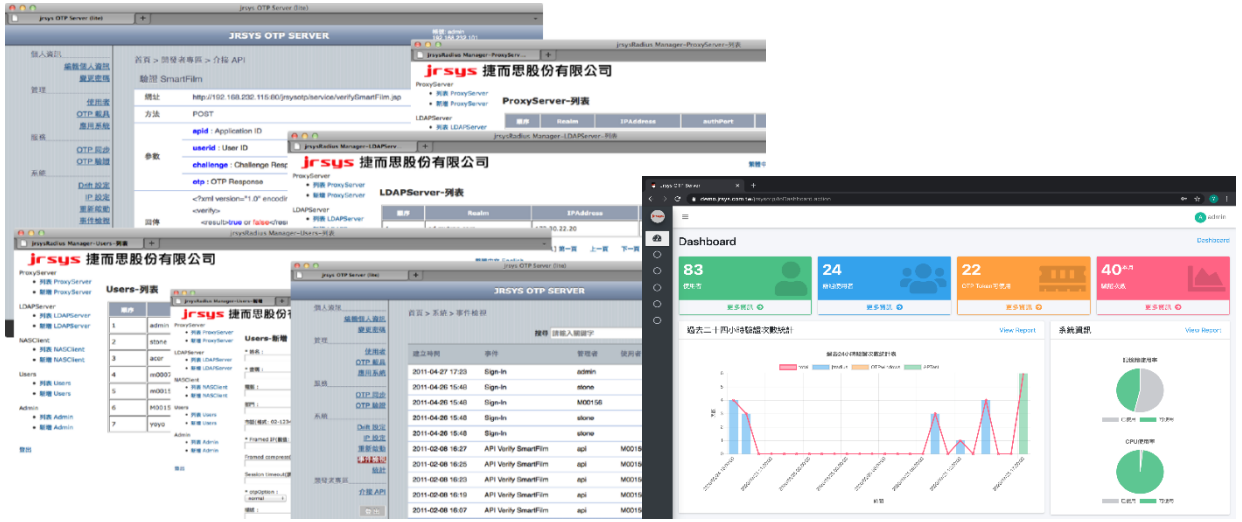
# 解決遠距作業、外包商資安問題

- 遠距上班 VPN, RDP遠端桌面及網站登入之強化
- 提供 Google、AMAZON 等級的企業OTP 驗證服務
- 不必記密碼，密碼 30秒自動變更
- 內部系統登入帳號授權管控
- 協防許多A級政府機關

**手機一次性密碼身份認證**




密碼每60秒自動更新



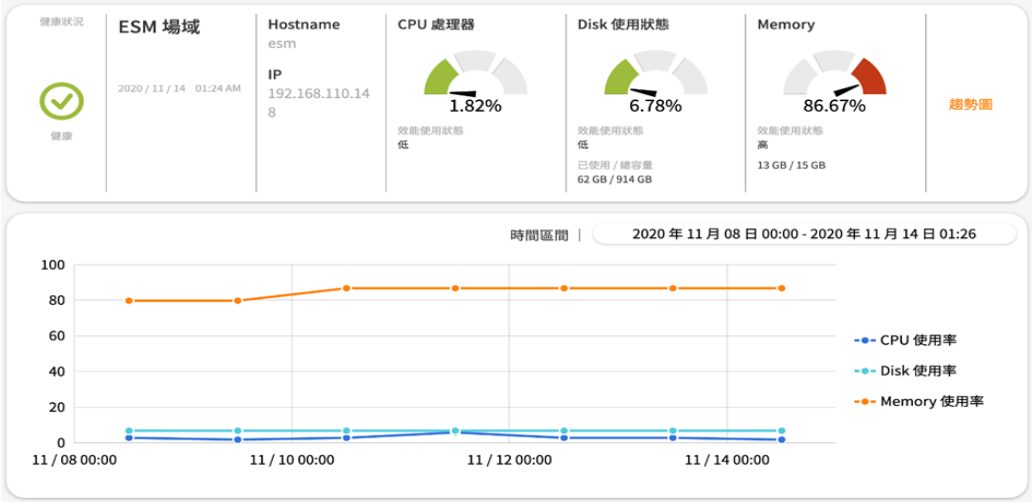
# 資安防駭，精準快篩

**SECURITY**

## 事件導向資安精準快篩與追蹤監控服務

**為台灣量身打造**，針對勒索軟體、DDoS 提供資安快篩服務，讓企業在資安事件接踵而來的高危險環境，免於攻擊威脅。

非現有SOC相關服務，為**新型態資安共創服務的體驗方案**




### 事件導向的快篩

對於最新情資通報或公佈之高風險漏洞攻擊事件，即時製作相對應的快篩工具

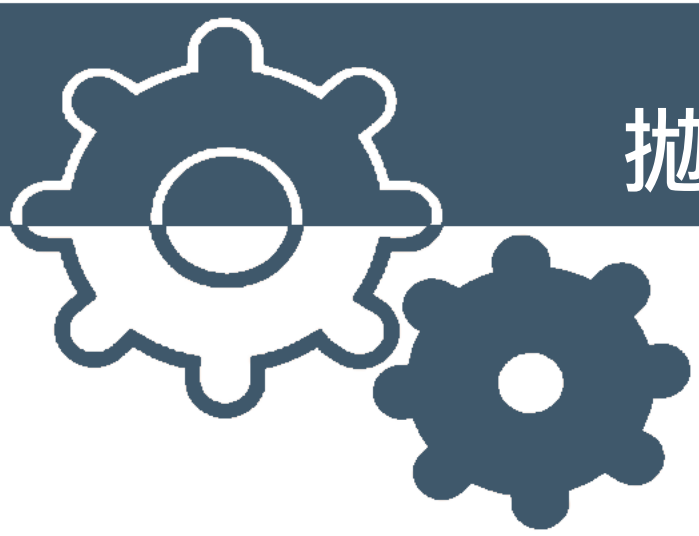
### 有效監控評估

對於現有CIIP ，增加監控可視性輔助，即時掌握威脅動態，降低因攻擊感染被癱瘓的風險

### 案件處理追蹤服務

針對已經遭到感染的設備持續追蹤處理進度，直到威脅消失

ISMS ISO 27001 ▒ PIMS ISO 27701 ▒ CSMS IEC 62443



# 拋棄式機台密碼自動化管理系統

控管千台電腦與近萬個管理者帳號

# 國內外獲獎實績

- The Asset Triple A Digital Awards, 2020
  - Digital Project Awards – Best Cybersecurity Project
- Global Retail Banking Innovation Awards, 2019
  - The Digital Bander - Outstanding IT Transformation
- Global Business Outlook：
  - Best Risk Governance and Intellectual Anti-hacking Initiative



# 多主機密碼自動化管理系統 – 痛點

- 當少數的管理者必須管理幾十台至幾百台機器時.....
- 每個機台的密碼都一樣？
- 不一樣，但紀錄在紙上？貼在機器旁？
- 多久換一次密碼？
- 多少人知道這些密碼？離職員工？
- 能否確認誰登入過？
- 是否一用過機台就立即更換密碼？

# 拋棄式機台密碼自動化管理系統

## 四大應用範圍：

### 主機管理

- 主機納管
- 資源存取控管


### 帳號盤點

- 防止幽靈帳號未授權存取
- 帳號管理，權責區分

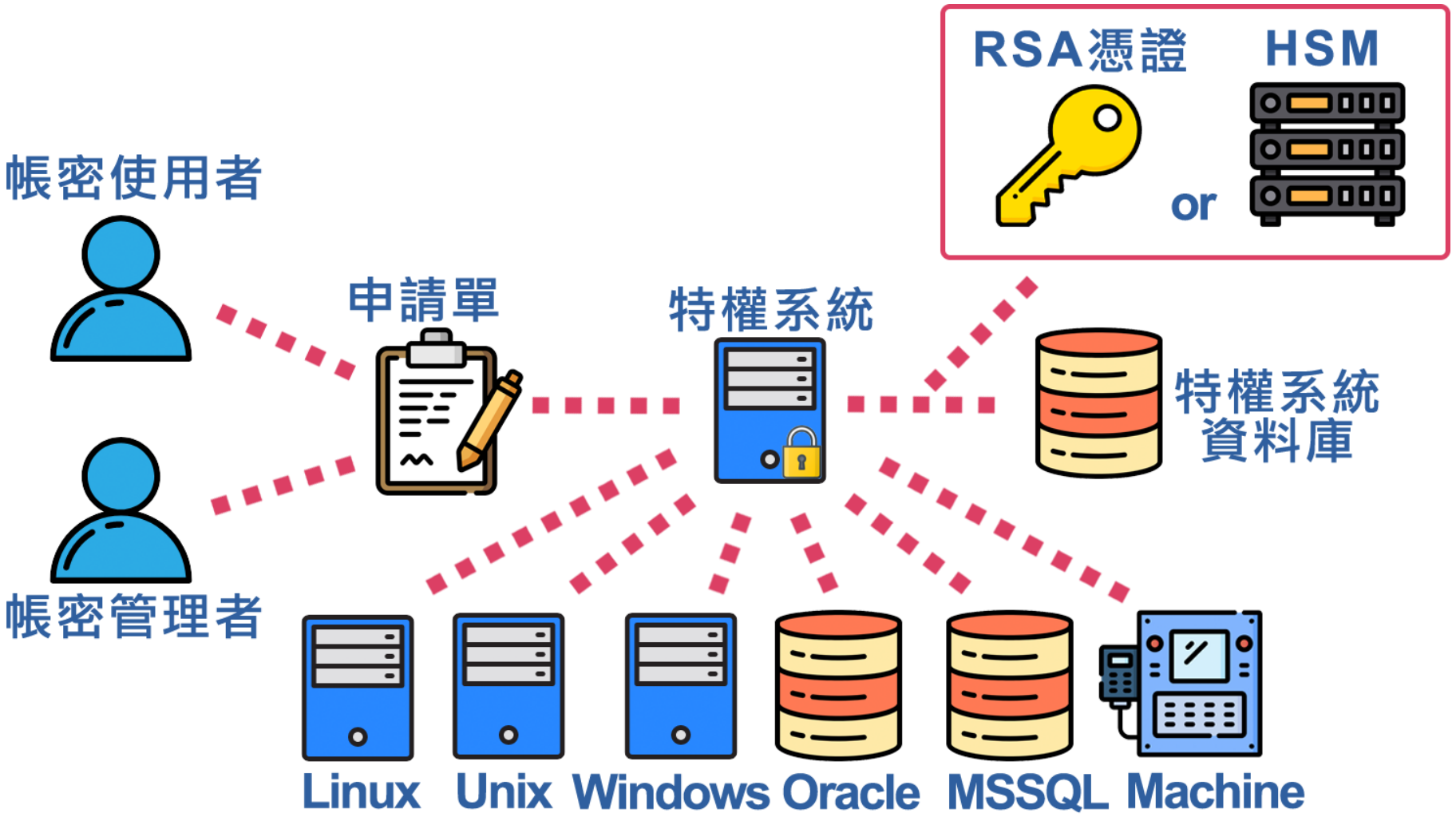

### 密碼管理

- 密碼簽出簽入自動
- 提升行政效率，降低人為疏失
- 無主機密碼登錄，減少主機密碼外洩可能

### 集中控管

- 集中式存取控管
- 行為稽核紀錄
- 跨平台服務
- 降低管理成本

# 拋棄式密碼自動化管理系統架構



# 應用範圍-帳號盤點

**01** 設定列管主機資訊

**02** 設定列管主機所有帳號

**03** 產生列管主機帳號盤點清單


- 抓出幽靈帳號，降低未授權存取資安事件
- 主機帳號列管，解決多人共用帳號權責不清問題

# 生產配方

當競爭者買跟我一樣的機台，也偷到我的配方參數時，

那麼生產出來的產品就會是一樣的！

**怎麼辦？怎麼辦？**

**確保機台配方參數不外洩的解決方案**

# 自動化機台如何防駭？

- 資料保密

  生產資料個機台加密傳輸，並確保資料完整性別

- 杜絕駭客攻擊

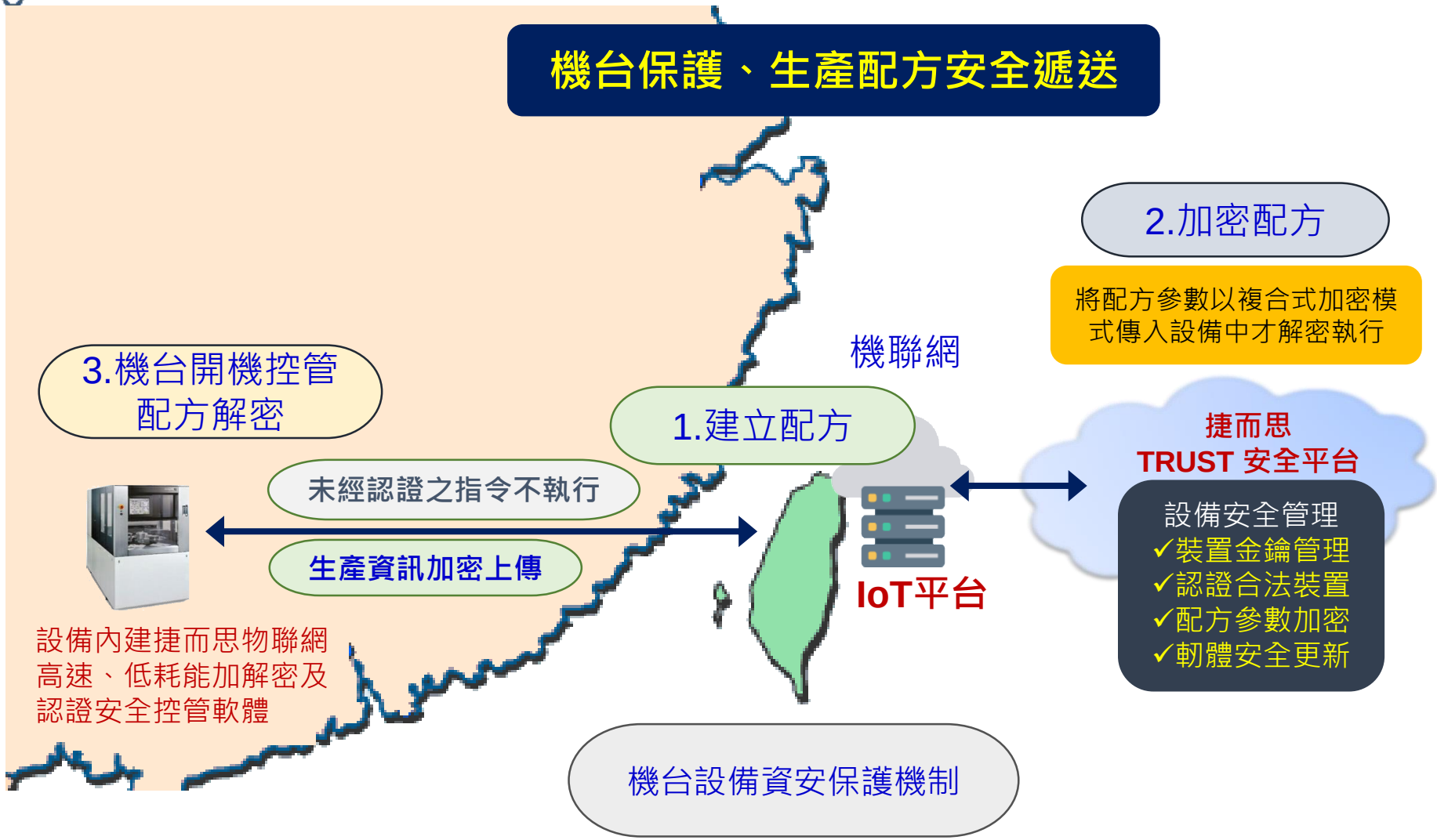
  驗證機台作動指令的正確性後才執行

- 管理數十台至百台機台使用不同密碼

  全自動化用過即換，拋棄式密碼管理系統

**本公司採用美國國家標準局認證之國防等級安全硬體加密器來產製、驗證及保護密鑰不被竊取**

# 機台設備資安智財權保護藍圖

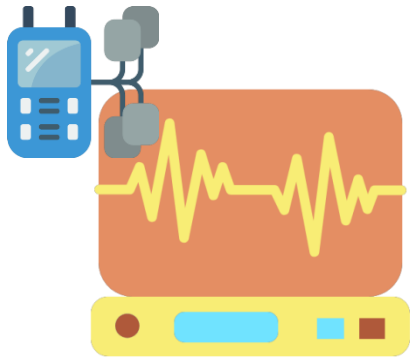


# 生產配方及自動化機台如何防駭？

- **資料保密**
  - 生產資料個別機台加密傳輸，並確保資料完整性
  - 研發配方拷貝到相同機台不能使用
- **杜絕駭客攻擊**
  - 驗證機台作動指令的正確性後才執行
- **管理數十台至百台機台使用不同密碼**
  - 全自動化用過即換，拋棄式密碼管理系統

**捷而思採用美國國家標準局認證之國防等級安全硬體加密器來產製、驗證及保護密鑰不被竊取**

# 捷而思物聯網資安解決方案



遠距醫療儀器設備

Microsoft Azure

AIoT

**Jrsys IoT Service**

裝置生命週期安全管理
✓身份認證
✓資料加解密金鑰管理
✓軔體安全更新

Restful API

IoT平台

**捷而思物聯網**
**安全控管**
**Gateway**

**ISO27701/GDPR**
**所有資訊加密**

2.資訊只給合法用戶看

3.未經認證之指令不執行

**設備內建捷而思物聯網高速、低耗能加解密及認證安全控管軟體**

1. 資訊加密後才上傳

**電腦、行動裝置**

**從電腦及手機可以根據權限安全地存取IoT裝置**

# 物聯網-金鑰管理系統

- 終端設備資料傳輸前預先加密
- 工廠端機台操作人員無法解密資料
- 韌體更新透過電子簽章驗證來源
- 支援多種 API 介接的解密平台
- 提供地端及雲端 兩種版本
- 可在Web或App解密資訊

# 防疫體溫監測智慧手環


## 智慧手環溫度監測解決方案

病患配戴智慧手環，可 24 小時監測健康狀況。當數據異常時，醫療人員可即時提供醫療措施、協助病患。
持續性的監測體溫和心跳，提供醫療人員病患的即時體徵數據，若數據超過正常值，便能立即採取醫療措施。持續的監測健康狀況，數據能協助更佳的人員健康狀況管理。

# 資安提前布署 (Zero Trust)

- 新冠肺炎大流行，不能信任”任何人”，所以大家都戴口罩
- 醫聯網資安除了WiFi, LoRa, NBIoT在通訊層的加密外，需要更根本的解決方案 ➔ 資料層加密
- 資料唯有系統維運商(防疫、長照)可以解密(零信任)

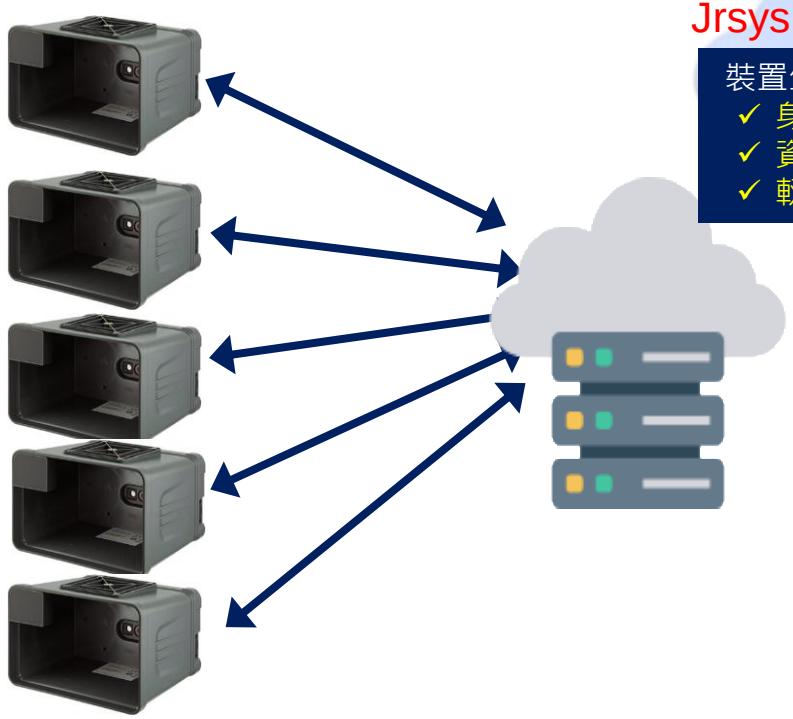

【Wi-Fi晶片出現安全性弱點，加密連線形同虛設】WPA2再現漏洞，10億臺設備暴險

# 防疫熱成像體溫體檢測儀實聯制流程

1.拍攝客人之台北通手機 QR碼，並同時偵測體溫

2.將資料加密後傳至捷而思物聯網資安平台資料不保留於設備

3.防疫熱成像體溫體檢測儀顯示或產生人聲音效
通過、QR碼有誤、單號/雙號 本日禁止進入、已打疫苗等各種訊息



Jrsys TRUST Service

裝置生命週期安全管理
- ✓ 身份認證
- ✓ 資料傳輸加密
- ✓ 韌體安全更新

Jrsys Edge
安控模組

# 捷而思物聯網資安解決方案

## 符合ISO27701/GDPR 病患個人生理資訊隱私保護要求

BTIoT

Jrsys

Catalog

CryptoLogs Table

CryptoLogs Chart

Home Contact

CryptoLogs

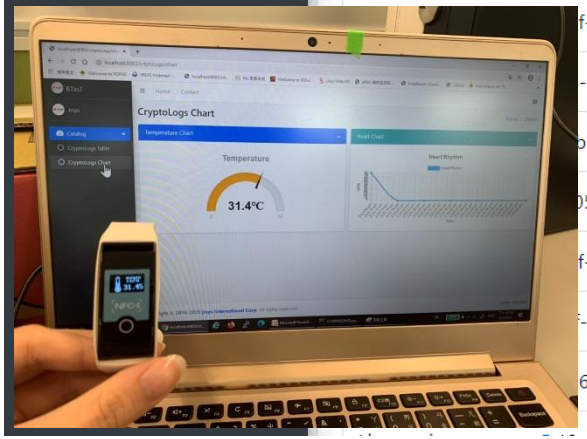
Home / CryptoLogs

CryptoLogs

加密

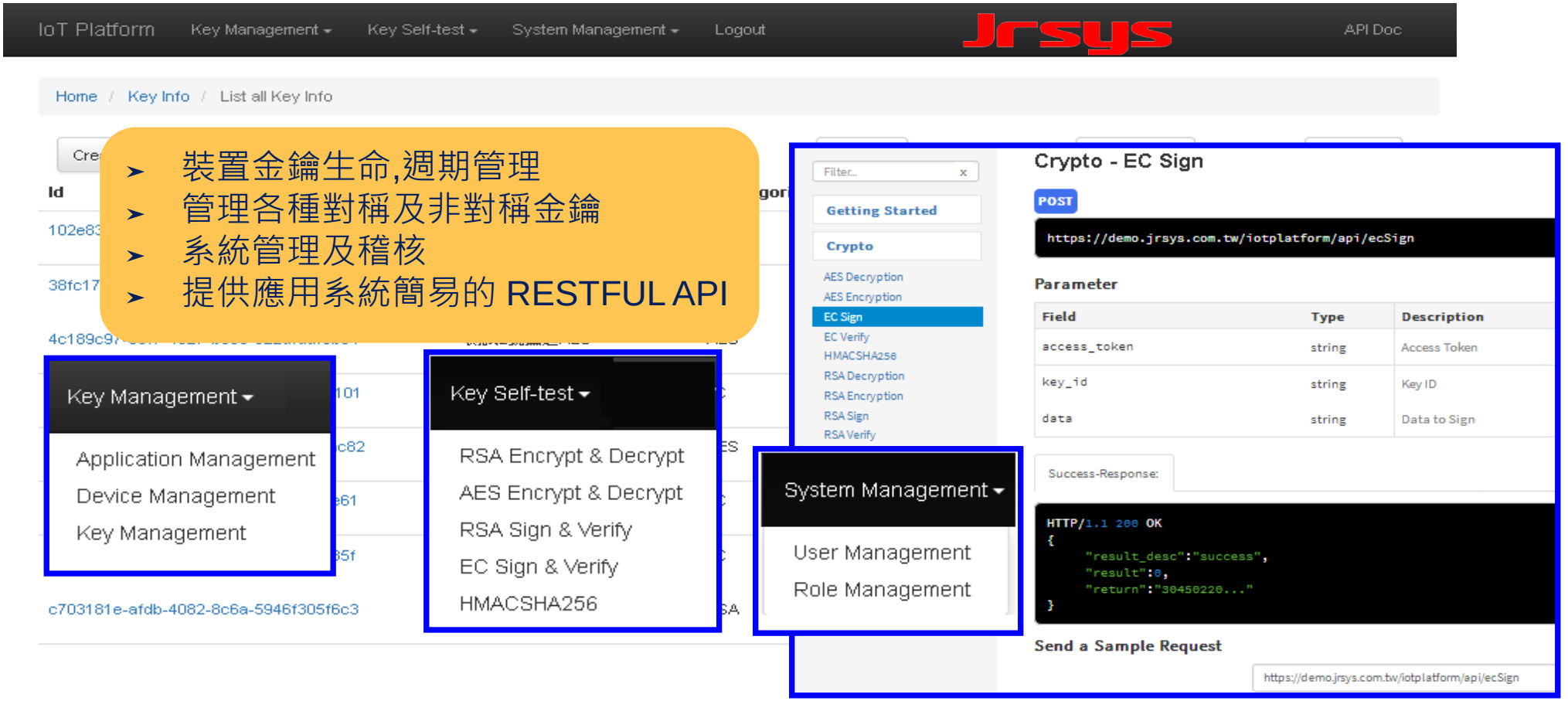
解密後資訊

| ID | Create Time | BT Address | Data | Heart Rhythm | Temperature |
|---|---|---|---|---|---|
| 41847bd4-8706-4df6-8777-4ec2a6f2baa6 | 2020-08-06 14:01:05 | 78:02:B7:80:15:5D | f334936af | 81bpm | 34.42°C |
| 8481495f-6d55-4e17-9a0c-e14ff4ad3c89 | 2020-08-06 14:00:55 | 78:02:B7:80:15:5D | 39b60ebc9 | 81bpm | 34.4°C |
| 6ae53f5f-2ba0-4426-a4eb-4f9ce9afdca6 | 2020-08-06 14:00:45 | 78:02:B7:80:15:5D | bbd5ea6e9 | 85bpm | 34.39°C |
| f-7eb82529beb2 | 2020-08-06 14:00:36 | 78:02:B7:80:15:5D | 676aa0463 | 86bpm | 34.3°C |
| -d5ce69084873 | 2020-08-06 14:00:25 | 78:02:B7:80:15:5D | ae695d9e6 | 84bpm | 34.26°C |
| o-20ab89f745b8 | 2020-08-06 14:00:15 | 78:02:B7:80:15:5D | 30b221e9d | 82bpm | 34.24°C |
| 05-4359552fa52c | 2020-08-06 14:00:06 | 78:02:B7:80:15:5D | b486b452c | 80bpm | 34.22°C |
| f-c89419406647 | 2020-08-06 13:59:56 | 78:02:B7:80:15:5D | 9886f02a9 | 82bpm | 34.16°C |
| -3913a82c3b58 | 2020-08-06 13:59:46 | 78:02:B7:80:15:5D | c05d34a42 | 84bpm | 34.15°C |
| 6-b4c931a0eb0f | 2020-08-06 13:59:36 | 78:02:B7:80:15:5D | af77f2ea5 | 84bpm | 34.09°C |



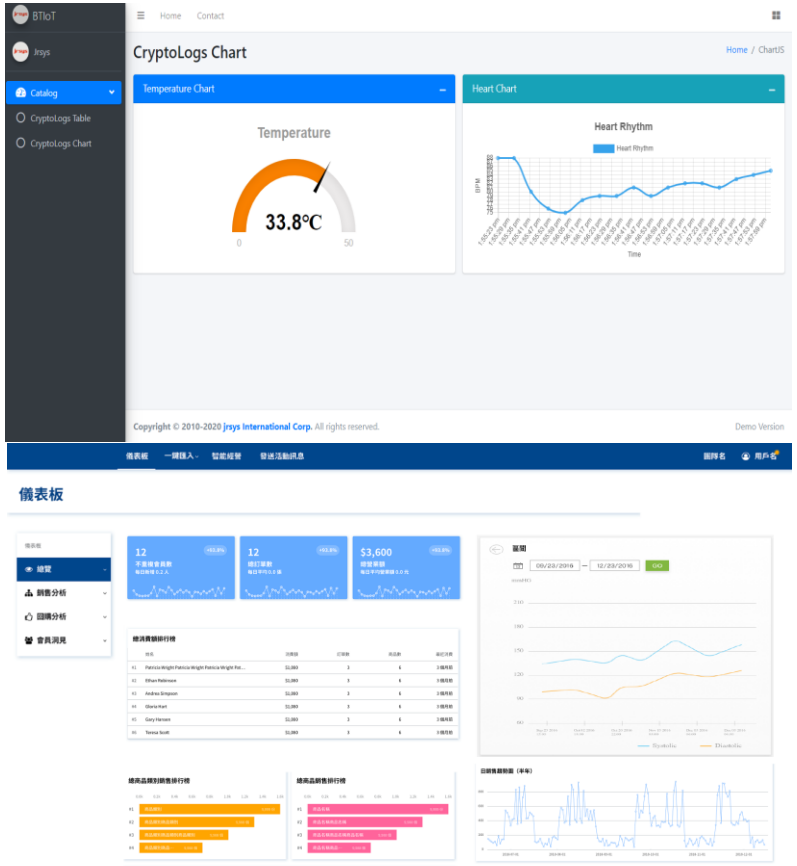
# 捷而思醫聯網安全管理平台

Server 端醫聯網裝置金鑰伺服器提供 RESTFul API 供服務系統使用



# 捷而思物聯網資安解決方案

## 符合ISO27701/GDPR 病患個人生理資訊隱私保護要求




# 捷而思物聯網資安產品

對於物聯網裝置多樣性MCU，依其效能及場域環境限制，提供 ：

- 國際標準的演算法 (RSA, ECC, AES, SHA) 安全軟體
- 嚴苛場域使用Jrsys 物聯網專用特殊演算法
  1. **加密強度高**
  2. **運算速度快**
  3. **超低耗能**
  4. **同時支援軟體(大量佈放之低價之感應器)及硬體解決方案**
- 完善的物聯網金鑰裝置全生命週期管理平台
  - **提供安全的金鑰佈放管理機制，防範內部人或駭客作怪**
- 嚴謹的使用者多因子認證機制
  - **適用 PC, iOS and Android**

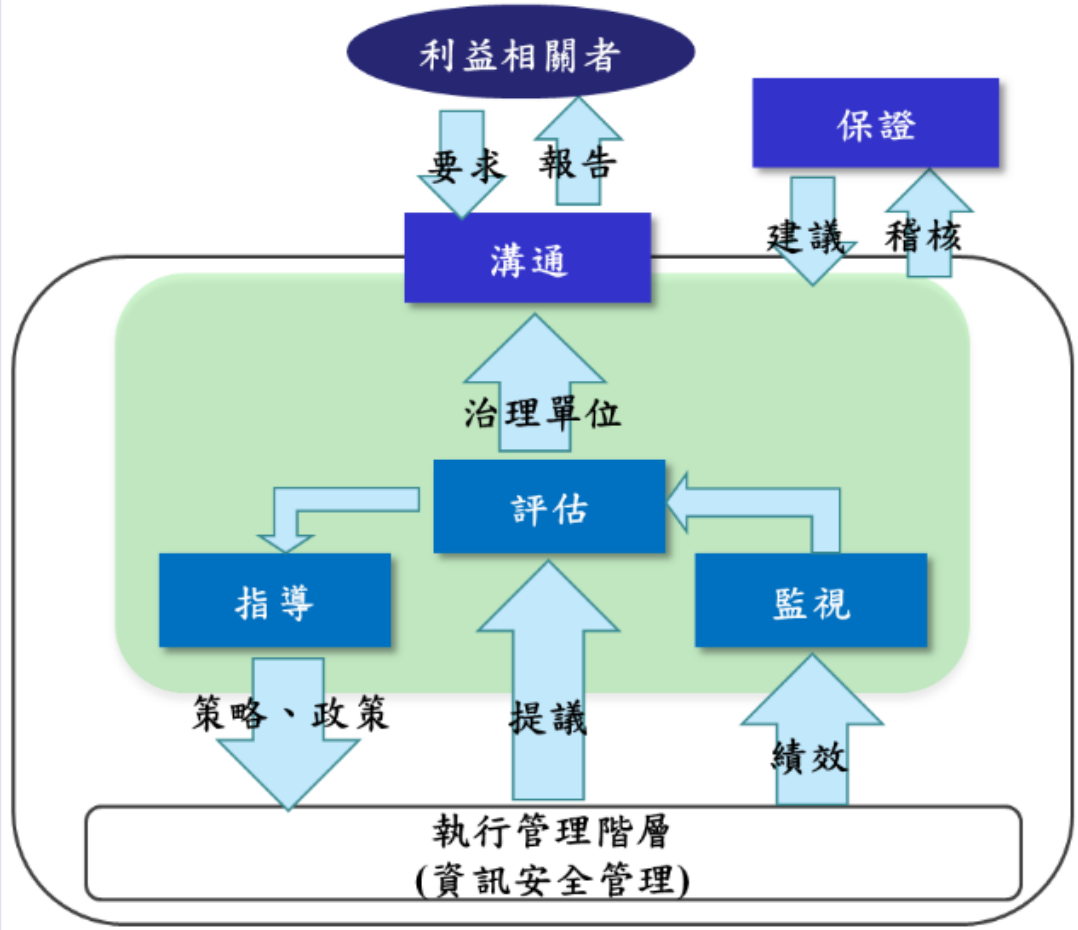
# 物聯網三大認證及傳輸加密保護

- 捷而思提供三大認證及傳輸加密保護：
  - **合法的使用者**：合法的使用者才能看到機台、居家及醫療護資訊
  - **完善管理的物聯網設備**：合法的設備才能與其他設備連結
  - **正確的執行指令**：確認是正確的機台、正確的物聯網裝置控制命令、正確的韌體的更新
  - **傳輸加密**：每個物聯網設備有獨立的動態金鑰，達成真正的點對點加密
- 符合國家物聯網資安檢核規範之要求：
  - **資料機密性**
  - **資料完整性與不可否認性**
  - **認證與授權**

# 捷而思提供符合國家物聯網安全規範解決方案

- 網路層
  - 資料傳輸於安全的加密通道
  - 安全的身分鑑別、白名單機制
- 監控及管理層
  - 傳輸資料的加密採用安全的機制
  - 設備的金鑰生命週期管理
- 控制層
  - 安全的指令鑑別機制
- 實體層加解密、認證
  - 具備強固加密機制
  - 雙因子認證功能
  - 安全的金鑰管理機制
  - 對稱式金鑰應以非對稱金鑰加以保護
- 物聯網實體感測裝置
  - 高效能、低耗電且安全之資料加密演算法
  - 資料完整性與不可否認性
  - 資料機密性
  - 韌體的完整性
  - 感知設備參數加密儲存
- 物聯網實體閘道器Gateway
  - 資料完整性與不可否認性
  - 資料機密性
  - RSA2048、AES256同級或更佳的演算法
  - 軟、韌體完整性確保系統安全啟動
- 備份、稽核機制
  - 安全的備份機制
  - 防篡改的操作稽核紀錄

# CNS 27014資訊安全治理模型




資料來源：CNS 27014

# 捷而思 簡介

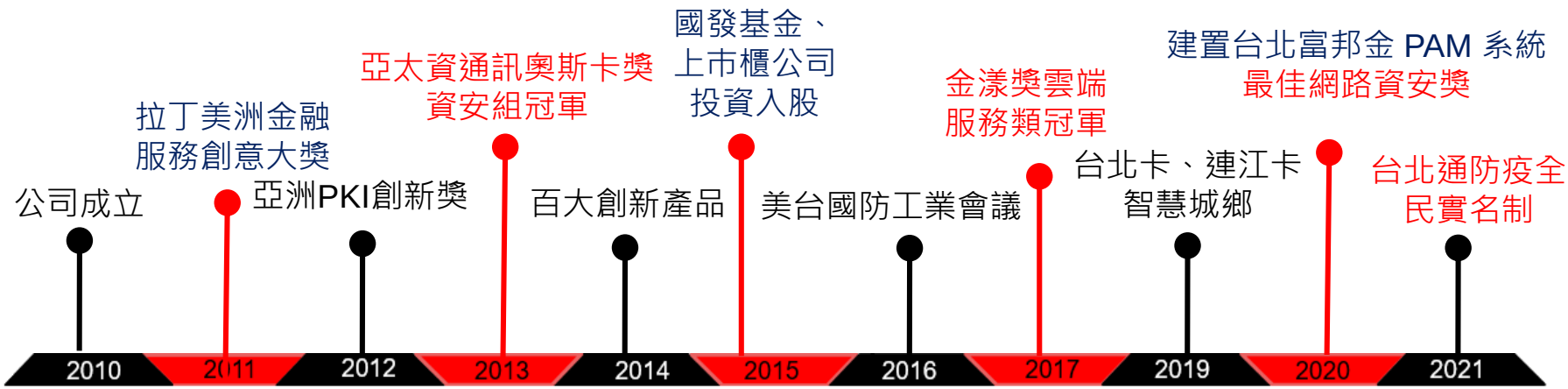
2010成立
實收資本額
6000萬

**資安技術**
**100%**
**自主研發**

國內外十多
項發明專利

國發/兆豐/
磐儀
皆為股東


APICTA
Asia Pacific ICT Alliance
AWARDS
2013 Winner Award

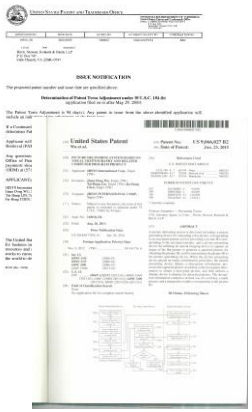


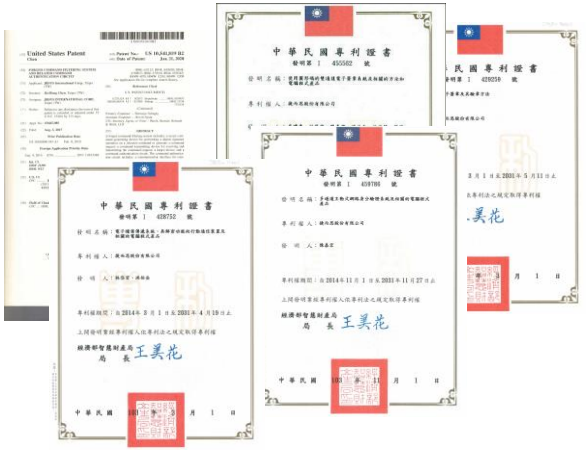
# 工業局工控資安服務能量


經濟部工業局技術服務機構服務能量登錄證書
Certificate of Registration as a Technological Service Organization


經濟部工業局技術服務機構服務能量登錄證書
Certificate of Registration as a Technological Service Organization


經濟部工業局技術服務機構服務能量登錄證書
Certificate of Registration as a Technological Service Organization





# 傑出的身份認證及工控資安成功案例

台北通、電子化政府資安建置、自然人憑證應用、外僑居留證智慧卡

自動通關生物識別、電子化政府資訊發展規劃顧問服務，援外計畫

國民健康雲資訊加值應用服務平臺

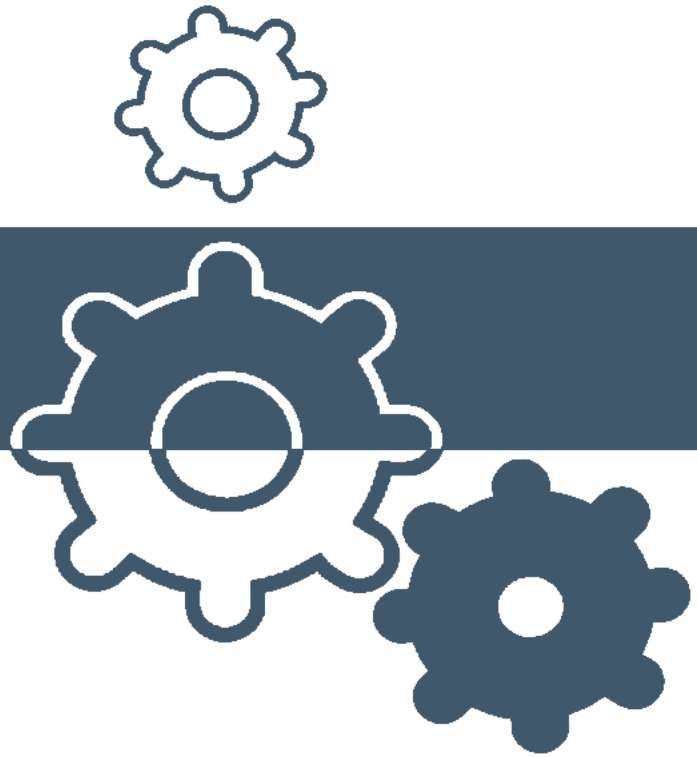
瓜地馬拉海關電子憑證報關系統、聖文森公務人員證

金融業電子合約系統及商業司商工登記PDF電子簽證文件

金融業最高權限特權帳號管理系統及憑證系統

金融憑證管理、安控系統及肥咖申報

**供應鏈廠商管理電子認證系統、智慧製造資安管控系統、物聯網設備資安**



# 附件

# IEC 62443-2-1

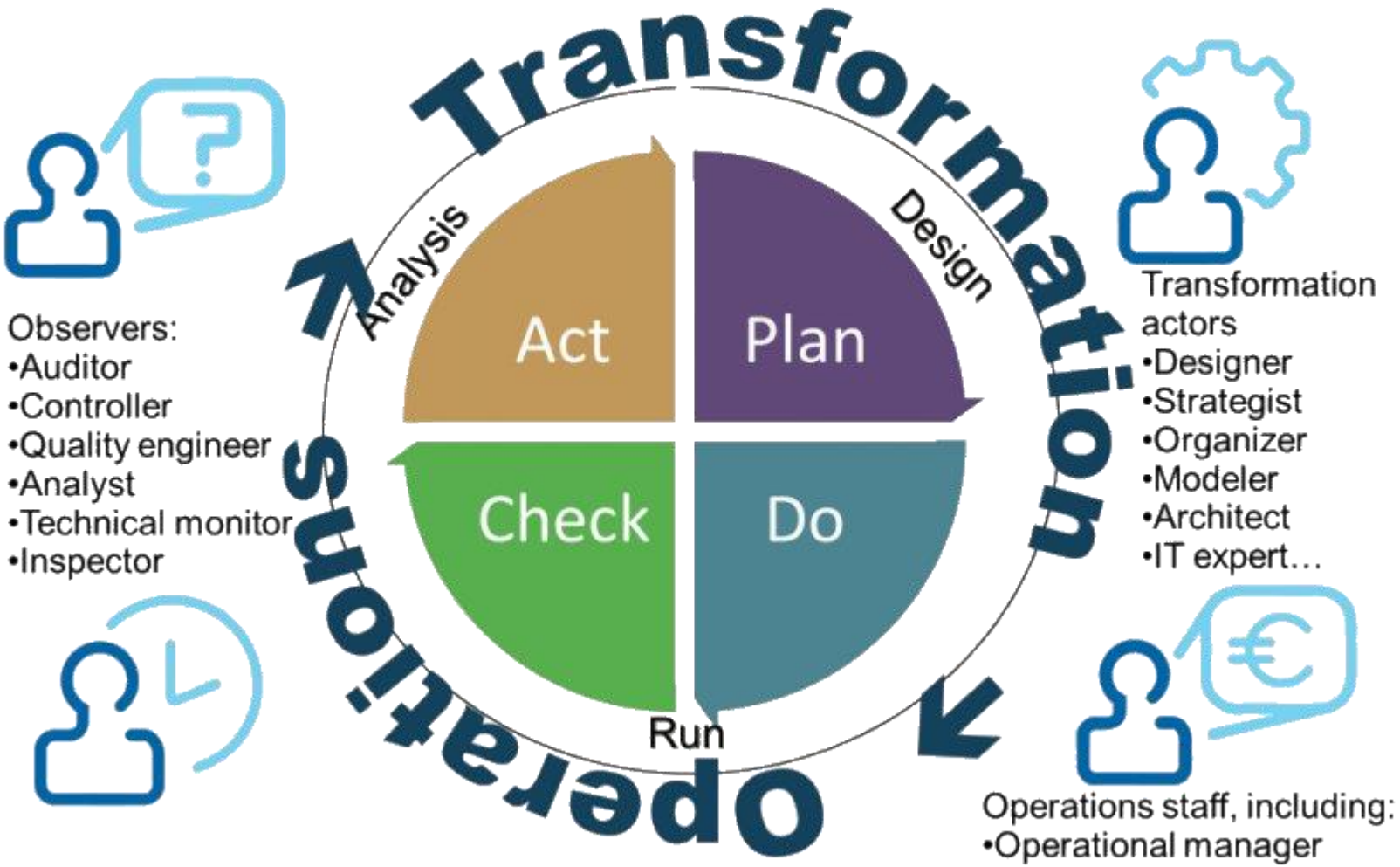
- 人力資源
- 法務
- 訓練
- 威脅模型檢查
- 風險識別與防禦
- 遠端存取
- 網段區隔
- 實體隔離
- 變更管理
- 使用者帳戶控制
- 事件和事故管理
- 風險目標檢視（漏洞檢查）
- 組態管理
- 可用性

# 資安管理系統

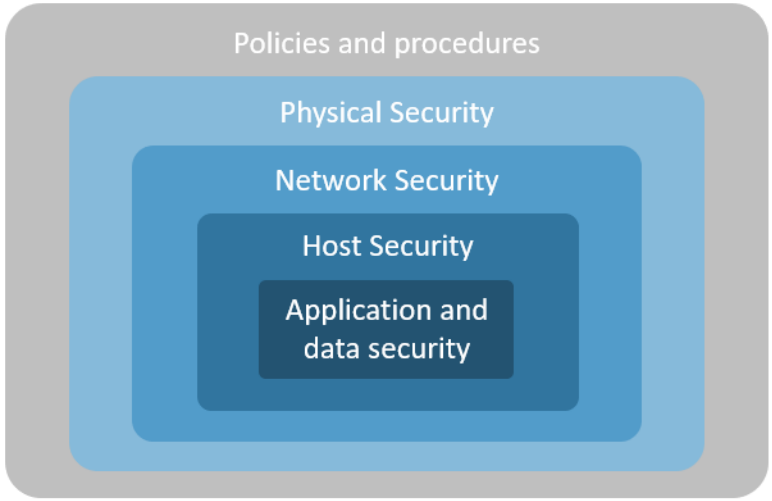
- Security ISMS ISO/IEC 27001/27002
- Privacy PIMS ISO/IEC 27701
- Sector Specific：
  - Telecom ISO/IEC 27011
  - Healthcare ISO/IEC 27799
  - Cloud ISO/IEC 27017
- IoT
  - ISO/IEC 27030 Guideline for security and privacy in IoT
  - ISO/IEC 30141 IoT Reference Architecture (IoT RA)
  - ISO/IEC 31700 Privacy by design for consumer goods and service


https://www.jrsys.com.tw

# 持續改善與運營


Transformation
Operations
Analysis
Design
Act
Plan
Check
Do
Run
Observers:
•Auditor
•Controller
•Quality engineer
•Analyst
•Technical monitor
•Inspector
Transformation actors
•Designer
•Strategist
•Organizer
•Modeler
•Architect
•IT expert…
Operations staff, including:
•Operational manager

# Defense in depth




- Policies and procedures: risk management, Incident-response, audit…
- Physical security: ID cards, CCTV, fences, barriers, fingerprints…
- Network security (corporate + ICS): Firewall, IDS/IPS…
- Host security: Restricted services, dynamic whitelisting…
- Application and data security: Timely patching, encryption…