DOI: 10.6653/MoCICHE.201912_46(6).0005

高科技半導體廠資訊整合與安全

鄭昭平／台灣積體電路製造股份有限公司 廠務處 技術經理

近幾年來製造業都在談「智慧製造」或是「工業 4.0」，而在這些名詞背後真正的目的，就是建造一個「智慧工廠」，來提昇生產管理的效能，不僅是自動化，還要智能化、最佳化。

數位化、物聯網、大數據、雲端資料庫、到現在的人工智慧都已被視為「智慧工廠」所必要的元素，但真正的關鍵是要把它們整合起來，將分散在工廠各處的資料彙整、做分析，把它們變成有用的資訊，再轉化成知識，這才能幫助效能的全面改善、輔助管理與決策，真正做到所謂的「智慧製造」「智慧工廠」。

而「資訊安全」與「智慧製造」的關係卻又緊密相連，工廠流程越自動化、越智能化，代表數位化的程度就越高，依賴資訊相互傳遞溝通就越頻繁、越緊密，當資安發生問題時，對工廠的影響就越大、越嚴重。資安做不好、做不到位，智慧工廠就完全失去了保護。隨著數位化時代的來臨，萬物皆聯網，資安就更顯得重要；只要有一次的網路駭客入侵成功，智慧工廠所帶來的效益將瞬間化為烏有。

工廠資訊整合

過去傳統工廠，功能系統大都各自獨立運作，系統間鮮少彼此有太多的整合。一旦需要合作，就只能透過各系統產出的報告，或額外由自各系統產出數據，以滿足系統間資訊交換或分享的需求。需要資訊的人可能連自己都無法確實掌握所需要的完整資訊，更別說要藉由分享彼此資訊來解決問題。

好比打籃球，有了教練、小前鋒、大前鋒、中鋒、控球與得分後衛就能形成一個籃球隊參加比賽；但若想要贏球、成為好球隊，每個隊員都必須先把自己的角色做好，同時還要能與隊友培養好的默契、有共同目標、相互合作，這很重要。同理，一個半導體廠能產出好的積體電路（IC, Integrated Circuit），是需要許多單位共同努力與合作才能做到；其中包含了廠務單位、機台設備單位、生產製造單位、品管單位、研發單位 … 等等，每個單位都扮演很重要的腳色，環環相扣，缺一不可。

一個工廠能夠運作有很多工作要做，這些工作執行必須靠不同的系統輔助來達成，透過網路將他們連結起來，讓這些活動資訊可視化、透明可見，有智慧、有效率來管理工廠一切大小事，並建立系統化的管理運作模式。

高科技半導體廠房設施

高科技半導體廠廠務的最主要任務是提供工廠製造所需的生產環境（無塵室），以及水、電、空調、氣體與化學品的穩定供應，並確保品質、可靠度與安全性；而生產製造所產生的廢氣、廢水，必須經過嚴格的處理，確認對環境無汙染才能排放，並盡最大能力使其回收再利用（圖 1）。廠務系統包含電力系統、機械系統、水處理系統、氣體化學系統、儀控系統與消防安全系統，這些系統要能相互配合，才能確保穩定運轉，有了廠務的穩定，工廠的製造就能順利產出。這些系統必需相互合作，所有的資訊必須整合起來，目的就是要能全面掌握資訊、讓不同平台相互支援，達到效益最佳化。把各種自動化機器、設備與管理系統都串起來，再與工廠生產製造資訊做進一步整合，將資訊活化。

圖 1　廠務系統總覽

廠務建置一套能強化運作及管理的系統資訊整合平台是必需，也是智慧廠務（Smart Facility）是否能成功的關鍵。自動化控制時代，廠務監控系統（FMCS, Facility Monitoring and Control System）是廠務的核心，它肩負廠務第一線的防護，做各系統運轉狀態的即時監控（圖 2 和圖 3）；但進入智能化控制時代，它需要更強大的資料整合與分析能力來創造更有效的管理價值，進一步提升廠務運轉品質及人員工作效率。廠務運作每天都有不同的系統在管控與紀錄，如晨夕會值班交接、系統運轉與警報監視、品質與工程檢視及設備維修保養作業 … 等工作，在這樣繁雜但有規律的運作中，要快速有效檢視這些資訊並找出問題，需要透過資料整合與分析，讓廠務運作與管控變得更精確、且容易。

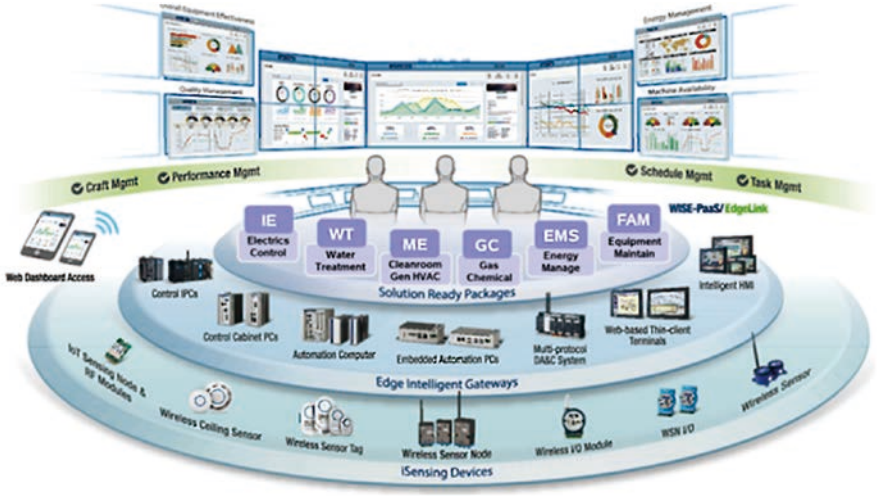

圖 2　FMCS 中央整合監控

圖 3　廠務 FMCS 監控中心

資訊整合實現

首先，蒐集來的資料必須要儲存在一個好的系統平台才能長治久安，這個 OneFAC 平台必需是符合高可靠性（HA, High Availability）軟硬體架構，並且要有支援故障備援的能力（圖 4）。

平台應用軟體之設計與功能開發，必需滿足下列需求（圖 5），整合之有效性才能真正被落實在實務的運作與管理上（圖 6）。

- 介面統一：讓各單位的操作、資訊呈現，乃至溝通語言皆一致，資訊分享及溝通合作就會有效率。

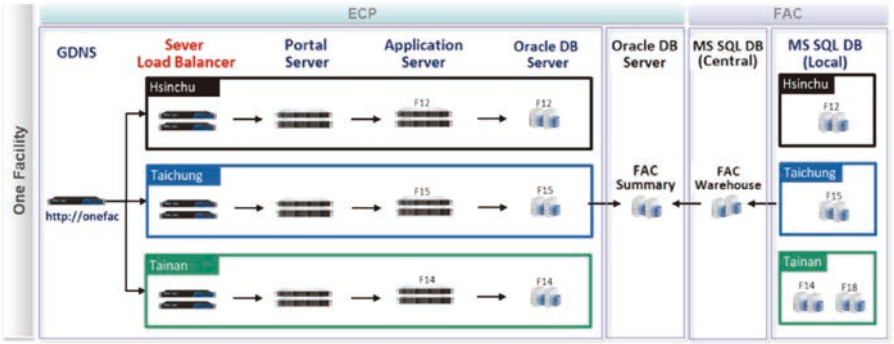

圖 4　廠務 HA 高可靠度系統平台架構

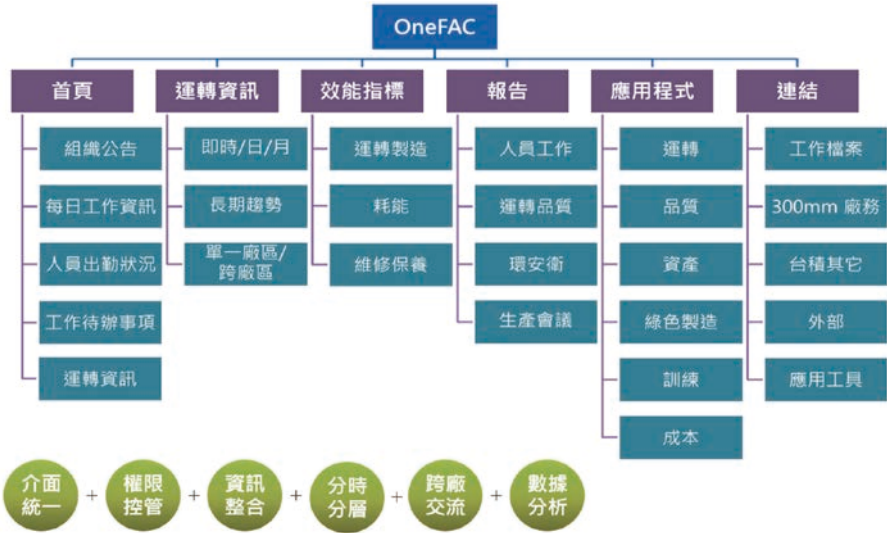

圖 5　廠務 OneFAC 平台功能需求

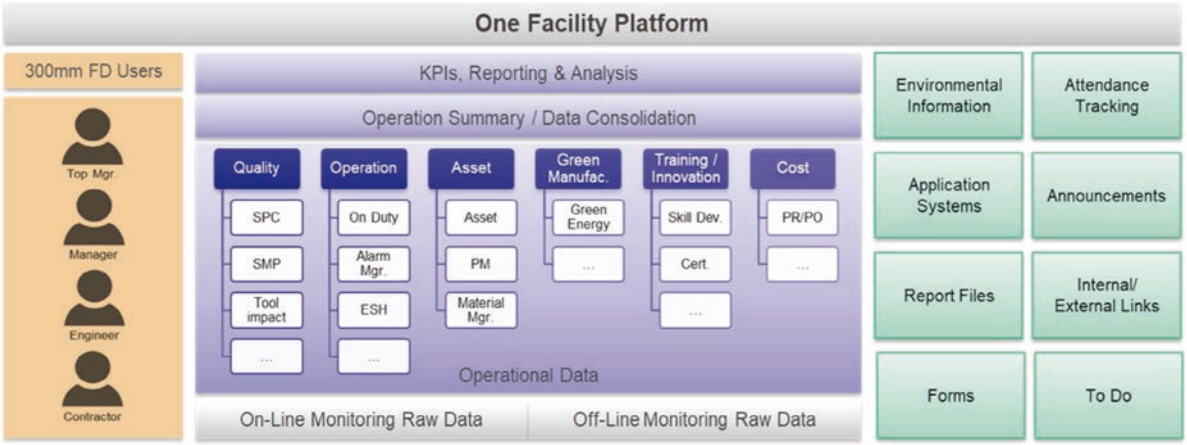

圖 6　廠務 OneFAC 資訊整合

- 權限控管：依人員職級、單位與工作屬性來定義不同權限，依角色不同提供其所需資訊（可加速所需之資訊查找），並能落實 Need to Know 原則。
- 分時分層：依操作目的不同，提供不同時間分隔（即時 / 日 / 週 / 月 / 年）之統計數據，協助即時或長期檢視運轉效能。
- 資訊整合：橫向整合廠務端系統、提供工作所需之廠務系統運作與管理資訊；縱向與工廠製造及設備端資訊連結，協助生產上下游異常原因之快速查找與分析。
- 跨廠交流：讓各廠區廠務的運轉資訊可以流通，促成資訊及經驗共享，發生的大小事即時得知，自我省視並適時給予跨廠支援。
- 數據分析：長時間、多面向進行資料分析與呈現，協助問題的解決及管理決策，並透過關鍵效能指標（KPI, Key Performance Indicators）檢視運轉效能及成果。

台積電廠務資訊整合平台（OneFAC Information Integrated Platform）將竹科、中科、南科各廠務資訊統整起來，提供了以下的資訊與成果：

- 組織公告及個人每日待辦資訊：掌握組織發生的大小事及以個人為單位各別提醒一天預計執行的工作與計畫。
- 各課每日工作及晨夕會值班交接資訊：掌握各課每日工作項目與執行狀況，如人員出勤、值班、工程風險與施作及設備維修保養等（圖 7）。
- 運轉品質資訊：提供即時、每日、每週、每月包含生產、品質及環安衛相關運作資訊成果進行檢視，並自動警示異常以及時發現問題與改善的機會點。
- 跨廠資訊：除自己廠，亦可檢視跨廠區資訊，涵蓋製程警報、設備妥善率等重要資訊，除了與它廠比對成果外，亦快速獲取它廠發生的大小事，藉以自我省視或適時給予它廠協助（圖 8）。
- 成果報告：主管週月報、各廠運轉品質與環安衛報告等，有助於資訊分享、互相學習、與聚焦團隊之共識。
- 數據統計分析資訊：長時間累計的數據，透過視覺化操作，從不同面向檢視短中長期趨勢，亦可聚焦於細部資料，定期檢視關鍵效能指標，從提供的數據比對分析，協助管理決策。
- 內外部連結資訊：將不同功能用途之應用系統、工作檔案與連結進行分類，如運轉、品質、資產、成本、訓練學習等，提升資訊查找的效率及避免重工。

資訊安全的重要

近幾年工廠遭駭客入侵的案例逐年增加，小從資料竊取，大到癱瘓工廠運作造成嚴重損失，2018 年的台積電 Wannacry 病毒入侵事件就是一例。

圖 7　組織個人專屬每日工作資訊

圖 8　廠務跨廠運轉資訊整合

高科技半導體廠對資安的要求遠超過一般傳統製造工廠，原因無他，因為高度自動化與智慧化所使然；當然資安問題造成半導體廠的損失也遠大於傳統工廠。企業中結合了 IT（Information Technology）與 OT（Operating Technology）兩大系統，讓製造系統的資訊可被最大化應用；而其中的廠務系統設備大量使用在工業生產製造 OT 系統，而絕大部分的工業控制系統設計之初不會將資訊安全（Security）納入考量，安全（Safety）及可用性（Availability）才是第一要務，因此工控在此操作環境下的資安體質天生就較脆弱，不像在一般商業應用資訊環境 IT 系統，對資安保護與應用已相對完整與成熟。但無論是 IT 還是 OT，如何達到更有效的資安防護都是現今最重要的議題之一（圖 9）。

資訊安全防護

要做好資安工作，必須從自我風險評估開始做起，重新檢視自己的資安體質，才能明瞭自己的弱點與可能受到的威脅。接下來再依據風險高低與成本花費，規劃出合適的資安防護策略與藍圖，這包含制度與程序的建立；像是定義資安團隊、組織人員權責（R&R, Role and Responsibility）、資安標準作業程序、異常應變處理程序…等，將制度與方案整合並融入工廠日常運作，定期檢視，同樣使其成為系統化的運作模式，如此才可以達到事前預防、事發應變處置與事後檢討的有效資安防護。

一般在工廠病毒入侵攻擊，常見以下幾種方式：

- 從任一有資安漏洞之裝置入侵（USB、CD Drive 等）
- 植入惡意程式（勒索病毒、木馬程式等）
- 阻斷作業系統或應用軟體之服務（殭屍網路 Botnet）
- 透過通信管道進行惡意程式植入（無安全性的通訊協定）

美國國土安全部（DHS）早在 2015 年就針對美國本土所發生之駭客入侵事件對工控資安提出七大防護策略（圖 10），包含建置防火牆、導入應用程式白名單、正確的組態設定與防毒軟體安裝、關閉未使用的通訊埠與服務、建立可防禦網路架構環境、強化權限密碼認證管控、持續監控及資安應變、強化安全遠端存取機制，而歐盟網路與資訊安全局（ENISA）在今年（2019）也發佈工業 4.0 資訊安全的挑戰與建議，包含了資安意識普遍不足且缺乏資安專家、公司資安策略不完整與投資的意願不高（投資資安無法明確獲得帳面上的利益）、現行工控資安技術標準及規範都不足且無整體性規範、無法整合舊有系統設備的技術與困難等問題有待克服。我們期望未來能發展更完整的資安防護規範，並落實防禦機制，來有效防止駭客的入侵，減少低資安問題的發生。

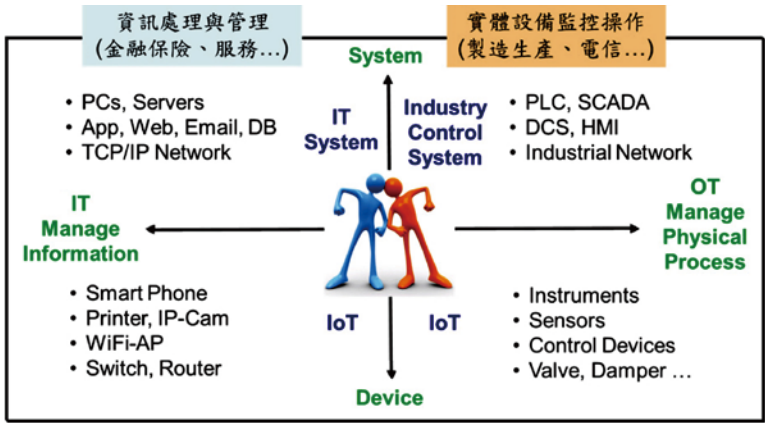

圖 9　IT & OT 資安範疇

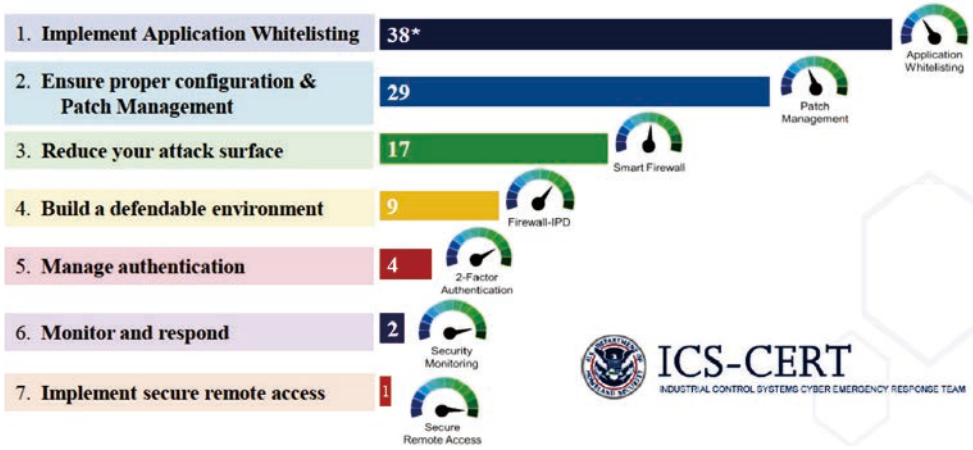

圖 10　工控資安七大防護策略（ICS-CERT）

結論

「智慧製造」與「資訊安全」二者息息相連、對任何高科技廠都非常重要，勢在必行。唯有做好了資安防護，智慧化願景才能踏實來落實。

工廠生產運作要有智慧，先要能整合所有資訊、建立完整的大數據，進而透過進階資料統計分析與人工智慧（AI, Artificial Intelligence）演算法技術來活化資料。如此，我們就真正可以做到系統異常自動判別分析、設備機台預知保養甚至準確預測失效發生，並運用巡檢機器人來無時無刻巡視廠房，發現問題、協助工廠運轉與決策管理、提高生產效率，這樣才真的算是「智慧廠務」、「智慧工廠」。

工廠隨著自動化與智慧化的導入會變更聰明，隨之而來的是員工會轉而專注於更高價值的工作。現在不只是系統、設備、資訊要整合起來，接下來人與機器的整合會更多、也更好、更有效，讓工廠營運的價值與獲利同步達到最高。

參考文獻

1. Will Wu & Tim Cheng, The Establishment and Development of OneFAC System Platform, tsmc FAC Journal v24, 2016
2. Internet Security Threat Report, Symantec, 2019
3. Seven Steps to Effectively Defend Industrial Control Systems, ICS-CERT,
4. Industry 4.0 Cybersecurity: Challenges & Recommendations, ENISA, 2019