運營技術（OT）系統所面臨的挑戰與保護策略

◆ 華梵大學特聘教授 — 朱惠中

運營技術（OT）系統對於工業和關鍵基礎設施的運營至關重要。然而，此類系統通常由可能已有數十年歷史（上世紀所開發製造的軟硬體）且缺乏現代安全功能的設備所組成，使得 OT 系統容易受到新型態的網路攻擊。[1]

OT 系統面臨的挑戰

歸納國內外相關文獻及我國國情後，綜整 OT 系統所面臨的挑戰及其可能造成之衝擊，如次說明：[2]

一、OT 系統之發展與沿革略可分為人力時代、電氣化時代、自動化時代及智慧時代等四個階段，各階段的主要控制機制分為機械及電子電力（類比）控制、電腦（數位）控制，及整合與智慧控制等，至於其相對應的時程，除智慧時代外，餘均早於 20 世紀初期，故負責操作與規劃人員大多數普遍欠缺資訊（安）技能。

[1] 對 OT 與 IT 的更多認識，請參閱本刊第 42 期頁 11 至 16，〈如何降低 CI 遭網路攻擊的衝擊〉，https://mjib-ebook.com/MJIB/no42/index.html；本刊第 45 期頁 56 至 61，〈如何縮小 CI 資安防護人才缺口〉，https://mjib-ebook.com/MJIB/no45/index.html。

[2] Cabrera, E (2016). *Critical infrastructure under attack: The vulnerability of converged IT-ICS networks.*

圖 1　OT 系統之發展與沿革

二、大多數的 OT 系統係由歐、美、日等地輸入，終端使用者在應用軟體（如 OT 之邏輯控制、系統的架構與安全標準等）及硬體操作介面的自主性均較低，因此資安問題更顯得重要。

三、基礎防護觀念與經驗薄弱，諸如安全防護不足、介入控制不嚴格、外包服務管理缺失（易受供應鏈攻擊）、教育力度不夠及應變能力不足等，均是需要強化處。

四、人員缺乏安全意識，管理 OT 系統的操作員和技術人員因可能缺乏安全意識和培訓，使他們容易受到社交工程攻擊。基本上成功的社交工程攻擊將可透過從業人員的輕忽，獲取對機敏資料或系統的存取控制。

五、資安工具疊床架屋的情況嚴重，這是因為觀念錯誤導致，認為工具越多越安全。事實上，工具太多會因增加複雜性，導致資安團隊疲乏、過勞，實際上反而會增加誤判風險。故新的工具應該是為了協助資安團隊，而非讓他們工作更加沉重。

六、OT 網路設備的基本精神是經久耐用而不是更新，許多工業設備對正常運行時間的嚴格要求（如無法隨時停機），迫使更新或更換變得困難、成本高昂或存在風險。

七、IT-OT 融合以及新技術將增加風險，隨著數位化轉型打破 IT-OT 障礙，以及嶄新複雜網路攻擊的出現，均使得 OT 網路框架的適應速度相對過慢。

八、許多 OT 網路所有者因對採用零信任機制的猶豫不決及對停機導致收入損失、基礎設施中斷甚至危及人員安全的擔憂，即使零信任仍然是保護現代網路的最有效策略，但工業運營商仍無法確定或權衡成本和複雜性的潛在危機。

九、普渡（Purdue）模型是否仍然適用於現代 OT 網路？傳統 OT 係使用區域概念以上下文為基礎（context-based）來進行分段（segmentation），但因 Level 0 感測器（sensor）所蒐集的資訊可以直接發送到雲端，並通過蜂巢網路（cellular networks）直接與雲中的監控軟體通信（亦即 OT 網路的分段框架通常被擱置一旁），復以蜂巢網路其本質上是扁平的，故 Purdue 模型似無法落實於蜂巢網路。

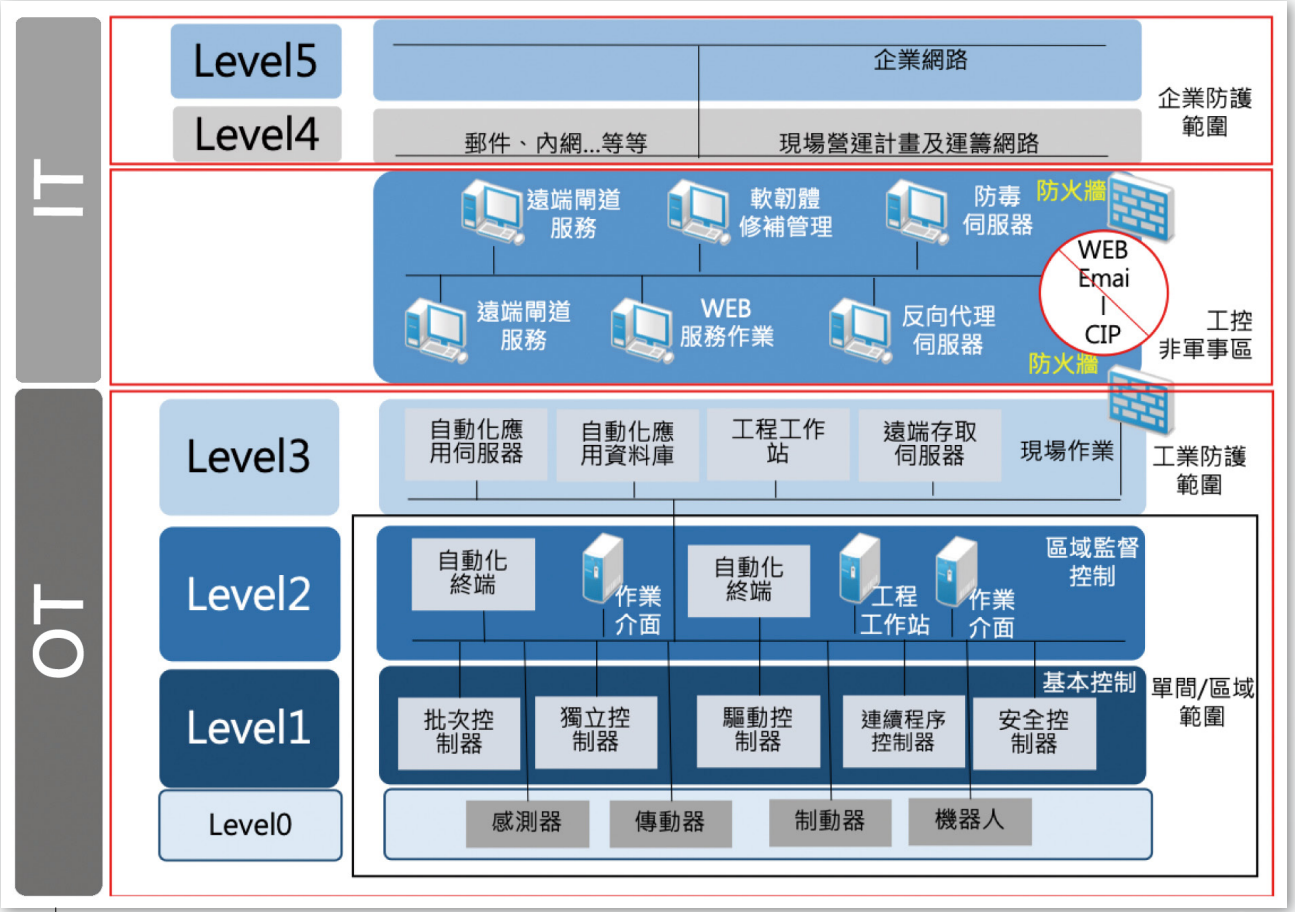
十、企業營運比以往更加仰賴即時數據提供收費依據，此外也需要遠端存取提供支援，因此，OT 網路必須與企業網路和網際網路連接。而原本跟外界 IT 網路隔離的 OT 網路對逐漸與 IT 網路整合的情況，尚未做好妥善準備。

十一、不安全且含有漏洞的 IT 網路一旦與 OT 網路直接相連，將使得控制系統（Purdue 模型中 L2 及 L3）暴露在網路攻擊的危險當中。歹徒可利用不安全的企業網路設備當成跳板，經由彼此依賴的複雜網路，一點一滴逐漸移轉到最容易攻擊的工業控制系統（ICS）設備和資料庫。

十二、OT 系統缺乏加密機制；加密對於保護現代工業和關鍵基礎設施流程中的機敏數據和通信至關重要。然而，運營技術 OT 系統因可能不支援現代加密演算法，使它們容易受到攻擊。復以系統缺少終端使用者行為紀錄，亦無法歸責或追溯被洩露的使用者帳號行為。

十三、因 OT 系統使用不安全的通信協議，故攻擊者較易入侵 OT 系統。

「零信任機制」是一種網路資安的架構和目標，它的假設前提是任何交易、個體與身分在獲得信任並持續維持信任之前，全都不可信任。



普渡模型為 OT 與 IT 網路環境整合的參考模型，共分為 6 個層級，但至今是否仍適用於現代 OT 網路已引起疑慮，且不安全並有漏洞的 IT 網路一旦與 OT 網路直接相連，將使控制系統（L2 及 L3）暴露在網路攻擊的危險中。（資料來源：經濟部，https://www.acw.org.tw/UpFiles/05- 網通產業工控物聯網資安實務指南 .pdf）

保護 OT 系統的策略[3]

一、進行風險評估

風險評估是針對「識別潛在危險」並「分析危險發生時可能發生的情況」的過程，其目的是識別、評估對 OT 系統所存在的風險並確定其優先等級的過程。組織將根據風險的潛在影響和發生的可能性及機率，對風險進行優先排序；並依據風險評估的結果，制定並實施降低風險的策略，以減少網路遭受入侵的機率。

二、實施網路分段

實施網路分段的目的為降低 OT 系統的風險，將網路劃分為更小、更安全的子網或網段，以縮小網路受攻擊的範疇，並為每個子網路提供獨特的安全控制機制和服務，保護關鍵資產遭受駭客攻擊或降低網路攻擊可能造成的損害。此外，組織應識別關鍵資產和系統，並將它們與非關鍵系統區分開來。依據最小授權機制精神，從外部連線之用戶，應配置於專屬網段，

[3] Abhay, S. K. (2023, April 24). *Securing legacy OT systems: Challenges and strategies.* Sectrio. https://sectrio.com/securing-legacy-ot-systems-challenges-and-strategies

網路分段係將網路劃分為更小、更安全的子網或網段，以縮小網路受攻擊的範疇，並為每個子網路提供獨特的安全控制機制和服務，保護關鍵資產遭受駭客攻擊或降低網路攻擊可能造成的損害。

並搭配防火牆予以隔離；不同類型用戶與不同類型資源，皆應以不同網段予以區隔，才能在發生攻擊事件時，將災害縮減至最小範圍。

三、實施存取控制

應控制對 OT 系統的存取，其機制應包括強大的身分驗證、授權和問責機制。組織應將對關鍵系統的訪問限制為僅允許有合法存取需求的授權人員進行存取。實施存取控制的第一步是確定需要保護的資產以及需要存取的個人或軟、硬體資產。接著應制定存取控制政策，來定義授予和撤銷對這些資產存取權限的規則。在授予系統存取權限之前，應使用強大的身分驗證機制，例如雙因子身分驗證（2FA）或生物識別身分驗證來確認用戶的身分。

四、實施系統強化

系統強化（systems hardening）通常是通過減少攻擊面（attack surface）來保護系統的過程，當系統能執行的功能增加時，漏洞面會隨之變大；原則上，單一功能系統的安全性比多功能系統來的高。減少可用的攻擊方式（attack vector）通常包括更改預設密碼、刪除不必要的應用軟體，以及禁用不必要的端口（port）或刪除不必要的服務、協議和應用程序等。此外，建置防火牆、入侵檢測（Intrusion Detection System, IDS）和入侵防禦（Intrusion Prevention System, IPS）系統、限制利用遠端桌面協定（Remote Desktop Protocol, RDP）對 OT 系統和組件進行存取，亦可降低網路攻擊成功的可能。惟須注意的是系統強化固可降低網路攻擊成功的風險，但任何錯誤配置可能導致意外後果或停機。

五、實施安全監控

包括實施網路和系統監控工具、入侵偵測系統以及安全資訊和事件管理（Security Information and Event Management, SIEM）解決方案，以檢測潛在威脅。同時，組織應同步建立緊急應變的復原計畫與程序。重要的是，安全監控應該是一個持續的過程，組織應該定期審查和更新監控策

在授予系統存取權限之前，應使用強大的身分驗證機制，例如雙因子身分驗證或生物識別身分驗證來確認用戶的身分。

系統強化是通過減少攻擊面來保護系統的過程，減少可用的攻擊方式包括更改預設密碼、刪除無需的應用軟體、服務、禁用無需的端口等；此外，建置防火牆、入侵檢測和入侵防禦系統、限制遠端桌面協定存取，亦可降低網路攻擊。

略，以確保在面對不斷變化的網路威脅時保持有效。

六、實施安全意識培訓

此培訓對於降低人為錯誤或疏忽導致的網路攻擊至關重要，應包括定期網路安全意識培訓以及通報潛在安全事件或威脅的明確程序。

七、定期更新和修補

OT 系統的使用壽命通常很長，並且可能運行在過時的軟體和硬體上，這使它們容易受到網路攻擊，定期更新和補丁（patch）將有助於解決這些漏洞。組織宜制定補丁管理程序，包括定期審查軟體和硬體更新、部署前測試補丁以及跟蹤和報告補丁部署的流程。同樣重要的是，要確保任何 OT 系統仍持續從製造商或供應商接收到安全更新，並擬定計畫來解決可能出現的任何安全問題。但是，由於傳統的定期更新和修補會造成關鍵運作中斷，使得更新和修補 OT 系統可能具有挑戰性。一般而言，更新和修補 OT 系統會配合關鍵系統大修時程進行。

八、實施數據備份和恢復計畫

OT 系統通常處理對業務運營至關重要的關鍵數據，這些數據的丟失或損壞可能會造成嚴重後果。組織應制定資料備份和恢復計畫，包括定期計畫的關鍵資料備份、備份和恢復程序測試，以及監控和報告備份和恢復狀態的流程。重要的是要確保安全地存儲備份並定期測試備份數據以確保在數據丟失或損壞的情況下可以恢復。此外，組織應考慮實施冗餘備份系統，如備份 3 份資料、2 種儲存媒體及 1 份異地備份的方式，以提供額外的保護層，防止資料遺失或損毀。

OT 系統通常處理至關重要的關鍵數據，組織應制定資料備份和恢復計畫，確保安全地存儲備份並定期測試以確保在數據丟失或損壞的情況下可以恢復。

九、實施災難復原計畫

包括識別關鍵系統和數據的過程、制定在發生災難時恢復這些系統和數據的計畫，以及測試和培訓人員執行該計畫，並定期測試和更新災難復原計畫以確保其有效。此外，組織亦應考慮實施冗餘系統或備份設施（High Availability, HA），以防主要系統或設施受到損害。

十、實施事件緊急應變計畫

事件的範圍從網路攻擊和系統故障到人為錯誤和自然災害，亦即須由天然災害、人為疏失及資訊安全等三個面向來規劃，並須考量當上述三個面向同時發生時的 SOP。組織應先確定最有可能發生的事件類型，例如網路攻擊或系統故障。然後，制定一個計畫概述應對每種類型的事件單獨或同步（兩種類型或三種類型）發生時應採取的步驟，計畫內容應包括檢測、遏制、根除和復原程序。

事件的範圍從網路攻擊和系統故障到人為錯誤和自然災害，亦即須由天然災害、人為疏失及資訊安全等三個面向來規劃，並須考量當上述三個面向同時發生時的 SOP。

結語

資安防護不難，難在如何落實。此外，針對不同關鍵基礎設施的 OT 之客製化，及作業疏失所造成的問題，均是本主題的關鍵成功因素。