關鍵基礎設施之脆弱點簡介

◆ 華梵大學特聘教授 — 朱惠中

地緣政治角力下，關鍵基礎設施成箭靶。各國八成以上的關鍵基礎設施，都是仰賴工業控制系統來執行自動化作業，因此，工控系統若防護失靈，將衍生國安危機。

工控系統為關鍵基礎設施運作主軸

關鍵基礎設施（Critical Infrastructure, CI），已由隱學變成顯學，為強化 CI 防護的有效性，必須瞭解 CI 弱點，亦即訂定其韌性（Resilience），以提高當資安問題發生時 CI 的可用性，並為主管階層進行資安風險管理相關決策時，提供各種必要的資訊。又因超過 80% 的 CI 是依賴工業控制系統（Industrial Control System, ICS）來執行其自動化作業，故 ICS 實為 CI 主軸，本文彙整國內外的相關文獻，匯整出 ICS 之相關脆弱點，供讀者參考。

目前幾乎所有 CI 運轉均由電腦化控制 ICS 來運作，因此 ICS 安全關係到國家的戰略安全；圖為航空交通管制設施，亦與 ICS 運作息息相關。

早期設計的 ICS 都是在封閉性獨立環境中使用，然現今系統大多會以網路互聯，隨著資訊技術的進步，資安威脅亦急遽提升。

工控系統脆弱點　影響國家安全

脆弱點（弱點）是指資訊系統、系統程序，控制或威脅來源可以被利用來使原設計之功能無法達成。911 事件後，美國國家科學院研究調查指出，目前美國幾乎所有 CI（電力、水源、交通、通訊與能源供應等）運轉均由電腦化控制 ICS 來運作，因此 ICS 安全可說關係到國家的戰略安全。

一般來說，**ICS 所面臨的安全風險，主要來自早期設計的 ICS 都是在封閉性獨立環境中使用**，並未設想到會以網路互聯，所以較少考量資安上的防護。而在網路開源社群興起與各類攻擊方法精進下，讓有心人士有更多管道能取得這些封閉性系統內的相關資訊；復以 ICS 掌握著許多國家的重要基礎建設，當然也就成為敵對國家網軍，或極端勢力的攻擊目標。

綜前所述，工業自動化生產領域在享受開放、資訊技術及網際網路技術帶來的進步、生產率提高與利益大大增強的同時，也面臨著越來越嚴重的安全威脅。

美國工業控制系統網路緊急應變小組（ICS-CERT）於 2016 年曾進行評估顯示，ICS 弱點包含邊界防禦、功能管理（最小功能）、認證機構管理（授權管理）、身分識別與驗證、最低權限以及資源分配等 6 大弱點，其中又以邊界保護不足為最普遍的弱點。

美國 NIST 的 ICS 脆弱點分類

美國國家標準暨技術研究院（National Institute of Standards and Technology, NIST）針對 ICS 之弱點，於政策面與程序面、架構面與設計面、配置面與維護面、實體面、軟體發展面以及通訊與網路架構面等面向均提出看法，說明如下（整理自 NIST SP 800-82 第 2 修訂版）：

一、ICS 政策面與程序面弱點

（一）**ICS 之安全政策不足**：ICS 弱點通常源於政策不足或缺乏。

（二）**缺乏 ICS 安全訓練意識宣導**：沒有具體 ICS 政策與程序來進行宣導或訓練，將無法期待員工可維持安全之 ICS 環境。

（三）**缺少或缺乏 ICS 設施執行指南**：設備執行指南應該保持最新狀態，並且隨時可用。

（四）**缺乏安全政策執行之行政機制**：執行安全的工作人員應負責管理文件化之安全政策與程序。

（五）**缺乏對 ICS 安全控制之審查**：應透過程序及時間表，確認安全程序被正確地執行。

（六）**沒有 ICS 緊急應變計畫**：缺乏緊急應變計畫將導致停機時間延長與生產損失。

ICS 設施執行指南應保持最新狀態，並隨時可用；且執行安全的工作人員應負責管理文件化之安全政策與程序。

（七）**缺乏配置變更管理政策**：導致無法管理高度脆弱的硬體、韌體與軟體。

（八）**缺乏適當的存取控制政策**：存取控制實施取決於策略是否正確地模擬其角色、職責與授權。

（九）**缺乏足夠之認（驗）證政策**：沒有認證政策，未經授權的存取更有可能發生。

（十）**事件檢測與回應計畫與程序不足**：快速檢測事件能減少損失與破壞，故須保留數位鑑識證據，降低被利用的弱點數與恢復 ICS 正常服務。

（十一）**缺乏關鍵組件之備援（份）**：缺備援（份），導致發生故障可能性增加。

二、ICS 架構面與設計面弱點

（一）**架構與設計之安全性考量不足**：設計時即應將安全性納入 ICS 架構中，包含使用者的識別與授權，存取控制機制，網路拓撲以及系統配置完整性。

（二）**允許不安全架構之演變**：ICS 的網路基礎設施經常依據業務需求進行開發與修改，須考慮因變更而產生潛在的安全影響。

（三）**沒有定義安全邊界**：沒有明確定義 ICS 的安全邊界，就無法確保安全控制被部署或正確配置，將可能導致未經授權的存取發生。

數位鑑識分析取決於收集和保留足夠的資料，如果沒有正確的資料收集，可能無法找出安全事件發生的原因。

（四）**非控制流量的控制網路使用**：控制與非控制流量具不同的要求，因此，若在單個網路上同時擁有兩種流量使得網路配置更加困難。例如，非控制流量可能會無意中消耗控制流量需求的資源，從而導致 ICS 功能中斷。

（五）**ICS 網路未提供網路控制服務**：ICS 網路所使用的 IT 服務如 DNS 及 DHCP，可能無法符合 ICS 所需的可靠性與可用性。

（六）**事件資料收集不足**：數位鑑識分析取決於收集和保留足夠的資料，如果沒有正確的資料收集，可能無法找出導致安全事件發生的原因。

三、ICS 配置面與維護面弱點

（一）**硬體、韌體與軟體未受配置變更管理**：缺少配置變更管理程序可能導致安全漏洞產生，為了妥善保護 ICS，應準確列出系統中的資產及其目前配置設定。這些程序對於營運持續與災害復原計畫至關重要。

（二）**作業系統與供應商軟體修補，直到安全漏洞被發現後才執行**：由於 ICS 軟體與基礎 ICS 間的緊密結合，變更時必須經歷耗時的回歸測試；此測試和之後發布更新軟體需要時間，因此提供了長時間的漏洞。

（三）**作業系統與應用程式沒有被維護，或供應商拒絕修補弱點**：過時的作業系統和應用程式可能包含漏洞；安全修補程序甚至可能不支援於過時作業系統的 ICS。

（四）**安全變更測試不足**：對沒有測試的硬體、韌體與軟體的修改，可能危及 ICS 的正常運作，因此，應發展測試變更的全影響記錄程序。

（五）**不足的遠端存取控制**：ICS 可能需要遠端存取，因此必須加強控制遠端存取功能，以防止未經授權的使用者存取 ICS。

（六）**不當的配置使用**：不正確配置的系統，可能會開啟不必要的連接埠與協議，增加漏洞產生；使用預設配置，通常亦會暴露出漏洞。

（七）**關鍵配置沒有回存或備份**：ICS 配置設定回存程序可防止 ICS 配置資料意外遺失。

ICS 可能會遠端存取，因此須加強控制遠端存取功能，防止未經授權的使用者存取 ICS；且須設定適當的存取控制權限，避免使用者的權限太高或太低，造成運作失衡。

（八）**移動設備資料未受保護**：弱敏感資料（例如密碼）被儲存在筆記型電腦和行動裝置內，當這些設備遺失時，系統安全性可能受到損害。

（九）**密碼的產生、使用與保護沒有依據政策執行**：違反密碼政策與程序可能會增加 ICS 漏洞產生。

（十）**不足的存取控制應用**：指定不當的存取控制，可能導致 ICS 使用者的權限太高或太低。

（十一）**不正確的資料鏈結**：ICS 資料儲存系統可能與非 ICS 資料源相連，可能導致資料從某個資料庫被自動複製到其他資料庫。

（十二）**未安裝或更新惡意程式防護措施**：惡意程式防護措施必須被安裝與更新至最新之病毒碼。

（十三）**未充分測試惡意程式保護措施**：在沒有充分測試惡意程式保護措施的狀況下，可能會影響 ICS 的正常運作。

（十四）**阻斷服務**：ICS 軟體可能容易受到 DoS/DDos 攻擊，導致經授權的存取系統被阻止或系統功能被延誤。

（十五）**沒有安裝入侵偵測（防禦）系統**：IDS（IPS）軟體可以防止各種攻擊，包括 DoS 攻擊，並識別受攻擊主機，例如感染蠕蟲的內部主機。

（十六）**沒有維護日誌**：沒有正確維護日誌，導致無法追查安全事件發生原因。

四、ICS 實體面弱點

（一）**未授權之人員可實際存取設備**：ICS 設備存取應僅限於必要人員。

（二）**射頻、電磁脈衝（EMP）、靜電放電、停電和用電尖峰**：ICS 硬體易受射頻、EMP、用電量影響，導致指令中斷，或對電路板的永久損壞。

（三）**缺乏備用電源**：沒有備用電源，一但停電將導致 ICS 關機。

（四）環境控制的喪失：溫度與濕度變動，可能導致 ICS 損壞。

（五）不安全的實體連接埠：不安全的連接埠，會讓未經授權的 USB 儲存設備連接。

五、ICS 軟體發展面弱點

（一）不正確的資料驗證：當 ICS 軟體無法正確驗證使用者輸入資料時，可能導致緩衝區溢位、命令注入以及目錄路徑穿越漏洞等。

（二）預設狀況下，未啟用安裝的安全功能（SIS）：若未啟用或至少被識別已被停用，那麼與該產品一起安裝的安全功能將無效。

（三）認證、權限與存取控制不足：未經授權存取配置和程式軟體將可能會損壞設備。

ICS 硬體易受用電量影響導致指令中斷，須確保備用電源充足，避免停電導致 ICS 關機。

六、ICS 通訊與網路架構面弱點

（一）未使用資料流控制：資料流控制能允許哪些資訊流通，防止資訊洩露。

（二）防火牆不存在或配置不正確：缺乏正確配置的防火牆，使敏感資料受到竊取。

（三）防火牆與路由器紀錄不足：沒有維護日誌，導致無法追查安全事件發生之原因。

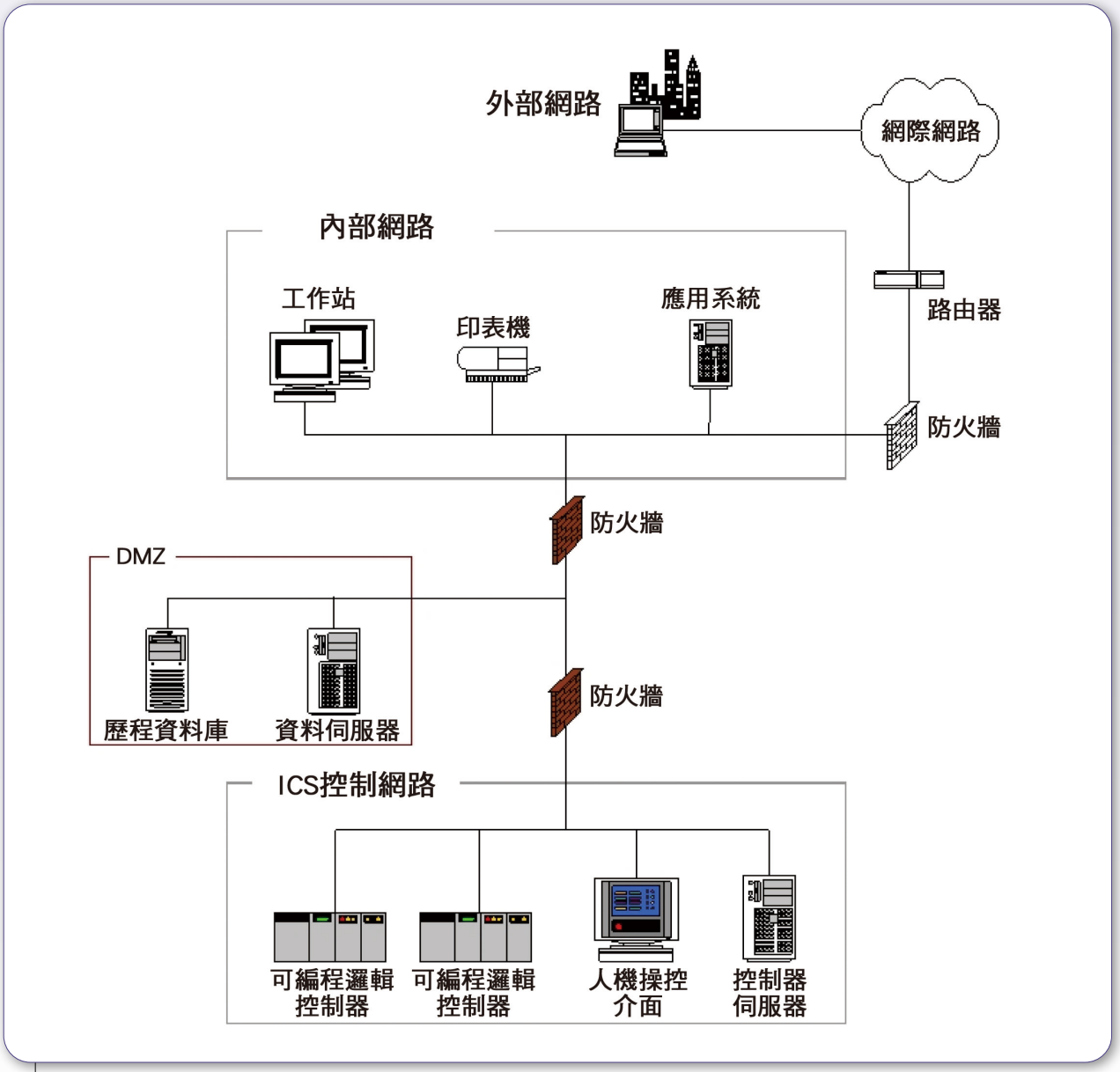
（四）標準、通訊協定使用明文傳輸：透過 ICS 網路活動的監聽，可以解碼資料傳輸。

（五）使用者、資料或設備的驗證不符合標準或不存在：許多 ICS 協議沒有任何級別的驗證，沒有身分驗證，會導致資料錯誤或欺騙設備的情況發生。

（六）使用不安全的 ICS 協議：ICS 協議通常具有很少（或沒有）安全功能，例如身分驗證和加密，會導致額外漏洞產生。

（七）缺乏完整性的通訊檢查：大多數 ICS 協議中沒有完整性檢查，為了確保完整性，ICS 可以使用提供資料完整性保護的低層協議（例如 IPsec）。

（八）缺乏無線網路使用者與存取點間的認證：需在無線使用者端和存取點之間進行較強的相互認證，以確保使用者端不會連接到惡意無線基地臺。



單一防火牆在遭受大量攻擊時，可能面臨功能喪失或效能降低等情況，建議架設兩道防火牆，分別對內部網路與ICS 控制網路進行封包過濾，強化安全防護能量，提升防禦能力。（資料來源：NIST, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82.pdf；國土安全辦公室，https://ohs.ey.gov.tw/Page/6C4A1386ACBA6734）

（九）無線使用者端與存取點間的資料保護不足：敏感資料在無線使用者端和存取點間應使用強化加密來保護，確保競爭對手無法獲得未經授權的存取。

結論

「知己知彼，百戰百勝」，故 ICS 保護必須滿足兩個要求，即**安全性（Safety）**—**知道自己的弱點**，及**可用性（Security）**—**如何保護自己免受傷害**。