# 強化
# 關鍵基礎設施的網路安全

■ 華梵大學資管系特聘教授　朱惠中
健行科技大學資管系助理教授　陳惠娟

趨勢科技於 2015 年提出「美洲關鍵基礎建設網路安全」（Cybersecurity and Critical Infrastructure in the Americas）報告，於全球 20 個國家的政府與民間企業進行調查，提出「53% 的受訪者認為去年專門針對 CI 的網路攻擊比以往更多」、「44% 的受訪者認為他們曾遭到惡意的刪除與破壞式攻擊」。[1]

[1] http://www.trendmicro.com/us/security-intelligence/research-and-analysis/critical-infrastructures-security/index.html; http:/www.trendmicro.com/us/security-intelligence/research-and-analysis/critical-infrastructures-security/index.html





## 背景

在傳統上，營運技術（Operation Technology, OT）與資訊技術（Information Technology, IT）分屬兩個不同的專業領域，彼此間鮮少交集，但隨著網際網路與 IT 的精進與普及，OT 與 IT 環境之間的專屬領域（Segmentation）已逐漸消失，原本與外界網路實體隔離的工業控制系統（ICS）逐漸必須與企業網路整合，利用 IT 在數據存儲、處理和通信方面的能力，來降低成本與風險，及提升效能與靈活度。

惟水可載舟，亦可覆舟，當不安全且含有漏洞的企業網路一旦與工控系統之專屬網路相連後，將使得工控系統暴露在網路攻擊的危險當中，越來越多原本以 IT 環境為目標的複雜網路威脅或攻擊行為，開始滲透到包括工控系統在內的 OT 環境。當此趨勢來臨後，使得仰賴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，受到網路攻擊的可能性大增，特別是進入工業 4.0 時代，原本可透過物聯網、大數據與雲端智慧，使 IT 與 OT 兩者終能展開對話，由 OT 領域的感測器獲取資料，上傳 IT 領域的雲端中心執行大數據分析，繁衍各種創新應用的目標將無法達成。


工業 4.0 的時代來臨，原可透過物聯網、大數據與雲端智慧繁衍各種創新應用，卻恐因為資安漏洞造成危機。

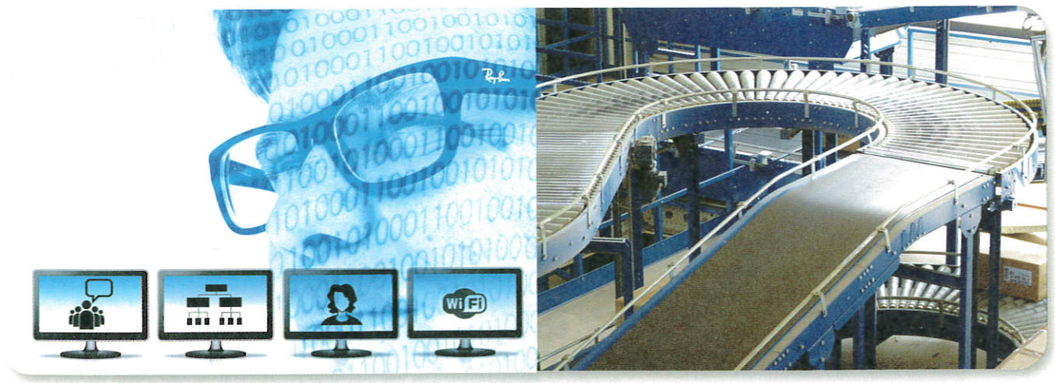
## 如何將 IT 與 OT 整合

整合 IT ／ OT 所需解決的問題，大致上可分成組織面及技術面二類：

### 一、組織面的問題

（一）獨立的企業過程（Business Silos）

組織方面的問題源起於 IT ／ OT 的系統、人力之間皆有各自的體系，IT 系統由 CIO（Chief Information Officer）指揮，負責公司資產、工作流程管理等等，含括電子商務（e-Commerce）、企業資源規劃系統（ERP）、供應鏈管理系統（SCM）、顧客關係管理系統（CRM）、產品生命週期管理系統（PLM）等工作；而 OT 系統則由 COO（Chief Operational Officer）主導，負責 CI 的實體操作與監控，一般而言，泛指與工廠營運相關的技術，主要涵蓋三個類別：一是自動化；二是自動化整合搭配操作流程整合；三是工廠自動化與資訊技術的整合，諸如製造現場控制（Shop Floor Control, SFC）、製造執行系統（Manufacturing Execution System, MES）、監視與整合控制（Supervisory control and data acquisition, SCADA）等工廠資訊系統，此類系統需與上列 IT 系統進行整合，若雙方各自為政，將難以結合；另在串聯資訊技術與工業現場實體世界的過程中，感測器（Sensors）扮演不可或缺的要角。為了完善整合 IT 與 OT，在策略上 CIO 與 COO 須達成一致。[2]



IT 系統含括電子商務、企業資源規劃系統、顧客關係管理系統等工作；OT 系統負責 CI 的實體操作與監控，涵蓋工廠自動化與操作整合系統等。

（二）文化上的衝突（Culture Clash）

IT 部門往往是成本中心，需配合與支持企業客戶，故其政策和規則因須配合客戶需求，必須要做客屬化，亦即可能會建立自己的標準作業程序，以符合客戶需求。依此，他們只需依照與客戶簽訂的服務協議進行，如發生非計畫停電時，按業務維運中斷程度處理即可。至於 OT 部門，在大多數情況下是核心業務，人員配置需反映 24x7（全年無休）的關鍵性質基礎設施，系統往往預計會不間斷持續運行數十年，故計畫外的中斷需按預先設定相關的程序啟動，以維持正常運作。

總而言之，OT 人員存有零故障的期望，而 IT 人員則強調靈活性和速度，一個成功的整合必須考慮到雙方的要求。

（三）風險容忍度（Risk Tolerances）

IT 系統下線或當機，往往僅會影響公司的正常運作，而 OT 系統（如電力）下線或當機，則很有可能影響所有用戶的安全；因此，許多 IT 系統視為常態保養的行為，如防火牆更新、系統維護等等，在 OT 系統上則認為是會有相當大的風險，故在整合雙方時，勢必需要列入考慮。[3]

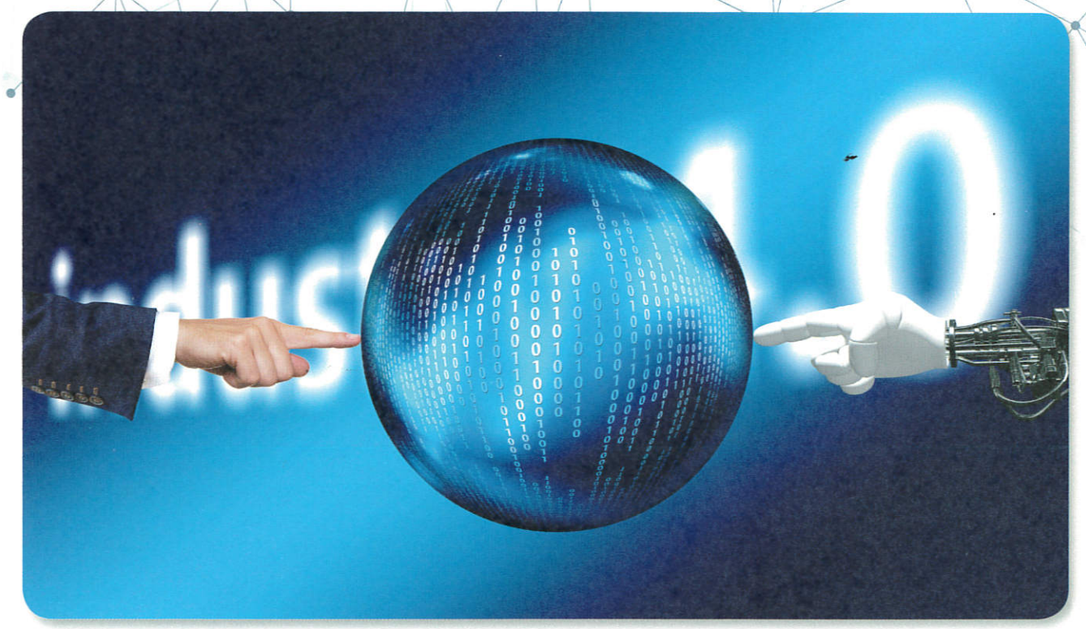
### 二、技術面的問題

（一）環境性（Environmental）

IT 設備的日新月異，代表其生命週期通常相對較短，一台主機可能使用 5 年就被淘汰；但 OT 設備正好相反，相較於 IT 設備，其可靠性和完整性是 OT 的主要考慮因素。

（二）相容性（Compatibility）

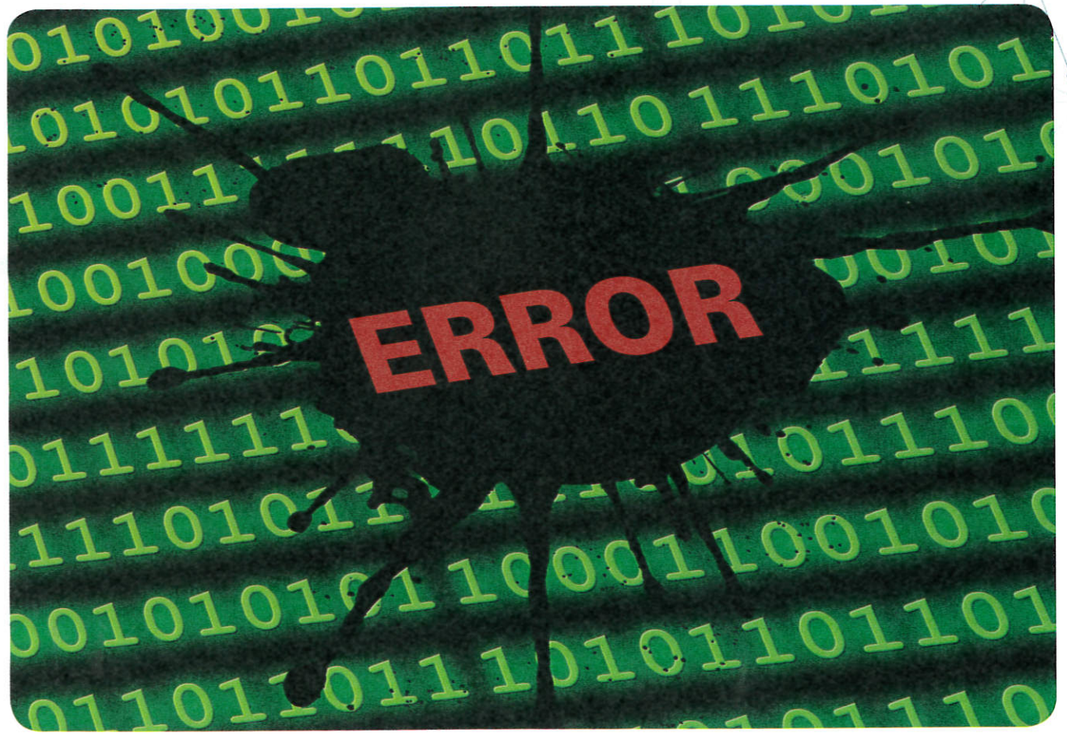
隨著 IT 技術的成熟，鑒於各式軟硬體相容性的問題，導致驗錯功能需求的產生。



OT 與 IT 系統需進行妥善整合，避免雙方各自為政，策略上也將仰賴 CIO 與 COO 協調與共識。

[2] 魏于寧，「整合 IT、工控與通訊 加速落實工業 4.0 轉型」，DigiTimes 物聯網，2016-03-28

[3] Atos, White Paper: The convergence of IT and Operational Technology, 2012




IT 設備的錯誤，往往會影響 OT 設備的正常運作。

OT 系統因為輸入、輸出均為特定格式及設備本身為專屬產品，因此，相容性之要求不高，故 IT 設備的錯誤（Bug），往往會影響 OT 設備的正常運作。

（三）跨領域人才短缺（Skills Shortage）

IT 與 OT 雙方的技術背景具有相當的差距，故具有橫跨領域的技術與經驗，且有能力接手整合後的系統人才極端缺乏。

（四）資安需求（Security）

OT 系統以前均侷限於工廠內部或是鄰近地區，故無防範外部威脅的需求，一旦與 IT 系統整合，便必須防範因使用 IT 由外界造成相對應的威脅。

## 結論

### 一、為何要將 IT 與 OT 合併

IT 之技術在其重點領域，即數據存儲、處理和通信等方面已經取得巨大的進步，相較之下，OT 大部分的進展都是在專屬的系統與程式中，造成非專業人士難以理解這些專業工作環境，故難以整合多種相關的技術和提供商。隨著公司的全球化與競爭的日益激烈，IT ／ OT 的整合將具有以下的優點：

（一）降低成本（Cost Reduction）

利用類似技術、標準來治理 IT 和 OT 的原則，公司不再需要維持兩套不同的規範。





（二）降低風險（Risk Reduction）

IT ／ OT 整合意味著資安問題可以利用整合 IT ／ OT 的方法處理，這對防禦外來入侵提供進一步的保護。

（三）提升效能（Performance Enhancing）

IT ／ OT 整合能節省時間和成本，縮短新產品開發完成到上市的時間，減少經濟廢品。

（四）提升靈活度（Flexibility Gaining）

IT ／ OT 整合將會提供更好的透明度，優化成本和調整成本結構；公司也會變得更加靈活，加速製造所在地的轉移。[4]

### 二、整合 IT 與 OT 需克服的困難

（一）發展 IT ／ OT 聯合組織和治理結構。

（二）共同管理 IT 和執行 OT 跨技術項目。

（三）協調、匯總重複的過程，精簡程序。

（四）發展跨 IT ／ OT 領域的技能，培養了解雙方需求和要求的人才。

（五）IT 與 OT 之間責任的分擔（特別在安全方面）。

（六）聯合管理現在不同的基礎設施，以方便未來的整合。

[4] Atos, White Paper: The convergence of IT and Operational Technology, 2012
Derek R. Harp and Bengt Gregory-Brown, IT/OT Convergence --IBridging the Divide, NextdefenseT