出國報告（出國類別：開會）

參加美國亞特蘭大工業控制系統（ICS）資安研討會出國報告書

服務機關：數位發展部資通安全署

職稱姓名：資安制度工程師郭哲維

分析師陳思翰

派赴國家：美國

出國期間：113 年 10 月 20 日至 10 月 27 日

報告日期：114 年 1 月

摘 要

SecurityWeek 的工業控制系統（ICS）資安研討會是美國規模最大、持續舉辦最久的研討會，該會議長期關注工控系統之資通安全。自 2002 年以來，聚集了各行各業包含科技、醫療、運輸、傳統產業等 ICS 維運機關及企業 ，並吸引全球相關營運和控制工程師、IT、政府、供應商和學者與會。

ICS 資安研討會係訂於本（113）年 10 月 21 至 24 日於喬治亞州亞特蘭大巴克海特洲際酒店舉辦，會議共分為 ICS 網路安全、OT 網路安全管理、人工智慧、數位轉型和新興威脅等共 87 個議題，本報告說明本屆會議重點及發現，並提出與會心得與建議，作為主管機關日後推動工業控制系統資安政策及規劃等相關工作之參考。

目 次

目錄

圖目錄

壹、簡介與目的

美國 2024 亞特蘭大工業控制系統（ICS）網路安全會議是全球工業網路安全領域的指標性論壇，於 2024 年 10 月 21 日至 24 日舉行。此次為期四天的會議匯聚了來自各行業的專家和領袖，深入探討工業網路安全的最新挑戰、解決方案及未來發展方向。自 2002 年創辦以來，該會議每年公開徵集與 ICS 安全相關的議題，並邀請全球學者和業界專家投稿研究成果，以解決全球 ICS 運營面臨的核心問題。

本屆會議討論的主題包含不同構面，如不斷升級之網路威脅、工業執行環境的限制，以及 ICS 專業人才短缺的現實挑戰。會議特別專注於如何保護如資料採集與監控系統（SCADA）、工廠控制系統、工程工作站、變電站設備及可程式邏輯控制器（PLC）等工業設備，隨著數位化轉型的推進和網路威脅形勢的演變，這些設備的保護至關重要。透過專家演講、案例分析及技術展示，為我國在工業控制方面提供有效的安全解決方案，降低 ICS 運營的風險與挑戰。

圖 1 演講設計與座位規劃，資料來源：自行拍攝

與會者來自全球各地，涵蓋從大型工業組織、政府和軍事機構到地方和區域性公用事業公司的專業人士。代表的產業範疇廣泛，包括製造、發電、輸配電、水務管理、化學、石油與天然氣、管道運輸、資料中心及

醫療設備等。參與者多為控制系統的使用者，如控制工程師、營運管理人員及網路安全專業人士。透過會議，能更好地了解當前網路威脅的態勢，並學習來自世界各地的成功應對策略，從而改進各自的安全架構。

各國供應商參與也是會議的重要亮點，多家技術供應商展示了針對 ICS 的最新安全技術，包括資產掃描偵測系統、身份管理解決方案及網路隔離技術等。這些創新工具為參與者提供了多元化的選擇，幫助企業組織提升其網路防護能力。同時，會議也強調實戰經驗的重要性，透過分享成功案例，參與者能了解實際應用中的挑戰與解決方案，為自己的運營環境提供有效的參考。

圖 2 供應商攤位，資料來源：自行拍攝

會議同時為跨產業人員的合作與交流提供了獨特的機會，參與者不僅能獲得最新的技術知識和實用策略，還能通過與同行的交流與合作，推動行業標準的完善與執行，透過與來自不同領域的專家交流，參與者能建立廣泛的合作網路，促進資源與技術的共享。這種跨領域的合作不僅能解決個別企業的問題，還能為整個產業提供更強有力的支援。

工業控制系統網路安全會議作為全球頂級論壇，不僅是技術與經驗的交流平台，更是提升全球工業基礎設施安全性的重要驅動力。透過分享知識、促進合作及推動創新，會議為應對不斷演變的安全挑戰提供了堅實支持，也為未來工業發展奠定了更穩固的基礎。

貳、會議過程

一、會議日期：2024 年 10 月 21 日至 10 月 24 日，共計 4 日

二、會議地點：美國亞特蘭大

三、會議重點摘要場次表：

日期	參加場次
10 月 21 日	Building Robust Enterprise OT Cybersecurity Programs: Lessons from the Field
	Getting Started with ICS/OT Penetration Testing
10 月 22 日	The Evolving Future of OT Network Defense: Lessons from National Security
	Responding to and Recovering from an OT Cyber Incident
	Where OT Passive Monitoring Projects Fail – Top 5 Lessons from the Field
	Dynamic OT Inventory; Learnings From an Application Installation
10 月 23 日	It's Raining SBOMs: What to Do with Them Once You've Got Them
	Zero Trust Approach for Secure ICS/OT Operations: Addressing 62443, NIS2, and Compliance Needs
	Security and Safety Challenges of Integrated Control and Safety Systems (ICSS) in OT
	OT, the More Things Change, the More They Stay the Same
10 月 24 日	Securing the Future: Advanced Strategies for OT GRC in Industrial Control Systems
	Overview of OT Technology Trends and Challenges

四、會議重點摘要

(一) 建立強大的企業 OT 資通安全計畫：來自實戰的經驗教訓（Building Robust Enterprise OT Cybersecurity Programs: Lessons from the Field）

1. 講者：Mohammed Saad

 Mohammed Saad	Mohammed 為 OT 資通安全和工業自動化領域的全球領導者，作為 InnovAKT LLC 的創始人，領導團隊為廠商及企業提供 OT 資通安全諮詢，制定了全球 OT 資通安全計畫，並為保護關鍵基礎設施做出了貢獻。

2. 重點摘要：

講者 Mohammed 在會中介紹了企業 OT 資通安全計畫，以及它與傳統 OT 安全方法的區別，藉由實務經驗的分享，讓聽者了解強化 OT 資安計畫的步驟，包括培養以安全為中心的文化，確保持續監控和改進，以及應對新興威脅和技術，以下是會議中關注的重點：

(1) OT 資通安全的重要性與挑戰：

由於 OT 環境的特殊性，傳統 IT 網路安全方法並不適用，OT 環境面臨的攻擊日益複雜，影響也越來越大，企業往往缺乏 OT 資安意識，導致資源投資不足或防護的方向錯誤。此外，OT 和 IT 部門之間往往缺乏溝通和協調，進而產生漏洞及風險。

(2) OT 資通安全計畫的關鍵因素：

講者 Mohammed 指出，企業需要進行全面性的風險評估，例如識別關鍵資產、漏洞和威脅，並制定復原計畫，評估的範圍應包含 IT 和 OT 政策、技術架構、組織架構等，結果可藉由成熟度評分、風險評分及復原建議等來顯示。另講者建議企業應該建立卓越中心（Center of Excellence），藉由 IT 和 OT 專家組成的團隊，負責制定政策、標準、培訓和技術創新，並建立 SOC 機制，提高監控和事件應變能力之效率和安全性。

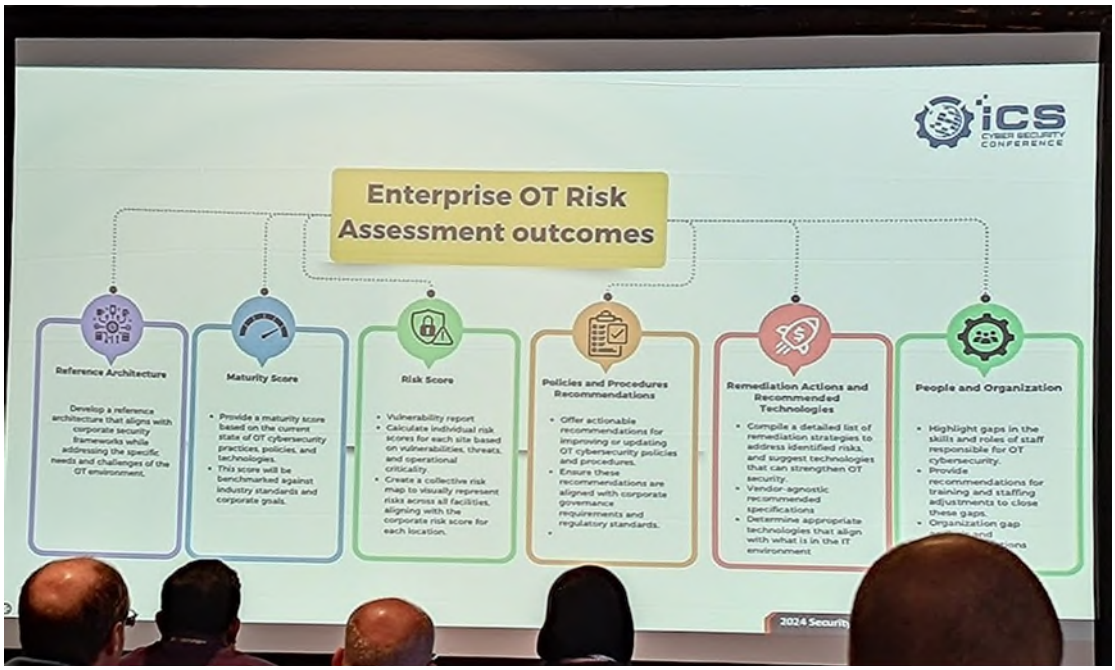

圖 3 企業 OT 風險評估結果，資料來源：現場照片

(3) 如何讓計畫有效施行：

講者 Mohammed 指出計畫能有效施行的關鍵在於企業高層級領導的支持，如何說服高層了解 OT 資通安全的必要性，並願意投資人力及資源在防護需求上，這需要透過 OT 資安專家的協助。並透過教育及培訓，提升企業員工資安意識，減少組織間知識差距，將網路安全目標與業務目標相結合，建立企業安全文化，使 IT 與 OT 有共同合作的環境。

(4) 配合在地法令調整：

隨著不同國家 OT 法令要求不同，企業應考量在地化經營之風險管理，在某些國家因為資安法令嚴謹，OT 資安發展速度較快，能達成一定的成熟度，並定期進行風險評估；惟在缺乏強制性規範之國家可能導致企業對 OT 網路安全重視程度不足，企業仍應考量如何提升資安防護量能。

(二) ICS/OT 滲透測試入門（Getting Started with ICS/OT Penetration Testing）

1. 講者：Mike Holcomb

 Mike Holcomb	Mike Holcomb 是 Fluor 公司網路安全研究員也是 ICS/OT 全球網路安全負責人員，於 Greenville 技術學院的網路學位課程撰寫且教授六門網路安全課程，擁有 CISSP、GRID、GICSP、ISA 62443、GPEN、GCIH 等國際證照。

2. 重點摘要：

講者 Mike 在會中就本身滲透測試與 ICS/OT 安全管控經驗，指出 OT 環境中容易被忽視的安全事項，提醒 OT 安全防護人員應採取的安全措施，並對 OT 系統導入滲透測試作業提供相關建議，避免在導入滲透測試時影響運作中的 OT 系統，以下是 6 點建議：

(1) 滲透測試需避免在生產環境中執行，以防止對系統運作和人員安全造成影響，同時，每個 OT 環境因其獨特性，需要制定量身定制的滲透測試方案。

(2) 攻擊者常利用 IT 系統的漏洞滲透 OT 網路，例如透過遠端存取、USB 裝置或供應鏈端植入軟硬體惡意代碼，內部員工可能因不滿、人員疏忽或外部利誘成為攻擊者的幫兇，使用雲端控管 OT 系統也會增加風險。

(3) 防禦策略包括使用防火牆分隔 IT 與 OT 網路，防範攻擊者突破 DMZ 層。此外，需強化密碼管理，研究指出高達 40%的 OT 系統密碼與 IT 系統相同，避免 IT 和 OT 使用相同密碼，可有效降低 OT 系統端的網路安全風險。

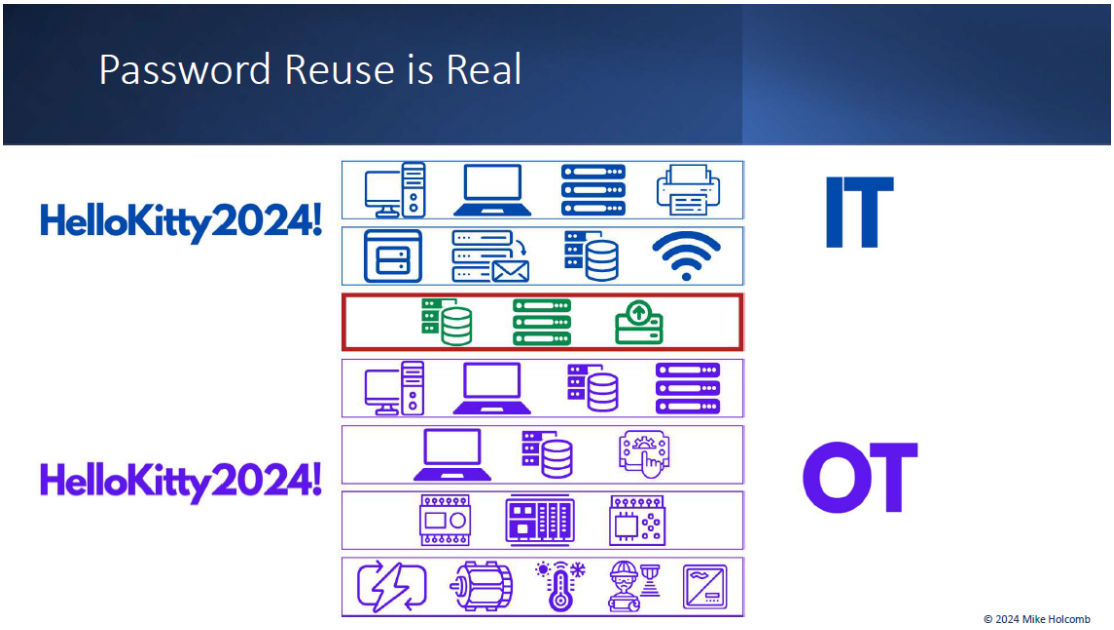

圖 4 IT 和 OT 系統常使用相同密碼，資料來源：講者簡報

(4) 滲透測試的目的是模擬真實攻擊者的行為檢測網路漏洞，滲透測試通常假設攻擊者已入侵 IT 網路並嘗試向 OT 網路滲透，但需特別留意滲透測試檢測的範圍，避免對運作中的 OT 系統造成影響。

(5) 攻擊者在入侵 OT 網路後會繪製網路架構圖並尋找 OT 系統控制系統元件（如 HMI、PLC、DCS 等），他們可能利用 OT 設備安全設計相同的特性，能更快速取得高層級的權限，並設法隱匿在系統中。

(6) Dragos 年度報告記錄了 ICS 和 OT 的安全威脅與攻擊模式，為網路安全相關人員提供重要參考。例如 Colonial Pipeline 勒索攻擊事件，顯示出 OT 網路的脆弱性和威脅的緊迫性。

講者最後建議要強化 OT 系統安全，安全人員也需要瞭解攻擊技術，例如：權限提升和遠程代碼執行能力以提升其防禦能力。此外，需加強對 OT 網路的監控和威脅識別，僅靠現有平均約 5%的網路監控覆蓋率遠不足以應對當前挑戰。

圖 5 會議過程，資料來源：現場照片

(三) OT 網路防禦的未來演進：國家安全之經驗（The Evolving Future of OT Network Defense: Lessons from National Security）

1. 講者：Tim Fahl

 Tim Fahl	Tim 為 OWL Cyber Defense 公司網路防禦的首席技術長，擁有超過 15 年的跨域解決方案（Cross-Domain Solutions）經驗，並為政府從軟硬體工程設計、建構和部署防護系統。

2. 重點摘要：

講者 Tim 在會中強調了 IT（Information Technology）與 OT（Operational Technology）於資安領域所面對的挑戰，需採取不同措施來因應，探討美國政府的網路安全模型如何指導 OT 防禦策略，並從網路防禦中吸取經驗教訓，實施最新的資安準則和最佳實踐，來強化 OT 系統抵禦不斷變化的威脅，確保關鍵基礎設施的安全性和可靠性。以下是會議中關注的重點：

(1) OT 網路的獨特挑戰：

OT 網路往往涉及到工業控制系統和其他關鍵基礎設施，這些系統的安全性維繫了國家安全和經濟穩定。隨著 IT 和 OT 越來越密不可分，系統面臨連網後的網路安全漏洞，使得機關難以保護這些系統運作。

(2) 國家安全的經驗：

講者 Tim 指出，美國政府的網路安全作法可以有效地應用於 OT 防禦中。例如防禦深度（Defense-in-Depth）和零信任架構（Zero Trust Architecture）是現今保護關鍵基礎設施的策略之一。這些策略強調了多層次的安全防護和持續的身份驗證，確保只有經過驗證的用戶和設備才能登入系統。

(3) 資料串流的控制：

實行嚴格的資料串流控制是保護 OT 和 IT 之間資料傳輸的關鍵。這包括使用跨域解決方案（Cross-Domain Solutions）和單向閘道（Data Diodes）來管理不同安全級別之間的資料傳輸，進而降低外部威脅的風險。

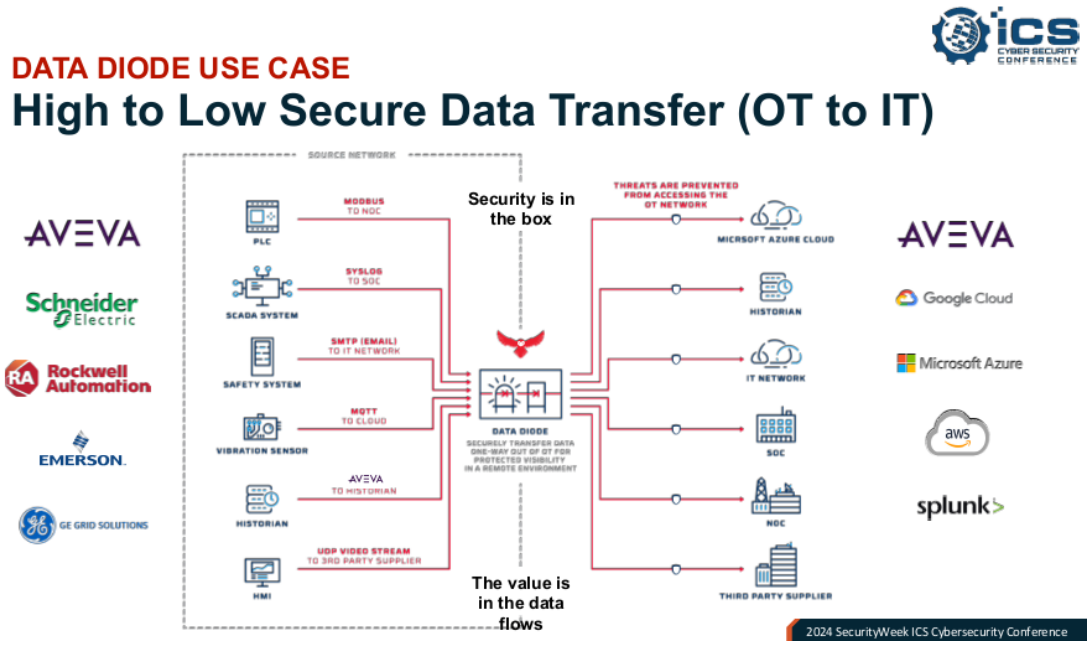

圖 6 單向閘道（Data Diodes），資料來源：講者簡報

(4) 網路分段：

講者 Tim 強調了網路分段的重要性，這可以限制潛在安全漏洞對整個系統的影響。透過將關鍵基礎設施網路進行隔離，減少橫向移動的風險，進而提高整體安全性。

(5) 各行業的監管：

隨著越來越多的能源、醫療和交通等行業採用美國政府的安全框架，機關需要建立符合自身需求的安全資料傳輸架構，以保護 OT 網路時，亦能保持營運效率。

圖 7 會議過程，資料來源：現場照片

(四) OT 網路事件的應對與復原（Responding to and Recovering from an OT Cyber Incident）

1. 講者：Michael Powell、Stephanie Saravia

	Michael Powell 博士是美國 NIST 國家網路安全卓越中心（NCCoE）的網路安全工程師。他的研究重點是製造業的資通安全，特別是工業控制系統。

Michael Powell	
 Stephanie Saravia	Stephanie Saravia 是 MITRE Corporation 的首席 OT 網路工程師。在過去的 3 年裡，她為多個政府機關提供支援，包括 NIST 和 NCCoE。主要研究無線技術、安全系統及其網路以及工業控制系統網路安全。

2. 重點摘要：

在會議中，講者 Michael 介紹 NCCoE 的工作流程，以及 NCCoE 與產業界和學術界的合作，如何發現網路安全問題並尋求解決方案。他指出小型製造業應建立有效的資安事件應變和復原計畫，以提高資安韌性。以下是會議中關注的重點：

(1) 事件應變計畫（IRP）的重要性：

講者 Stephanie 強調了制定資安事件應變計畫的必要性，特別是對於小型製造業。這些計畫不僅能幫助企業在發生資安事件時能迅速反應及復原，亦能降低對企業帶來的營運衝擊。他提及企業應該建立專業團隊來開發和施行這些計畫，並確保所有相關人員接受必要的培訓。

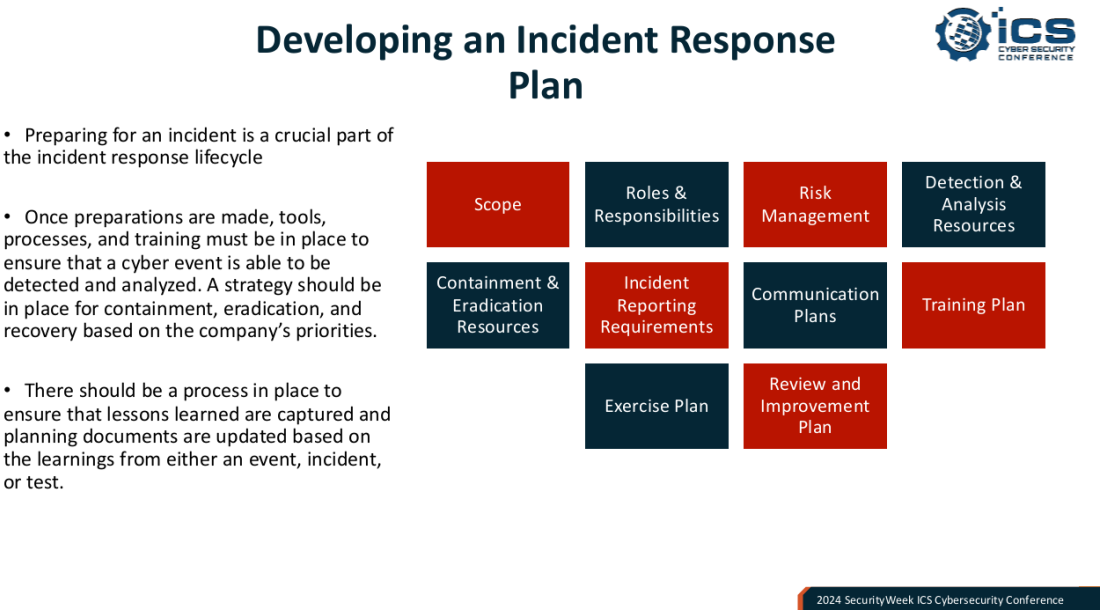

圖 8 事件應變計畫（IRP），資料來源：講者簡報

(2) 簡化的指導方針：

NCCoE 正在開發一份白皮書，協助小型製造商提供簡化的應變和復原計畫指導方針。這份白皮書將涵蓋「角色與責任」（R&R）的生命週期，並提供最低限度的要求，幫助企業在計畫中考量資安的潛在威脅。

(3) 實戰演練和測試：

講者 Stephanie 強調了資安攻防實戰演練的重要性。通過模擬各種網路攻擊場景，企業可以檢驗其應變計畫的有效性，並在真實事件發生前，進行必要的資安防護及調整。會議中列舉了可能的攻擊場景，如未經授權的命令和參數的篡改，這都是企業需要提前準備的情境。

(4) 資源和參考資料：

NCCoE 提供了多種資源，包括可參照的指引和範例，以幫助企業制定和完善其應變和復原計畫。這些資源不僅能提高企業的準備程

度，其內容還能促進人員對網路安全的認識。

(5) 團隊合作：

強調 IT 團隊和 OT 團隊之間合作運行，需要有組織並凝聚共識，兩個團隊需互相配合，來監控及應變資安事件；此外，企業應與供應商建立良好的合作關係，確保系統或實體設備復原時，能夠獲得所需的材料，避免材料短缺造成的困難。

圖 9 會議過程，資料來源：現場照片

(五) OT 被動監控專案失敗的原因：從現場經驗的五堂課（Where OT Passive Monitoring Projects Fail – Top 5 Lessons from the Field）

1. 講者：Peter Morin

	Peter 是 PwC 公司的 OT 網路安全總監，擁有超過 25 年的經驗，專注於 ICS 和關鍵基礎設施，在資訊科技和網路安全方面擁有相關的背景，在快速發展且複雜的營運技術安全領域中擔任顧問一職。

Peter Morin	

2. 重點摘要：

講者提出 5 項被動監控項目在實施過程中常見的失敗原因，並提出了解決方案，目的是幫助企業更有效地部署和運營這些系統，從而提升被動監控效用和資產管理能力。

(1) 對變革的抗拒：

OT 被動監控系統通常由 IT 或資安團隊主導，而非 OT 工程部門。導致 OT 工程部門常出於工作量及營運目標考量，對於安裝此類監控工具或系統的配合度極低。講者提出解決方式在於讓 IT、資安與 OT 工程團隊協同合作，建議監控系統可從 OT 工程團隊的資產管理和營運監控的效益著手，從中間尋找雙方共同需求而非單一方需求，以達到共同目標。

(2) 缺乏對 OT 環境的了解：

許多團隊未在監控專案啟動前先進行 OT 環境調查，導致監控工具在安裝後無法收集相關資料，例如支援無線傳輸的設備、被獨立區隔的網路或由於資產數量龐大而導致系統成本過高或過於耗時等問題。講者建議可透過 PCAP（封包捕獲）工具提前收集網路流量數據，先全面了解網路結構與資產分佈或以實地考察方式並與 OT 工程人員交流，早期發現被忽略的網路環境和潛在問題。

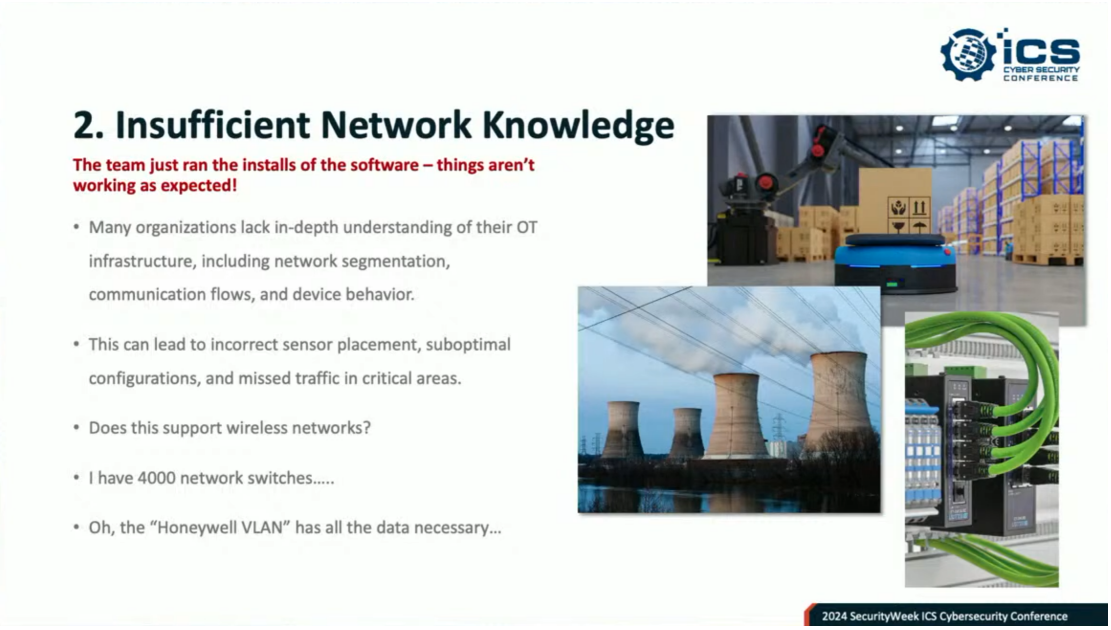

圖 10 缺乏對 OT 環境的了解，資料來源：講者簡報

(3) 輕忽 OT 環境的複雜性：

被動監控系統經常因傳感器部署不當或缺乏完整的權限而無法掃描整個網路。建議可增加傳感器部署，根據網路拓撲合理佈置傳感器避免數據收集盲點，另外對於數據驗證與改進，定期測試監控系統的數據完整性持續調校收集結果。

(4) 與 SOC 整合不足：

被動監控系統若未整合至 SOC（安全監控中心）或其他資安工具，將導致收集的警報數據無法有效利用。建議組織制定應對手冊（Playbooks），並設計分層式回應模型（Tiered Response Model），來提升事件告警的處理效率。

(5) 錯誤的期望：

被動監控工具的收集到的資料往往難以包含韌體詳細資訊，如韌體版本或 CVSS 漏洞評分，這可能不符合初期建置時的期望，講者建議可在特定的範圍搭配主動監控（Active Scanning），例如在特定期間段針對關鍵裝置進行檢測，來取得所需的數據。

圖 11 會議過程，資料來源：現場照片

(六) OT 動態庫存：應用程式安裝的經驗（Dynamic OT Inventory; Learnings From an Application Installation）

1. 講者：Stuart Powell

 Stuart Powell	Stuart 擁有 40 年的專業經驗，涵蓋大學技術教學、專案管理、工業控制系統工程、企業 IT 管理（包括 Unix 和 Windows 系統管理）以及運營技術(OT)安全。在大學教授技術課程，成功管理過多個專案，其專業領域包括工業控制系統的設計、實施和管理，擁有深厚的技術知識。

2. 重點摘要：

講者從自身實際經驗出發，分享了在製造業環境中推行動態資產管理及提升網路安全的經驗，強調識別和管理 OT 資產是提高網路安全的重要一步且過程經常充滿挑戰。

(1) 資產可視化的重要性：

講者多次強調：「你無法保護你看不到的資產。」要改善 OT 網路

安全首先要意識到 OT 網路安全是長期需求，其中資產識別是最重要的一環，並說明成功的資產管理必須從人工手動盤點逐步轉換為自動化的動態盤點。

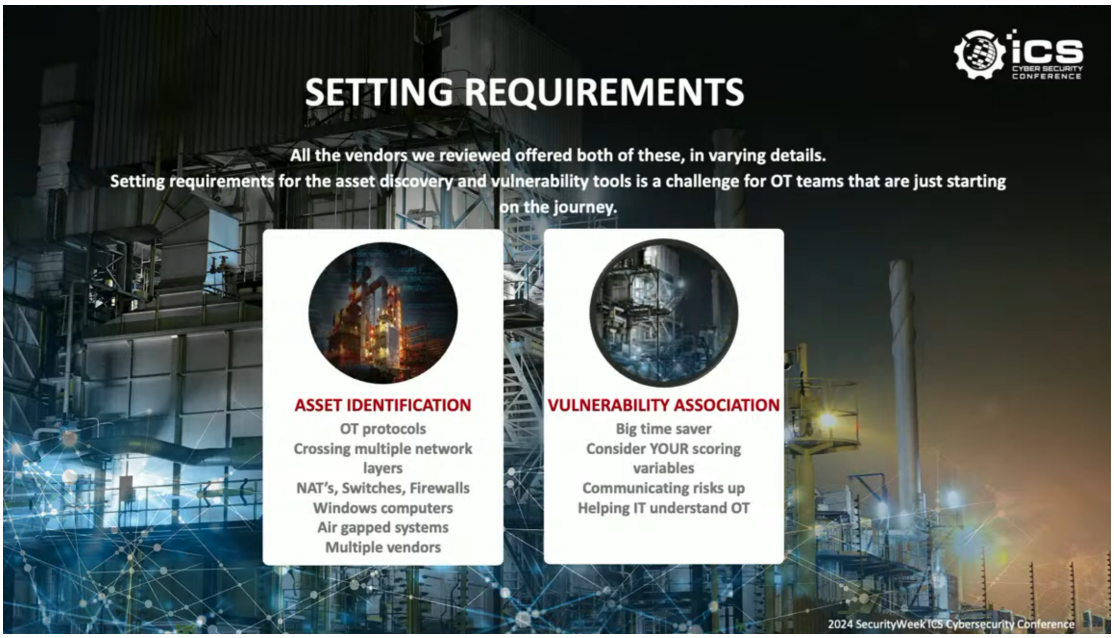

圖 12 資產盤點的注意事項，資料來源：講者簡報

(2) 手動盤點庫存的局限與過渡：

手動盤點庫存是資產管理的基礎，但存在更新困難、維護耗時等問題，講者建議組織先從各站點手動清單入手進行資料格式標準化，為未來自動化建立基礎，動態庫存應用程式能通過被動監控設備流量，提供更完整的資產視覺化圖表，但動態庫存收集的資料格式需要在初期明確規劃，避免收集過多雜亂且不必要的資訊。

(3) 動態庫存的挑戰：

不同 OT 協定間的差異帶來挑戰，特別是在不同站點使用多種 OT 協定的情況下，動態庫存盤點應用程式對不支援的協定處理能力需要特別評估。此外，因複雜網路架構包括多層次網路架構和邏輯隔離將增加資料收集的難度，因此講者建議在部署前進行充分規劃並

與供應商協商解決方案。在設備兼容性方面，則需特別注意舊系統及非管理型交換機可能對數據收集造成影響。在資安漏洞與管理方面，雖然動態庫存盤點工具可以自動關聯資安漏洞，但其準確性與更新頻率仍需人工定期檢視。

(4) 供應商選擇與合作：

供應商在資產識別和漏洞管理中扮演著關鍵角色，使用者應該清楚自己的需求、網路環境和目標，並在選擇供應商時特別注意以下能力：例如動態庫存盤點工具所支援的 OT 協議與資料收集方法，尤其是對跨網段的收集處理方式，以及漏洞關聯的準確性與更新頻率。

(5) 改進流程與實踐：

講者建議通過小範圍的驗證（POC）測試供應商工具可用性，降低實際實施的風險。此外，IT 與 OT 團隊需加強合作，雖然 IT 團隊在漏洞管理方面有經驗，但需避免以傳統 IT 方法應對 OT 場域的問題。

(6) 管理層溝通與支持：

最後，講者強調動態資產管理的成功需依賴管理層支持，向管理層說明相關風險時應說明這是一個持續改進的過程，要達到 OT 網路安全和動態資產管理都並非一朝一夕即可完成的事項，需要靠持續投入和調整優化的過程。

圖 13 會議過程，資料來源：現場照片

(七) SBOM 如雨後春筍般湧現：如何妥善運用（It's Raining SBOMs: What to Do with Them Once You've Got Them）

1. 講者：Eric Byres

 Eric Byres	Eric Byres 被公認為 OT 網路安全領域的世界領先專家之一。他致力於 OT 軟體供應鏈的安全性，並為美國國家電信暨資訊管理局 NTIA SBOM 委員會成員，撰寫了許多關於軟體物料清單的文章。

2. 重點摘要：

講者 Eric 在資通安全、供應鏈管理及軟體開發等領域擁有豐富的經驗，並致力於推動行業資安標準的制定與實施，特別是在軟體物料清單（SBOM）方面。本次主題說明 SBOM 的重要性及如何應用於資安環境

中，隨著網路攻擊的頻率和複雜程度不斷增加，企業和政府機關越來越重視軟體組件的透明度和可追溯性。以下是會議中關注的重點：

(1) SBOM 的定義與重要性：

SBOM 是一份詳細列出軟體組件及詮釋資料的清單，能夠幫助組織了解其使用軟體中包含哪些第三方元件。這對於識別潛在的安全漏洞具有幫助，特別是在面對如 Log4j 等已知漏洞之情況。

(2) 供應鏈安全的挑戰：

講者 Eric 於會議中提到，許多企業在面對供應鏈危機時，往往需要主動聯繫數十甚至數百個供應商，來確認其產品的安全性。這種傳統的對應方式不僅耗時，還可能導致資訊不對稱，增加其資安風險，Eric 建議應該好好運用 SBOM，而非忽略。

(3) 政策與法規的推動：

隨著美國政府對網路安全的重視，相關政策和法規如《行政命令（EO）14028 號》和《國土安全部軟體供應鏈風險管理法案》相繼通過，要求企業提供 SBOM 以增強透明度和安全性。這些政策不僅影響政府機關採購，也將改變私人企業的營運方針。

(4) 標準格式趨於統一：

目前主流 SBOM 格式欄位已趨於相近，且已有許多開源且免費的工具可提供不同標準格式間轉換，方便使用者查詢。

(5) 技術的應用：

透過 AI 進行弱點通報搜索，在龐大的資料量篩選出與特定版本相關的安全警示，於面臨潛在威脅下，能有效提升應變效率，減少人為錯誤。

(6) 未來的展望：

隨著 SBOM 的普及，未來軟體開發和供應鏈管理將更加著重於透

明度和可追溯性。企業需要建立健全的 SBOM 管理體系，幫助組織識別高風險組件，以應對不斷變化的資安威脅和合規要求。

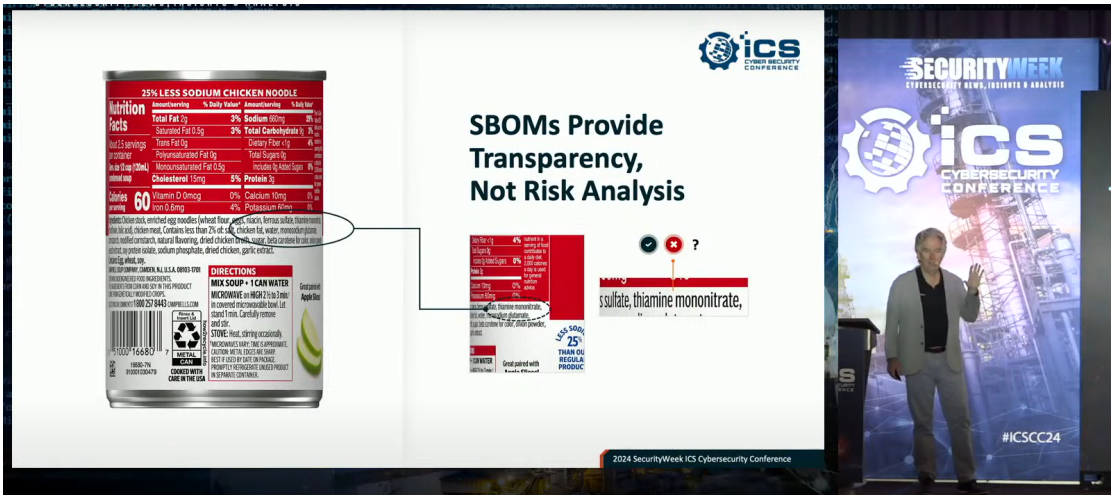

圖 14 SBOM 介紹及會議過程，資料來源：現場照片

(八) 零信任方法於安全的 ICS/OT 營運：滿足 62443、NIS2 之合規需求（Zero Trust Approach for Secure ICS/OT Operations: Addressing 62443, NIS2, and Compliance Needs）

1. 講者：Philip Griffiths

 Philip Griffiths	Philip 是一位經驗豐富的商業領袖，在開發零信任業務和建立高績效團隊方面經驗豐富。目前擔任 NetFoundry (零信任研發公司)業務開發全球副總裁。

2. 重點摘要：

講者 Philip 指出傳統的資安措施已不足以保護關鍵基礎設施的 ICS 和 OT 環境。採用零信任架構可以保護這些系統，同時確保符合 ISA/IEC 62443 和 NIS2 等標準。會議內容探討了零信任原則應用於 ICS/OT 操作，提供超越網路邊界的全面資安策略。通過將零信任架構直接嵌入到工業產品和系統中，組織可以提升系統的安全性，將其與來自網際網路、區域網

路或主機操作系統的威脅區隔開來。以下是會議中關注的重點：

(1) 零信任架構的核心理念：

零信任架構的基本原則是「永不信任，持續驗證」，無論是內部還是外部的請求，都必須經過嚴格的身份驗證和授權。此理念在工業控制系統中尤為重要，因為這些系統通常涉及關鍵基礎設施，任何安全漏洞都可能導致嚴重後果。

(2) 工業自動化中的應用：

講者 Philip 於會議中提到，將零信任導入工業控制系統（如 IFWs、IPCs 和 PLCs 等），以推動工業 4.0 的發展，提高系統的安全性，促進新技術的整合，使營運更有效率。

(3) 面臨的挑戰：

雖然零信任架構提供了許多機會，但在實行過程中面臨不少挑戰。例如，如何在不影響系統性能的情況下，對每一個資料存取進行身份驗證和授權。此外，有別於 IT，在 OT 的獨特性及差異性極大情況下，如何遵循 ISA/IEC 62443 標準、確保安全性和合規性也是一大挑戰。

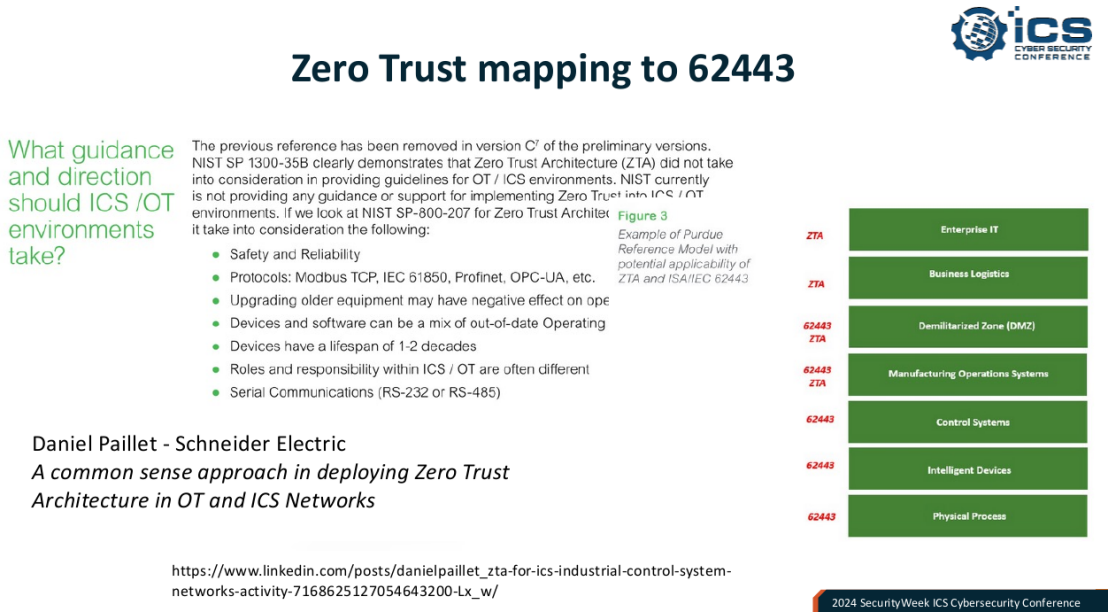

圖 15 零信任對應 ISA/IEC 62443，資料來源：講者簡報

(4) 威脅風險不斷提高：

講者 Philip 引用喬治亞理工學院的研究，展示了他們如何在網路上找到 8000 個程式邏輯控制器可以操控連網的系統，這是未來工業控制系統面臨的安全挑戰。風險的不對稱性，使得防禦者安全受到威脅，攻擊者只需找到一個漏洞即可入侵系統。零信任架構作為一種新興的安全策略，可為企業提供了一種有效的解決方案，助其在複雜的網路環境中保護關鍵基礎設施。

(5) 未來展望：

隨著工業環境資訊化轉型，零信任架構將成為未來資安策略的核心。講者 Philip 強調，企業需要不斷更新其安全產品，並將重點放在開發「更安全的產品」上，而不是增加用以「保護」產品的數量。

圖 16 會議過程，資料來源：現場照片

(九) OT 中整合控制與安全系統（ICSS）的安全性與挑戰（Security and Safety Challenges of Integrated Control and Safety Systems (ICSS) in OT）

1. 講者：Kevin Kumpf

 Kevin Kumpf	Kevin 是一家軟體公司（Cyolo）的首席 OT 策略規劃師，有 20 多年的 IT 安全和安全規定導入經驗，並在能源、醫療、製造、運輸相關的安全治理和關鍵基礎設施管理有豐富的經驗。

2. 重點摘要：

講者分享了整合控制與安全系統（ICSS）在現代運營技術（OT）場域中的安全和保障挑戰，特別在 IT 和 OT 系統整合的影響與風險。

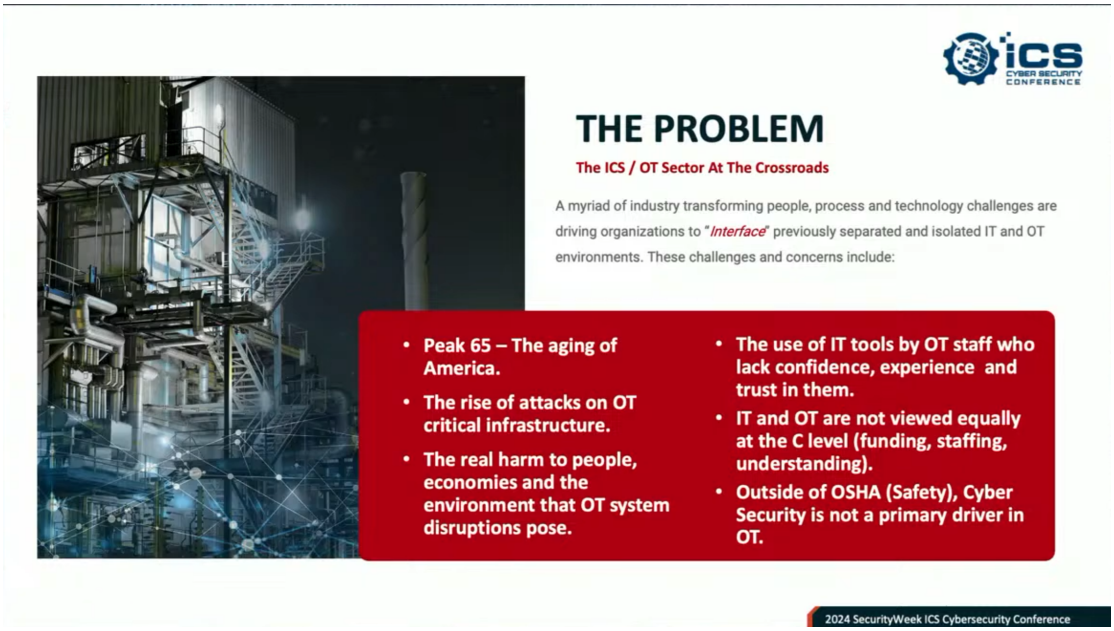

圖 17 OT 環境所面臨的各種難題，資料來源：講者簡報

以下 5 大項為主要內容：

(1) IT 與 OT 人員的目標差異與溝通障礙：

多數 IT 人員注重資訊安全性（Safety），而 OT 人員更在意設備系統的可用性（Availability）。例如，IT 注重來自電子郵件的網路威脅，而 OT 則重視實體設備的安全運行。另外，IT 和 OT 人員使用不同的專業術語所造成的溝通障礙，例如 IT 熟悉雲端技術和防火牆，而 OT 專注於 PLC（可程式邏輯控制器）和 HMI（人機界面），

這些差異常時常導致雙方人員溝通不良。

(2) 系統整合困難與風險：

講者強調將安全系統與控制系統分開管理的重要性，防止因單一端點故障進而導致設備全面癱瘓的結果，隨著數位轉型（如工業 4.0 和 5.0）的推行，導入系統日誌與網路監控工具這類 IT 工具到 OT 環境，往往也增加了被攻擊的可能性。

(3) 人力流失的年代：

美國即將進入 65 歲退休高峰期，每年有數以百萬計的勞動力退休，尤其在製造業和 OT 場域特別明顯，經驗豐富的員工流失也造成知識傳承的斷層，新進且經驗不足的人員面對龐大的工業環境更加無所適從，而且 OT 場域的工作常被認為是"骯髒、危險和困難"的工作（Dirty、Dark and dangerous ; 3D job），降低了年輕人進入該領域的意願，人力不足導致現有的 OT 人員常常負擔過多的工作。

圖 18 美國退休潮來臨，資料來源：講者簡報

(4) 人身安全與事件回應計劃的關聯性：

在 OT 場域中人身安全是最重要的，化學藥品外洩或工業設備故障

可能導致生命安全受到傷害，因此，講者認為需要建立安全控管系統和監控系統來避免災害發生，此外，建立 IT 和 OT 的事件回應計劃包含惡意攻擊（如網路攻擊）和意外事件（如人為錯誤），才能在災害發生時快速的因應。

(5) 介接優於整合：

講者建議將 IT 與 OT 系統以介接方式連接而非將 IT 整合到 OT 系統，確保系統邊界清晰並可在危機時迅速隔離受影響部分，使 OT 核心系統運作不受影響，並強調 OT 安全與人身安全對整體運營的重要性，需要將"讓每個人安全回家"的理念作為導入 OT 安全的核心目標。

ICSS 為 OT 帶來了巨大的改變，但同時也帶來了更複雜的 OT 環境。IT 和 OT 人員需要有清楚的系統介面、良好的溝通以實現安全與效率的雙贏。此外，企業應高度重視人員培訓與管理，確保知識的有效傳承，並構建一個能快速回應事件的體系，以應對未來複雜多變的 OT 環境。

圖 19 會議過程，資料來源：現場照片

(十) OT：越是變化，越是保持不變（OT, the More Things Change, the More

They Stay the Same）

1. 講者：Paul Brownridge

 Paul Brownridge	講者 Paul 是一位具有工程師背景白帽駭客，並在過去的 10 年中一直從事網路安全相關工作，是一位對工業環境和網路安全有實際經驗的工程師。經常出席國內外技術和安全事件的演講，參與過如 Defcon 和 (ISC)2 安全大會等活動，特別專注在汽車、海事和 OT 領域的資安風險。

2. 重點摘要：

講者分享工業控制系統(ICS)、物聯網(IoT)、營運技術(OT)等領域的現狀與挑戰，並分析現代化技術整合帶來的安全風險。演講者具備工程和網路安全背景，過去的經歷包括在煉油廠、加工廠等場所工作，以及執行 OT 測試、物聯網 API 測試及威脅模組工作。

演講強調了現代技術（如：IoT 和雲端系統）整合到可程式邏輯控制器（PLC）的挑戰。例如，關鍵基礎設施和其他如汽車、海事 IoT 及建築管理系統，都因缺乏原始安全設計而導致新威脅的出現。許多漏洞並非複雜漏洞，而是由於系統開放性或供應商不當操作引起，例如：安裝過時或未更新修補程式的設備、未設限存取限制的管理介面和寬鬆的遠端存取機制、缺乏身分認證的設備和過時的防火牆設定等，這些問題不斷發生在設備供應商與系統整合商之間，原因在於 OT 設備設計目的過於注重可用性而忽略安全性。

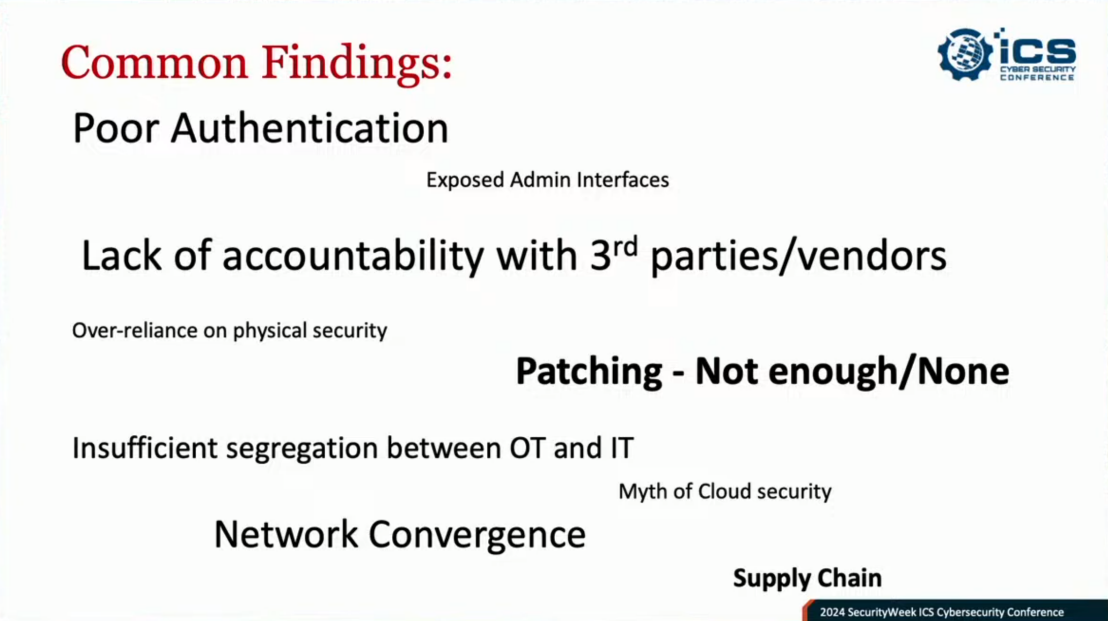

圖 20 OT 常見的資安問題，資料來源：自行截圖

講者舉出多個實際案例來說明這些問題：

(1) 德國廢物處理廠：

該廠內網路在防火牆有進行網路區隔，但供應商在主要網路中安裝了過時的遠端存取設備，導致內部設備暴露在網際網路攻擊中。

(2) 哥倫比亞水處理廠：

設備使用 GSM （Global System for Mobile）與控制中心通信，但 APN（Access Point Name）設定欠缺基本的安全保護，使攻擊者能夠輕鬆利用後端漏洞入侵。

(3) 船舶測試案例：

海事環境中，裝載主機和燃料效率監測系統因網路未適當隔離，導致船上管理系統被遠端操控。

(4) 建築管理系統：

在建築物管理中，未設置管理介面認證，設備供應商未經許可接入網路，甚至使用廉價硬體（如樹莓派）導致網路安全薄弱。

講者總結出隨著 IoT 和 OT 的深度融合，系統間互相結合使得網路

攻擊的影響更為廣泛。因此，企業必須強化端點保護、網路分隔與存取控制，並加強供應商安全管理的透明度。

圖 20 會議過程，資料來源：現場照片

(十一) 安全的未來：工業控制系統中 OT GRC 的進階策略（Securing the Future: Advanced Strategies for OT GRC in Industrial Control Systems）

1. 講者：Roger Hill

 Roger Hill	Roger 是 Hillstrong Group Security 的創始人，在工業自動化和資安方面擁有 30 多年的專業知識。他專注於 OT GRC（營運技術治理、風險和合規性），指導全球製造企業加強其網路防禦，致力於推進 ICS 安全實踐。。

2. 重點摘要：

隨著工業控制系統（ICS）的獨特性和複雜性，對治理、風險和合規性（GRC）策略的需求越為迫切。以下是會議中關注的重點：

(1) 整體風險管理：

講者 Roger 強調了利用實際資訊和預測分析來主動識別風險的重要性。此方法不僅能夠幫助企業發現潛在的安全漏洞，還能根據每個設施的營運和環境變化制定風險模型，以提高風險評估的準確性和有效性。

(2) 合規框架：

企業應該為每個工廠開發特定的資安應變框架，以便在發生資安事件時能夠迅速控制局面。這包括利用通訊工具來協調各個地點的應變行動，並於事前定期演練並完善事件應變計畫，以因應突發狀況。

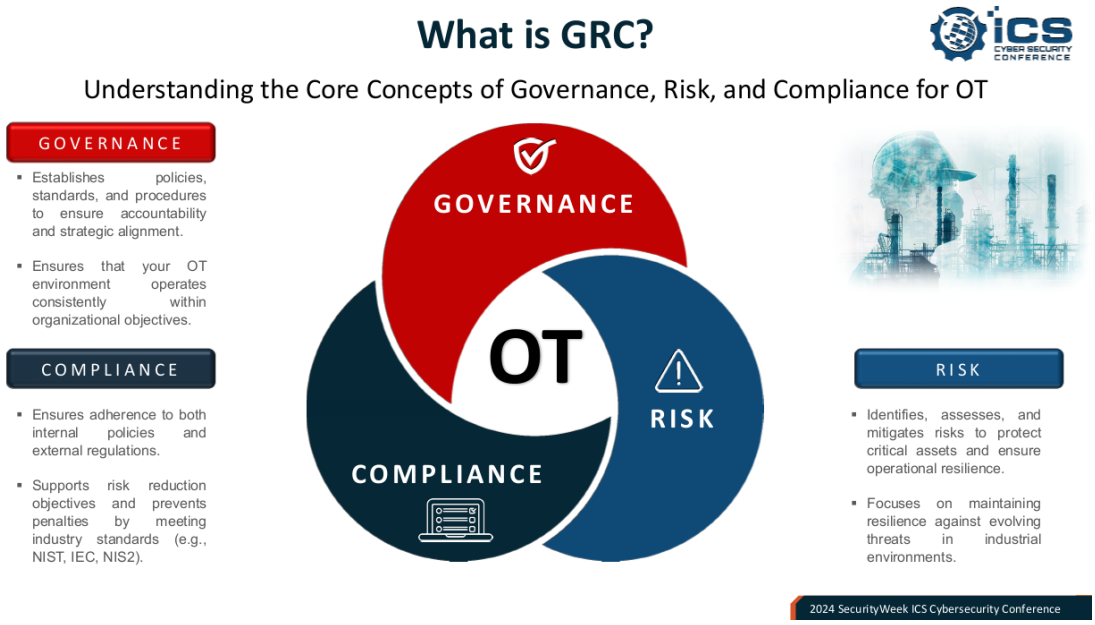

圖 21 治理、風險和合規性（GRC），資料來源：講者簡報

(3) 可擴展的解決方案：

探索及開發可擴展的 GRC 策略，以調適分布於全球的製造工廠和各種工業控制系統的複雜性，講者 Roger 指出，企業需要定期評估和更新其 OT GRC 框架，以應對不斷演變的風險和監管變化。這種持續改進的過程應包括回饋循環，以確保 GRC 流程持續優化。此

外，靈活性是 GRC 策略的關鍵，企業應該能夠根據業務需求的變化和新技術的出現進行調整。

(4) 技術整合與預測分析：

講者 Roger 提到，將新興技術整合進 GRC 框架，可以增強可見性和威脅偵測能力。利用自動化來簡化合規流程和提高應變效率是重要策略之一。預測分析的應用能夠幫助企業在風險實現前先行識別，進而減少事件發生的可能性。

(5) 對齊業務目標：

講者 Roger 強調 GRC 應與企業整體業務目標對齊。這理念能夠幫助企業更好地理解 GRC 的價值，確保資源有效分配，降低資安風險。

圖 22 會議過程，資料來源：現場照片

(十二) OT 技術趨勢與挑戰概況（Overview of OT Technology Trends and Challenges）

1. 講者：Mike Bova

 Mike Bova	企業客戶經理 5 年以上，與財富 1000 強公司、大型醫療保健、州和地方及教育機構合作經驗。

2. 重點摘要：

講者分享在現代 OT 環境中，關鍵設備的穩定運行直接關係到企業的生產與經濟效益。然而，隨著技術需求的不斷增長，OT 管理者面臨諸多挑戰，包括勒索軟體攻擊、惡意軟體威脅以及老舊系統和硬體的安全問題。維持系統全天候正常運行是每個企業的核心目標，但未預期的停機卻可能造成企業巨大損失，根據統計，某些大型製造企業的每小時停機成本高達數百萬美元。許多 OT 設備仍在運行過時的操作系統，如 Windows XP，這些系統通常由已退休的專家設定，當設備出現故障時，企業可能難以找到合適的替代設備或重新設定的方法，進一步加深了系統維護的困難。此外，OT 領域也面臨人力資源短缺問題，特別是隨著經驗豐富的技術人員逐漸退休，知識傳遞和技術延續面臨嚴峻考驗。

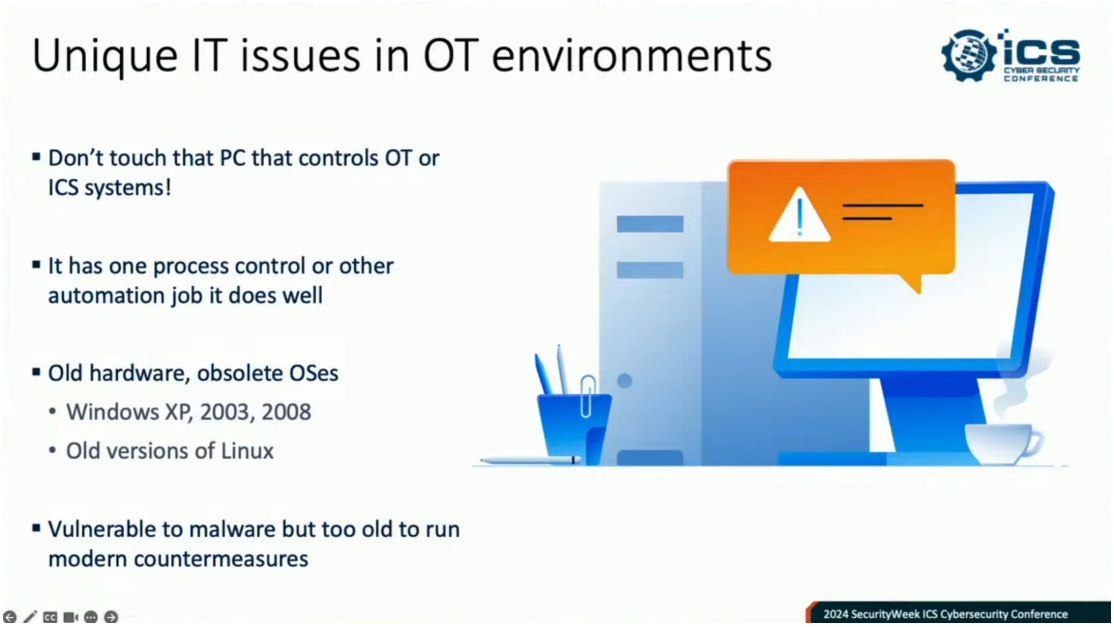

圖 23 OT 環境的特殊考量，資料來源：講者簡報

為應對上述問題，企業需要引入快速復原與備份機制，以確保在出現故障時能夠迅速回復系統運行。提高備份效率與建立災難復原系統並透過採用虛擬化環境進行測試與修補更新，減少對生產設備的直接影響，同時透過集中化管理工具實現對分散式網路的統一監控。這些技術的應用不僅簡化了操作，還幫助企業有效降低停機時間。此外，面對勒索軟體與惡意軟體的威脅，企業應該啟用主動防護功能，並針對備份數據進行完整性檢測，以避免恢復過程中因惡意軟體感染導致進一步損失。

隨著 IT 與 OT 技術的結合成為新趨勢，企業應在確保業務需求與科技技術之間找到平衡，特別是在導入新技術或升級現有系統時，並與主要自動化供應商保持密切合作，以簡化整合過程並提升設備兼容性。未來，企業需進一步加強對新興威脅的應對能力，並積極投資於新技術與技能培訓，確保具備快速復原的靈活性。通過簡化管理流程並採取可靠的恢復機制，企業將能夠有效降低整體成本和減少停機時間，從而實現更高的運營效益。

圖 24 會議過程，資料來源：現場照片

參、心得與建議事項

SecurityWeek 的工業控制系統資安研討會主要目的是促進工控領域知識分享、技術交流和行業合作，以因應當前日益嚴峻的網路安全挑戰，內容包含 OT、工業自動化與控制系統、網路安全、系統架構、工業控制管理及分析風險，以及實體安全與風險管理。多位政府及業界專家分享於資通安全領域之實務經驗和案例研究，以面對資安威脅研擬應對策略和最佳實踐，不僅提供了理論基礎，亦含實務的操作建議。本次會議相關心得及建議如下：

一、當前工業控制系統安全挑戰

近年來科技演進工業控制系統網路化，眾多公私部門將面臨更多資安威脅。相關資安威脅自 IT 延伸至 OT，且針對供應鏈攻擊及勒索病毒之威脅大增，如何有效進行防護將是各機關的重要課題。於工控領域為確保設備系統高可用性及人員人身安全前提下，加強資安防護並避免影響 OT 之日常營運，與會專家們建議需重新評估其資安策略，並採取靈活和具前瞻性措施以應對這些挑戰。

多數工業控制系統因其系統獨特性及技術限制，難以直接適用法遵之防護基準，仍有賴各中央目的事業主管機關，制定各工業控制專屬領域之防護基準，輔以落實補償或替代措施，以降低資安風險，並應留下相關紀錄佐證文件，俾利後續定期檢視其補償措施之有效性。此外，機關應定期審視工控系統，並因應主客觀技術與檢查方式等環境變化，持續精進資安防護作為，以維護系統安全。

二、技術創新與解決方案

與會者探討了多種新興技術在資通安全中的應用，人工智能（AI）、機器學習（ML）及零信任架構皆為提升資安防護能力之重要工具。透過前揭技術協助各機關於 OT 場域自動化安全監控，快速偵測異常行為，有

效持續驗證身份，並即時應變潛在的資安事件。此外，區塊鏈技術亦可作為增強資訊完整性和透明度的手段，以提升工業控制系統資安防護量能。

我國為因應新興科技帶來之解決方案，推動零信任架構試行及導入，以身分鑑別、設備鑑別及信任推斷 3 大核心機制，提高系統的安全性，促進新技術的整合；且為確立推動 AI 技術與應用發展之方向及作法，建構 AI 技術及應用環境，國家科學及技術委員會於 113 年 7 月 15 日已預告制定「人工智慧基本法」草案，並由數位發展部參考國際標準或規範發展之人工智慧資訊安全保護、風險分級與管理，推動與國際接軌之人工智慧風險分級框架，以利機關參考使用。

三、法令與標準合規

隨著各國對資通安全的重視，合規性成為各機關必須面對的重要議題。會議中專家們提及各種國際標準和法規，如 NIST SP 800-53、ISO 27001 等提供機關內部實施標準的指引。與會者多認為遵循這些標準不僅能夠提升機關的資安防護能力，還能增強客戶和合作夥伴之信任。

我國刻正推動「資通安全管理法」修正草案，內容並納入跨機關合作及區域聯防，有效落實納管機關之資安管理及防護。另因應國際資安法令及標準更新，本署每年定期檢視現行資安相關規範或資安指引，並滾動修正及調整，以符合國際資安趨勢及合規性。

四、人員培訓與意識提升

本次會議強調了人員培訓對於資安之重要性。員工資安意識不足可能導致資安事件發生，因此，機關需定期進行資安職能培訓，提升員工的防範意識和應變能力。與會者分享了成功的培訓案例，並建議應建立持續性學習文化，如網路安全人員需了解攻擊者攻擊手法，確認如何進行防護及修補，以加強工控環境的資安防護。

我國數位發展部資通安全署已建立資安人才培訓多元管道及機制，

辦理資安職能訓練課程、資安工作坊、資安實戰人才培訓、資安主管治理研習及資安長共識營等，積極充實國內資安人才養成訓練。