發展結合物聯雲霧計算平台與異質生產設備之智慧化資安技術暨攻防演練場域驗證

The Study of Key Information Security Techniques and of Offensive and Defensive Verifications on Intelligent IoT Cloud-edge Computing Platform and Heterogamous Manufacturing Equipment

陳彥霖、楊士萱、陳金聖、何昭慶、林志哲、王正豪、曾釋鋒、張世豪、劉佳明、余兆偉

Yen-Lin Chen, Shih-Hsuan Yang, Chin-Sheng Chen, Chao-Ching Ho, Chih-Jer Lin, Jeng-Haur Wang, Shih-Feng Tseng, Shih-Hao Chang, Chia-Ming Liu, Chao-Wei Yu

本整合型研究將以工業 4.0 之發展情境中之製造工廠為例並加入 IEC62443 系列標準之資訊技術系統的安全標準為基礎，建構一個基於智動機電平台之智慧工廠，並將於工廠中可能存在的資安事件為樣本，並在臺北科技大學機械工程系自動加工機械工廠作為攻防驗證與 IEC62443-2-4 認證的試驗場域，為臺灣企業對於智動機電的實現與轉型提供一個完整的解決方案與示範樣本。在研究主軸上可分為三個總體研究目標：「IT (Information Technology)-應用層」、「CT (Communication Technology)-傳輸層」與「OT (Operation Technology)-感知層」。本研究預期工廠產線的加工設備運作資訊以及生產資料會由「OT-感知層」感測器在設備上進行來進行相關機電感測單機的擷取資料整合，並且再根據資料種類透過「CT-傳輸層」之閘道器實現異質網路將資料上傳至「OT-感知層」的「邊緣」端，以進行初步運算與分析管控；「邊緣」端主要工作為透過「OT-感知層」設備取得的影像與感測資訊，並進行資料的標示辨識與分析運算，然後再將分析後的模型透過高效率加密編碼的方式傳送至「IT-應用層」區域的霧端平台上。當「霧端」蒐集到資料後，會進行更進一步的學習與整合，並且透過學習衍生出 AI 的決策分析，最後再由「OT-感知層」針對相關工具機進行加工參數的最佳化決策，已進行加工設備的生產調整；由於此層資料甚為珍貴，故在資安部分，本研究會透過混沌加密演算法與 3DES 及傳輸層安全性協定 (TLS) 來確保資料傳遞的安全性，防止在交換資料時受到竊聽及篡改。最後經由「霧端」分析與學習後的模型及決策會與「OT-感知層」進行辨識模型與 AI 決策的模型更新與強化，最後再將相關控制指令傳送

至「實體」設備上進行相關控制數據的修正，使得產線生產上得以最佳化最有效率，使得形成一個「IT-應用層」、「CT-傳輸層」與「OT-感知層」之間相輔相成的智動機電資安系統。

This study takes the manufacturing field in the development context of Industry 4.0 as an example and integrates key points in IEC62443 standards. We plan to build up a smart factory based on a smart-motor-electrical platform which takes the possible security incidents in the factory as a practical example and adopt the smart manufacturing factory of National Taipei University of Technology as a POC site for offensive and defensive verification on information security issues and gets the IEC62443-2-4 certification. The study includes three overall research goals: “IT-application layer”, “CT transmission layer”, and “OT-aware layer”. This plan expects that the sensor machine inductive sensing "OT-sensing layer” will capture and integrate the operation information as well as production data of the factory production line, then is realized through the “CT transmission layer” gateway according to obtained data. The heterogeneous network uploads data to the “Edge” end of the “OT-sensing layer” for preliminary learning, analysis and control. The “edge” end mainly works with the image and sensor information obtained through the “OT-sensing layer” equipment. In addition, the proposed system will perform data label identification and analysis calculations, and then transmit the analyzed model to the fog terminal platform in the “IT-application layer” area through high-efficiency encryption and encoding. When the “Fog End” collects the data, it will conduct further learning and integration then derive the AI decision-making analytics. Because the manufacturing data is very precious, in the information security part, this plan will apply chaotic encryption algorithms, 3DES and the Transport Layer security (TLS) to ensure the security of data transmission and prevent eavesdropping and tampering when exchanging data. Finally, the model and decision after the analysis and learning of the “fog end” which will be updated and strengthened with the “OT-sensing layer” for the identification model and AI decision model. The relevant control commands will be sent to the “physical” device for relevant control. The correction of the data makes the production line optimized and most efficient, which means that the “IT-application layer”, “CT transmission layer”, and “OT-sensing layer” become a perfect cooperated intelligent electrical security system.

一、本研究重點成果

本整合型研究以工業 4.0 之發展情境中之製造工廠為例並加入 IEC62443 系列標準之資訊技術系統的安全標準為基礎，將原本僅有單機運作且無聯網之既有機械工廠加工設備、機械手臂與 AGV 載具等設備，透過自行開發客製化 OPC UA 裝置與機聯網關鍵技術，使 CNC、雷射加工機與自動化載具設備聯網能力。透過身分認證進行異質設備的連線驗證：建構一個基於資安智動機電平台之智慧工廠，以臺北科技大學機械工程系智動化機械工廠作為資安攻防的驗證場域，期為臺灣企業對於智動機電的實現與轉型提供一個完整的解決方案與示範。

本研究之主要目的，在於集合跨領域與跨校老師及同學的專長與心力，整合感測技術、聯網技術、邊緣計算技術與異質加工設備整合平台等各項核心技術，並實現於一套結合物聯雲霧計算平台與異質生產設備之智慧化資安技術，完成一套雛型系統，期望可以帶給使用者以及國內相關產業一個使用體驗與參考設計。

1. IT 端應用層

(1) 聯邦式學習運算平台：透過聯邦式學習結合 MEC 霧端平台與 docker 快速建立多個聯邦式學習平台，並依照不同機器類型區分進行資料收集與訓練，再將訓練後的模型透過加密 VPN 通道上傳至伺服器並儲存到資料庫中，可降低生產資料上傳至雲端訓練的洩漏風險，再由伺服器的聯邦式管理器選擇是否要結合資料庫中的模型或給予 client 端更新。

(2) MEC 霧端平台：可在 OT 端環境提供資料庫、Edge Computing 等 IT 平台，降低資料存取延遲影響及強化系統即時運算之能力。

(3) 透過 Brute Force Detection、2FA (two factor authentication) 機制、加強系統內部的安全性。並將系統落實分離式架構，提高服務的可用性與日後開發、佈署、維運的方便性，也導入 Keycloak Log 供日後審視系統漏洞為用。

2. 資料傳輸層

(1) OPC-UA 閘道器：實現客製化 OPC-UA Gateway 讓受信賴認證的設備接到本機或通過與 OPC-UA Server 端交換資料後主動傳輸 IT 端，加上混沌理論作為傳輸加密的基礎，實現隔離高風險設備，並導入 IEC62443 安全標準基礎。客制化閘道器提供可視化操作介面。

(2) 混沌加密演算法開發：在每次傳輸中，將使用者所鍵入之帳號名稱藉由 ASCII 轉換成數字與英文的組合，依序透過二進制 (binary)、十進制 (decimal) 轉換成驅動渾沌系統 (logistic map) 的初始值 (initial condition) 以生成亂數密碼，最後將生成的亂數密碼與原文做互斥或得到密文。

3. OT感測層

(1) 整合機械手臂與 AGV 載具資訊，AGV 載具更換至 Voronoi 路徑規劃演算法，使其符合 IEC62443 的規範。

(2) 透過整合量測機台量測資訊與雷射機台加工資訊，建立 MEC 系統平台將資訊可視化，使其符合 IEC62443 的規範。

二、資安實測場域建置情形說明與使用技術方法

本研究整合終端異質裝置與物聯網技術與智慧化資安技術之開發工作，以及規劃與設計臺北科大機械系之智能工廠、北科附工與東元、東訊與福壽實業工廠等相關系統平台之展示空間，透過實際的使用、體驗，可以有效的推廣與轉移本研究所完成的各項技術至產業界，協助本土產業應用於終端異質裝置與物聯網資訊安全技術的自主性，提昇產業於全世界的競爭力。並以 IEC62443 之相關規範進行場域實體安全計劃的管理及權限劃分，完成最佳化本

研究所完成之終端異質裝置資訊處理、聯邦式學習架構、物聯雲與異質網路核心技術、資訊安全所需之整合 OT 及 IT 端的資訊，並維持整體場域的可用性及即時性。

1. IEC62443 工業控制系統場域資訊安全管理規劃

本研究在完成認證 IEC62443-2-4 範圍確認後，協助本研究的雷射加工場域進行 OT 場域設備盤點，針對 IEC62443 的規範，盤點出整體研究中不同系統、區域 (zone) 及場域的設備，用以進一步地進行資訊分流及權限的劃分，接著由於 IEC62443-2-4 的認證，較偏於制度的管理面，因此在這個階段本研究盤點了可用於參考的相關之規範文件，進行建立本研究整體場域的制度，來瞭解整體場域的目前現況，以及檢視所盤點出的 OT 及資訊設備各自的風險，接著本研究透過各子系統的系統架構圖及網路架構圖現況，檢視目前系統是否有符合 IEC62443 所規範的橫向獨立分區、服務縱向防禦是否足夠，如此一來便可檢視過去所設立的防禦機制及安全性是否足夠，並加強整體架構的安全性。

2. IEC62443-2-4 認證範圍確認

由於 IEC62443-2-4 比較偏制度管理面，因此本研究透過安華聯網科技公司，協助在進行本年度 IEC62443-2-4 規範導入前先進行差異性分析，用來釐清目前本研究驗證場域與 IEC62443-2-4 規範差異為何，因此需要先確認本研究整體認證範圍，因此本研究先以雷射加工-量測生產流程進行場域空間的確認如圖 1，並寫出雷射加工流程的過程如圖 2，這時候可以清楚的瞭解在 OT 設備場域中主要有會有一台雷射加工機、雷射檢測平台、AMR 自動化設備及人員兩名，接著再觀察過去所設立的網路架構，如圖 3 及圖 4 分別可以看到人員要從網路上取得 OT 設備資訊，瞭解本研究在資訊傳遞上透過 OPCUA 閘道器將 OT 環境進行區隔，並由 IT 服務連線至 OT OPC UA 閘道器將資料上傳到資料庫，最後再透過獨立的網頁服務將資料庫的資料呈現及提供操作功能給使用者。如此一來，便可以確認本研究 IEC62443-2-4 所需要進行設備資產盤點及網路架構圖的範圍，便能夠進行接下來差異性分析的流程。

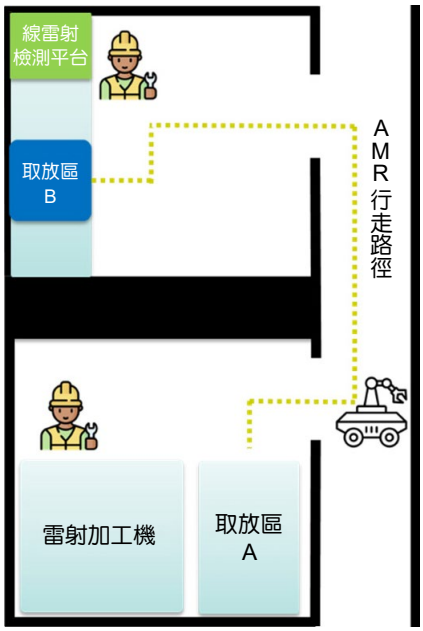

圖 1. IEC62443-2-4 認證場域圖。

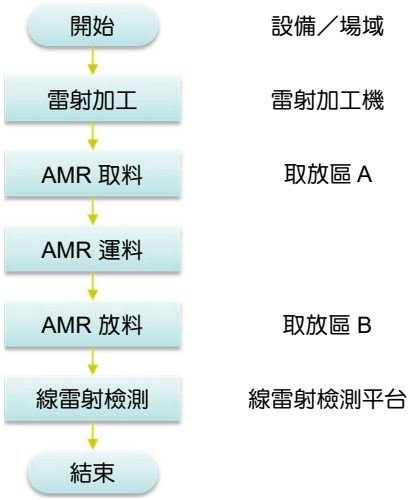

圖 2. 雷射加工－量測流程。

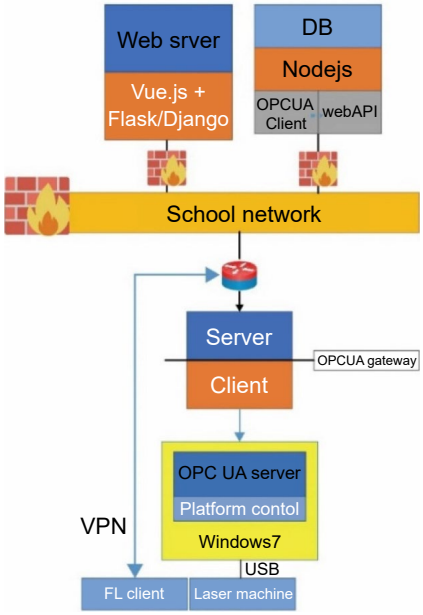

圖 3. 雷射加工網路資料架構圖。

3. 資安驗證場域系統架構圖

在完成盤點後，使用盤點表中的各項資訊及確認好的認證範圍，如圖 5，認證場域系統架構圖進行系統架構圖繪製，在這過程中可以確認各項系統的組件及系統組件中資訊交換的過程及方法。

4. 資安驗證場域網路架構圖

在完成資安驗證場域系統架構圖繪製後，便可以依照前項的流程，將本研究驗證場域的網路架構圖繪出，如圖 6 可以很明確地確認在場域中，哪邊有防火牆設備、資訊介面邊界、網段區域及傳輸方式，便可以進一步地瞭解整體研究場域架構的威脅所在。

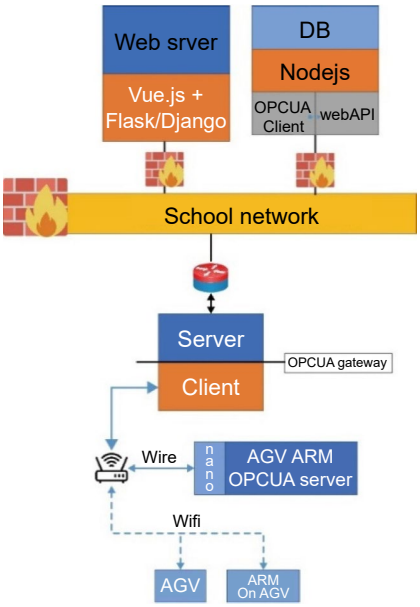

圖 4. ARM 網路資料架構圖。

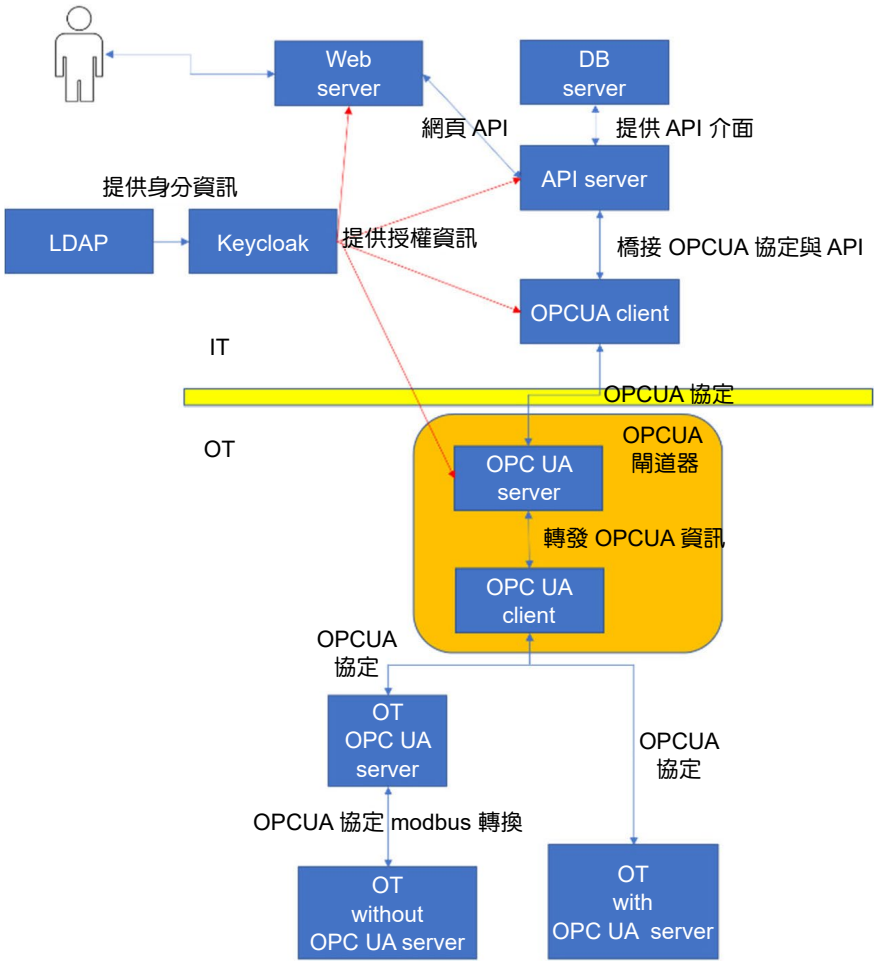

圖 5. 認證場域系統架構圖。

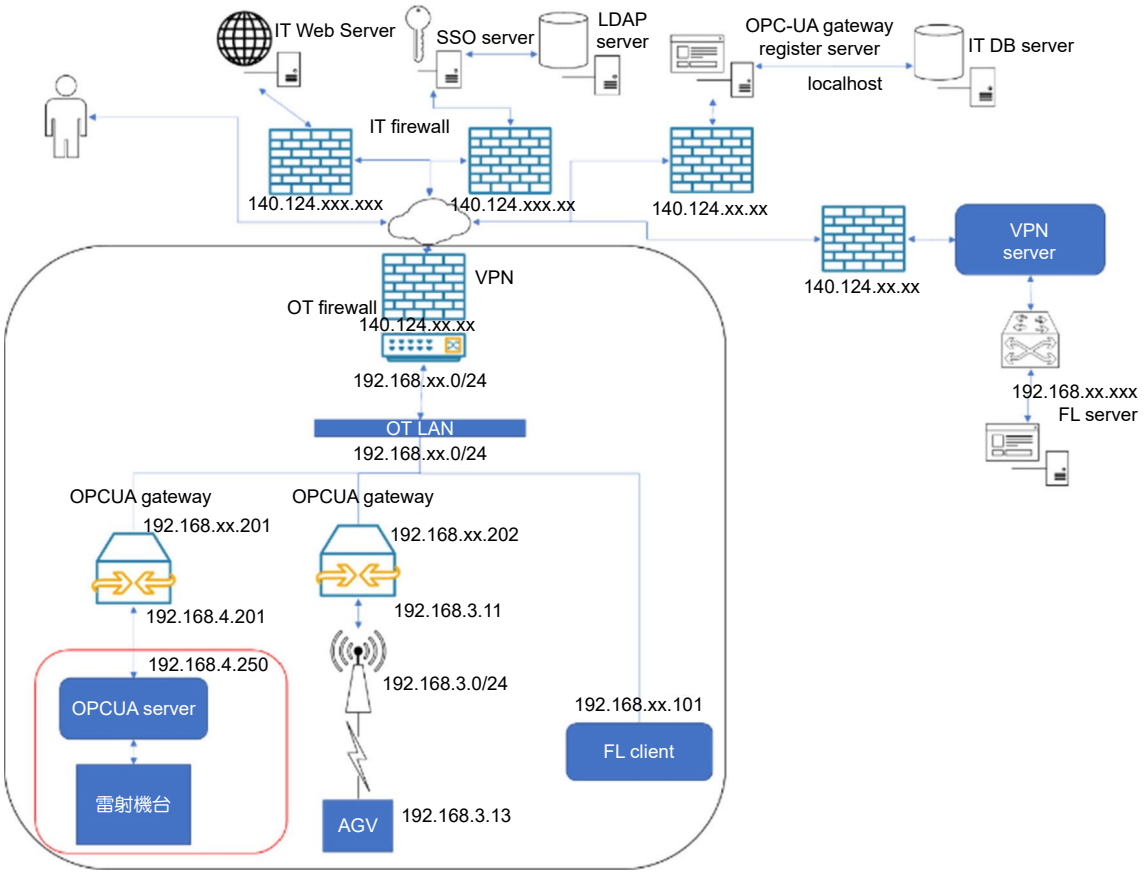

圖 6. 認證場域網路架構圖。

5. 網路架構與系統架構的改善

在完成上述流程後，可以看出本研究場域在 OT 及 IT 網路區域間，資訊會是直接穿過網際網路，因此在去年度建置的場域網路與系統架構上，將資訊在 IT 及 OT 間交換需要有更多的防護，且要減少 OT 資料直接上傳至 IT 資料庫的數量，減少資料外洩的風險，並要加強 OT 的防護邊界讓網際網路的駭客無法直接窺看到 OT 的設備資訊，在 IT 上由於去年都由各 IT 系統各自開發系統，導致了許多 IT 設備有各自的資安政策，在管理上將會發生溝通上的困難，導致個系統失效，因此本研究重新規畫了整體的網路架構與系統架構，如圖 7 為改善後的網路系統架構圖，可以看到本研究將 IT 服務上，透過 MEC 建置虛擬化服務，將原本分散的資訊服務建置在 IT MEC 伺服器中，並整合了 IT 防火牆規則，減少需要重複設定防火牆導致系統失效的問題，並透過 Proxy 代理對外服務轉換，隱藏 MEC 中的服務實際的位置，並讓 OT 區域網路透過 VPN 連線建立一條安全的通道，讓 OT 環境的資料仍可以正常的交換，而在減少 OT 資料上傳上，讓 OT 資料庫從 IT 環境中搬移至 OT 環境並建立 IDMZ 區域，並透過了 MEC 進行 SDN 的功能，透過 VPN 通道在使用者有需要檢視時，再提供給 IT 環境中所要的相關服務，如此一來便可達到 IEC62443 所訂定的三層式網路架構，提升整體網路的安全性。

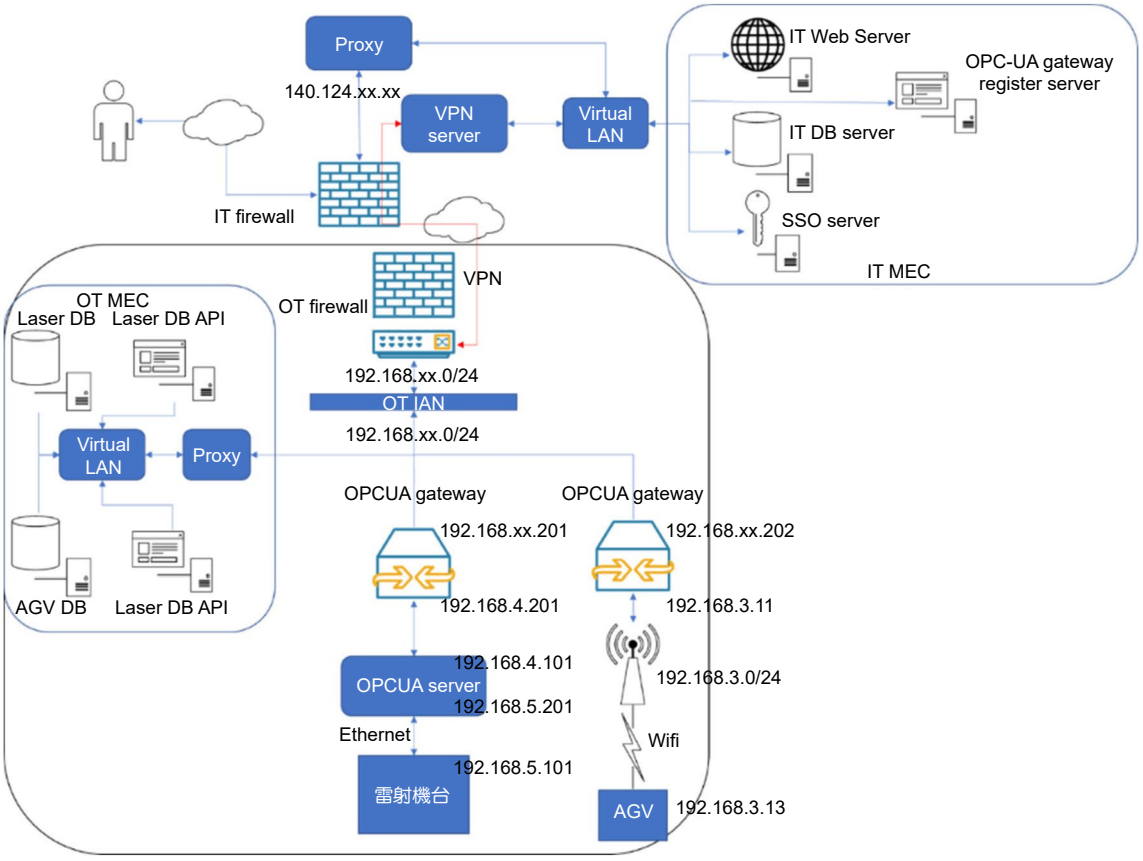

圖 7. 改善後網路架構與系統架構圖。

三、關鍵技術研究方法與結果

1. 異質生產設備 OT 之 SCADA 佈建與資安攻防之關鍵技術開發

智慧無人載具架構主要核心為嵌入式主機板，將感測器 (2D LiDAR、深度相機等) 資訊進行讀取後，進行主要核心處理計算，以達到定位及導航之規劃功能，再傳輸控制命令至馬達驅動器以驅動車輪，智慧無人載具開發環境為 Ubuntu16.04 下的 ROS Kinetic 版本，ROS 除了整合容易之外，另一大特點是因為它的開源系統，因此使用者有更多的資源可以使用及探討，使得開發機器人、智慧載具更為簡單且方便。在此主機板中，我們將進行智慧無人載具的設計及探討，例如：實地地圖建制、定位及導航、動靜態避障等功能，透過 ROS 平台，便可將多種功能加以整合，以達到智慧無人載具行駛於工廠的功能。智慧無人載具以及移動式機械手臂架構圖如圖 8 所示：

為確保運送料件安全性以及確認取得工件之人員身分，在智慧無人載具上放有配置電磁電控鎖的盒子，可利用盒子旁邊系統進行身分認證即可操作。因此只有符合規定之人員有權限使用及取得物件。電磁鎖盒子以及認證控制系統如圖 10 所示：

無人機上嵌入式主機板是由機構封閉，備有外接擴充孔位可供人員進行維護與操作。為符合 IEC 62443 2-4 SP.01 資訊安全規定，操作人員須進行訓練並符合操作規範規定。需確認操作人員身分，是否為符合經過安全與職業訓練之人員。因此在接上 USB 插槽意圖操作或使用嵌入式主機板時，系統會偵測到有外接式裝置插入操作，並主動進入鎖定。須經由密碼

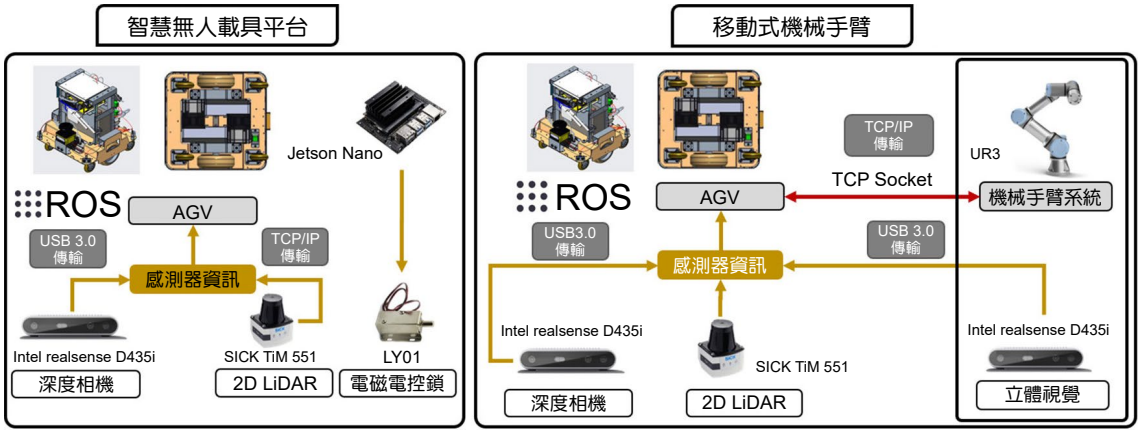

圖 8. 智慧無人載具以及移動式機械手臂架構圖。

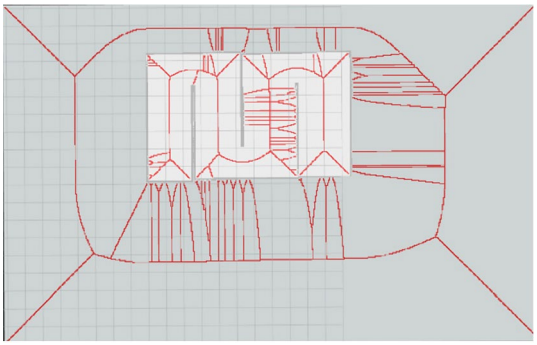

圖 9. Voronoi 路徑規劃圖。

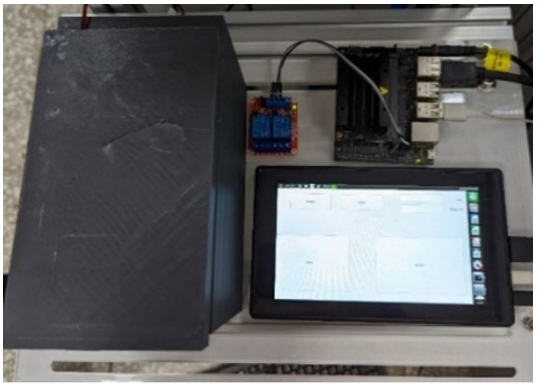

圖 10. 電磁鎖盒子以及認證控制系統。

進行認證解鎖才可以進一步進行操作。IEC 62443 2-4 SP.08 資訊安全規定針對 OT 系統安全建立事件偵測，並由內部程式建立記錄檔記錄插入操作之裝置與時間。在維護時即可利用記錄檔進行確認是否有被攻擊或被非規範人員操作。

2. OPC UA 工業網路資安攻防之網路層關鍵技術開發

工業物聯網中的閘道器，就是負責搜集和詮釋資料的裝置，它要能透過有線和無線等不同通訊介面， 與外部的感測器裝置、生產機械設備、雲端資料庫連結，並整合資料分析

功能。子研究開發之閘道器以 Open62541、Free OPC-UA 等通訊協定函式庫為基礎，加上混沌理論作為傳輸加密的基礎，使用本研究之 LDAP 做人員登錄認證，連結本研究的 CNC、AGV、雷射加工機等 OT 端設備，透過本研究的 VPN 安全通道傳輸到本研究的遠端監控網頁。從安全的角度來看，閘道器是工業物聯網網路安全的重要安全防禦邊界的核心之一，根據 IEC 62443 SP.03 的準則，必須內建完善的工業網路安全防護機制，如圖 11，才能將資料傳至資料中心做更為大量的資料分析及處理或是生產製造設備的參數控制等。OPC UA 為近年來愈來愈被工業界重視的工業物聯網通訊協定，且其安全性與靈活性而被選為德國政府推動的工業 4.0 計畫的骨幹，因此本研究將提升基於 OPC UA 的工業物聯網網路層資料安全，其中包含 (1) 採用 Basic256Sha256、混沌理論、DES 加強傳輸過程的安全性，可防止惡意竄改資料造成資安危害。(2) 使用兩個網卡，其功能可隔離安全性較不佳的 OT 裝置或設備，使其安全性增加。(3) 交換對稱金鑰作為會談金鑰 (session key)，將通訊兩方交換的資料做加密，保證兩個應用間通訊的保密性和可靠性，使客戶與伺服器應用之間的通訊不被攻擊者竊聽。(4) OPC UA 閘道器通過 MEC 服務所發放的 OT 憑證後再與 OT 設備作連線，並以僅對外開放網際網路的方式作為傳輸準則，提高了資料傳輸的安全性，也符合我們所使用的 IEC-62443 標準。除了技術的發展，也可培育優秀資訊安全人才，讓台灣的網通工業在物聯網與資訊安全興起之時代蔚然倔起。接下來將說明本研究於通訊層中的元件與通訊協議的規劃目標。以及實現規劃目標的方法與當前進度：

1. 通用性：本研究的安全管理必須能適用於各種工業物聯網通訊技術與系統。
2. 系統安全性與穩定性：系統安全性與穩定性必須能有效抵抗外部攻擊，有效地增加使用者的資訊安全與信任。此目標與各層皆有關聯，並把焦點放在系統的安全性與穩定性，而此特性包含了使用者對此系統安全可靠性及系統穩定性的挑戰。
3. 資料轉換及傳輸過程中必須被安全保護：資料傳遞必須經過加密通道，以防竊聽、揭露、竄改等情事。而任何未經授權的系統裝置，不可在資料傳輸過程中存取任何資料。此目標與工業物聯網的安全性及隱私性有關，也因此更強調安全性、信任、隱私等相關解決方案的重要性。在網路層，可以使用金鑰管理解決上述的關鍵議題及技術。
4. 身分認證能力：每個裝置之使用目的都應依照本身提供的服務被妥善的管理。進一步而言，需實現階層式及有效的身分管理。
5. 易操作性：工業物聯網閘道器需要有可視化操作界面，便於使用者管理閘道器的訊息與工控設備的連接狀況。

3. 異質生產設備之聯邦式學習與物聯邊霧計算平台之 IT 資安攻防關鍵技術開發

• 邊緣運算暨 SDN 架構整合系統

利用邊緣運算暨軟體定義網路系統減少延遲與頻寬使用，最佳化整體系統傳輸效率，提供終端快速的應用體驗。本研究中根據 IEC 62443 2-4 SP 03 架構－數據安全及敏感數據保護中所要求－應由授權使用者發起或批准，以及通過已批准的連接在批准的方向傳輸。因此，使用者在 Keycloak 完成身分認證後才可取得身分證明，此時可以藉由此身份進入區域邊緣雲霧段運算平台 (K8s) 應用及檢索其服務。本研究在智慧工廠配置與實際運作情形，把 SSO (雲端) 與 F1、B1 (霧端) 需要的相關應用都包裝成容器 (container)，在由 Kubernetes 系統來管理雲端與霧端溝通傳輸並且維護容器間的穩定，以下會針對該服務管理系統與 IEC 62443 之安全規範做更詳細的說明。本研究目前已實現系統內的穩定性，跨系統穩定性還在開發中。

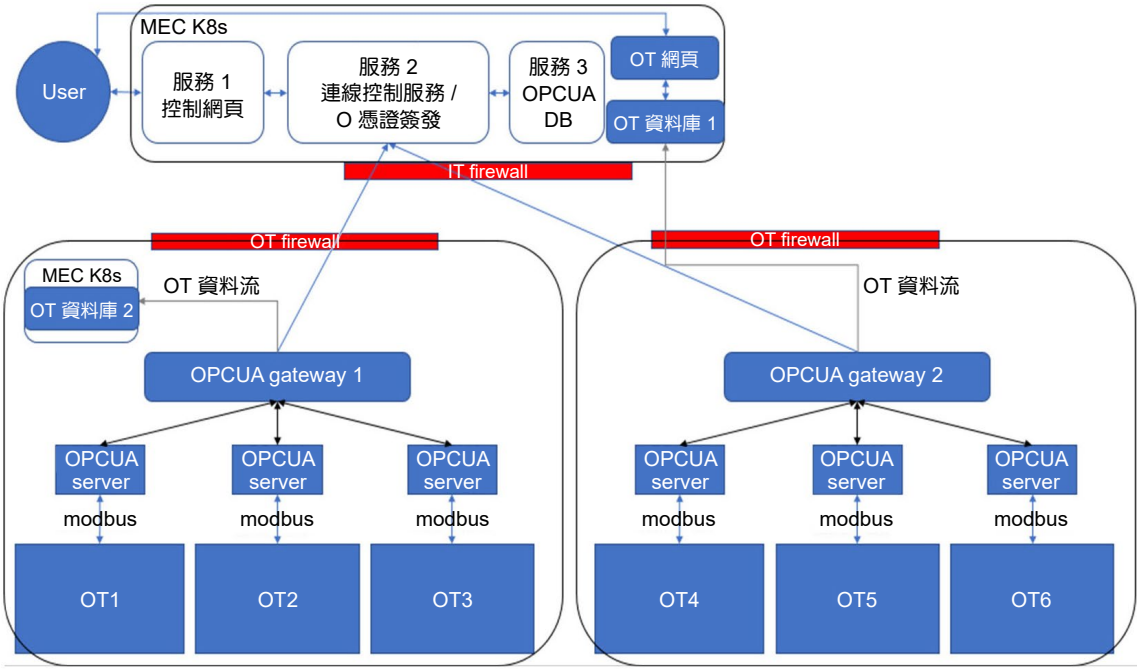

圖 11. 閘道器上下層架構示意圖。

(1) 基於資訊安全服務之 MEC 架構

此架構重點為穩定性與輕量化，本研究選擇使用 Docker 來獨立 Flask、MongoDB 等等應用服務成基本單位，以此提高交付軟體的速度，將各服務包裝成容器再交由 Kubernetes 管理，而 Kubernetes 不只能夠自動部屬設定好的環境 (deployment, StatefulSet, etc..)，同時也可以使用動態持續性的安全檢查 (liveness probe)，滿足網路安全架構強化的需求，更詳細的 Kubernetes 部屬與設定會在 (2) 詳細說明。使用 Flask 輕量化後端與 MongoDB 的 Index Search 機制來達到資料快速存取的功能，由 uWSGI 框架串接後端與 Nginx 反向代理伺服器完成保護網頁負載均衡，由圖 12 中可大致檢視其互動性。

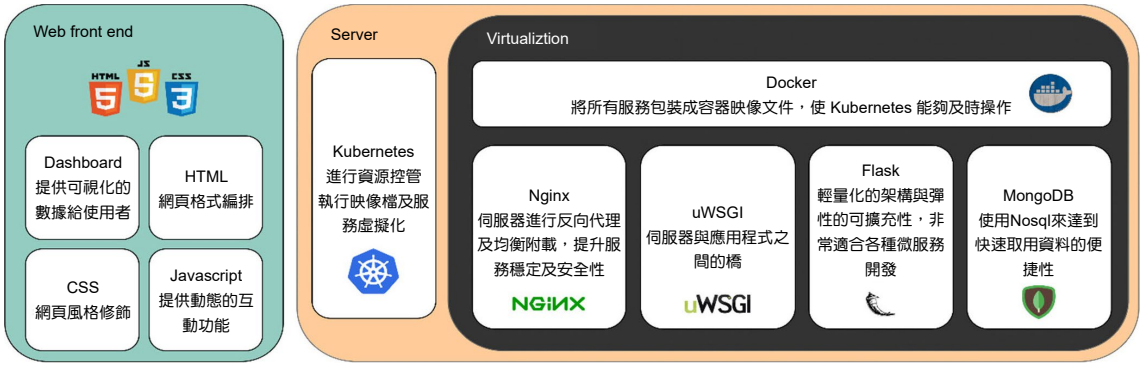

圖 12、應用服務架構圖。

(2) Kubernets 實現容器管理與安全穩定機制

Kubernetes 在雲服務上不只有著輕量化的優勢，生命週期檢測 (liveness probe) 也提供很優秀的系統穩定性。當生命週期檢測偵測到異常時，Kubernetes 會創建新的 container，確

保應用服務可正常運行，當我們所建立的 Mongo 資料庫或者 Flask 後端失去連線時，Health Check 會向我們回報與該容器之間的溝通狀況出現異常，如圖 13，可以看到伺服器延遲狀況、檢查尋訪週期以及訪問成功與失敗之次數。

Kubernetes 由兩大部分組成[2]，第一部份為 Master Node 負責整個 Cluster 控管、排程、權限管理及系統資訊，在本研究中用於管理 Flask、Keycloak 跟 MongoDB 等等服務的同步與架構之間的功能控管，第二部份為 Worker Node，負責運行容器間的通訊與功能，而我們設定 Worker Nodes 可以偵測容器中的 Pods (Kubernetes 中運行環境的最小單位，其中可包含多個容器) 是否發生 Crash、Failed，當非正常性的終止運行時，我們建構的 Worker Nodes 會幫我們自動偵測，通報 Master Node，讓 Master Node 尋找適合的新部屬環境，再交給負責該環境的 Worker Node 執行部屬，創建一個新的 Pod，確保 Pod 運行的數量與設定檔的指定的數量相同，讓 Flask 與 MongoDB 或者與其他的服務可以保持穩定安全的資料流，滿足了 IEC 62443 2-4 SP 03-網路架構圖及網路設備安全控制、設定、檢查機制。

在 Pods 之中的 Containers 使用了 Loopback 機制去進行網路的溝通，同一個 Container 之中的服務都是共用同一個 Namespace，而 Nodes 中的 Pods 網路溝通是不需要 NAT 的，因此我們利用了這個機制把不同功能取向的服務區別出來，Flask 與 MongoDB 各自獨立一個 Pod，而各終端也有其專屬的 Node 去使用。依靠著這個分割機制與上述提到的生命週期檢測，能讓 Flask、Mongo 與其他服務之間的架構更加穩定與安全，不會因為一個服務的錯誤而導致了整個系統的崩潰。

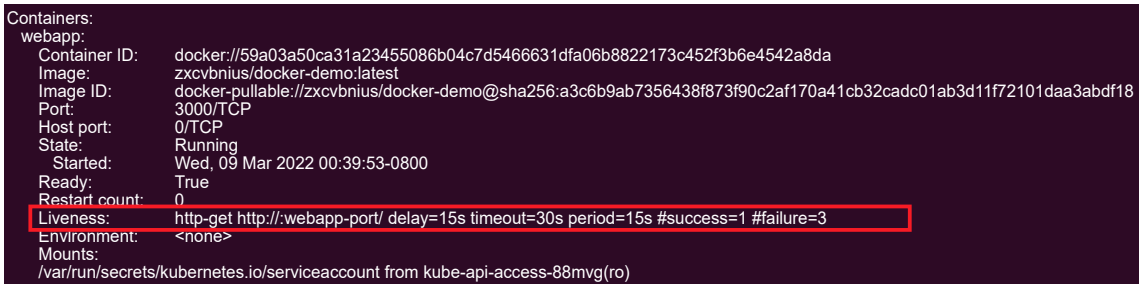

圖 13. 在 Liveness 欄位裡，可以檢視 Health check 的狀態。

• 智慧製造場域資安權限管控系統

本研究第一期已使用 Keycloak 作為實現 SSO (single sign-on) 的身份驗證系統，透過 FreeIPA 驗證使用者帳號密碼以達到 IEC-62443-2-4 規範中的 SP.09.02，並將結果傳回至 Keycloak，產生對應的 Token (該 Access Token 可依據不同場域的情景設定不同的存取效期，以此利於資安風險的管控。此外，身份管理系統則以支援 LDAP (lightweight directory access protocol) 協定的 FreeIPA 開源軟體來實現，用以儲存本研究中各個不同身份的帳號與密碼，以利於統一的管理與控制，透過結合 Keycloak 以及 FreeIPA，來達到 IEC-62443-2-4 中的使用單個整合數據庫管理使用者和服務帳戶並且在此資料庫定義使用者的操作權限。

對於系統的安全防護，除了原先已採用的服務、管理分離建置 (Web Server、FreeIPA 兩者間以 Firewall 作區隔)，並由 Router 控制存取 IP 來降低系統被外部入侵的風險之外，對系統內部使用者的登入，現已針對 Realm 使用 Brute Force Detection (暴力破解檢測)，系統一旦檢測到使用者密碼連續輸入失敗三次，便將該使用者帳號鎖定十五分鐘，甚至也能夠將使

用者永久封鎖，延遲有心人士對系統進行暴力破解成功的時間，如圖 14 所示，此部分已達到IEC-62443-2-4 規範中的 SP.09.02－服務提供商應有能力確保內置管理員帳戶被禁用。

此外，登入步驟也加入雙重驗證 (two factor authentication, 2FA) 機制，使用者必須通過兩種的認證機制之後，才能得到授權。也就是帳號密碼的正確輸入，以及一次性密碼、動態密碼 (one-time Password, OTP) 驗證，如圖 15 所示。OTP 得以用來作為驗證機制的原因，便是因為此密碼為動態產生，於某一時間區段內有效，並且僅能被使用一次，難以被暴力手段破解，此機制更提升了系統安全程度。2FA 機制的目的是為了減少單一驗證機制被破解（例如使用者帳號密碼外洩）導致資料被外洩的機會。當使用者輸入帳號密碼登入後，必須使用行動裝置的 Google Authenticator Application 或 FreeOTP Application 進行 E-mail 驗證，方可完成系統登入。

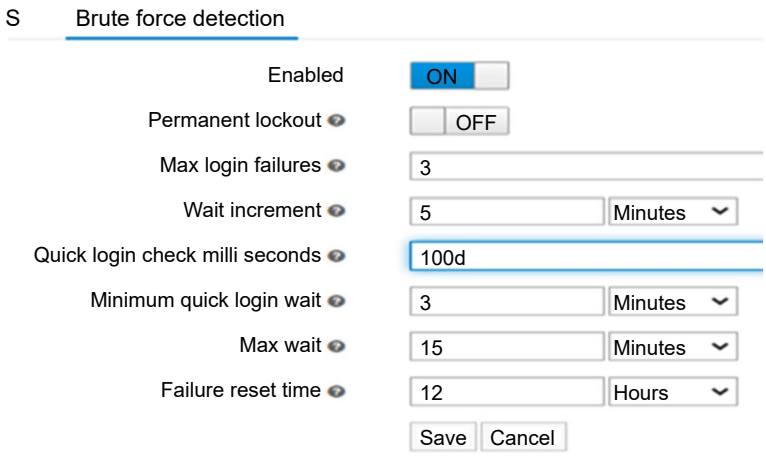

圖 14. Keycloak Brute Force Detection 設定，以此延遲被暴力攻擊破解。

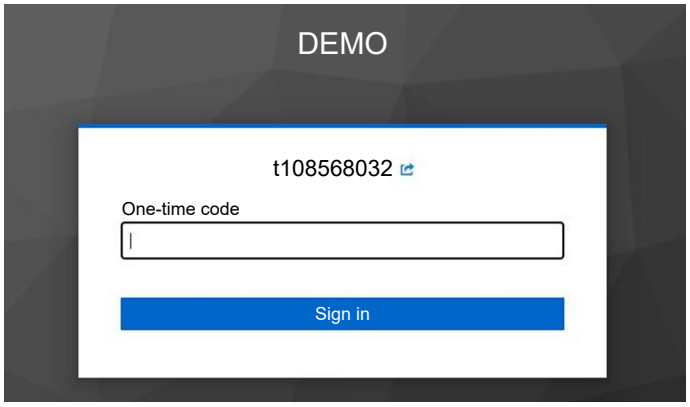

圖 15. 使用者登入 Keycloak 後，必須再透過 2FA 驗證，輸入 E-mail 中的 OTP，完成登入。

本研究之本期安全目標以 Security 為主 (亦即人員與設備安全)。配合 IEC-62443-2-4 中對於資訊安全的定義－成功建立資料防護安全。(例如：使用 Https 提供 Authentication、存取控制、權限管理的安全，避免 http 可能遭受的 Clickjacking attack、Downgrade attack 等攻擊，以達到 IEC-62443-2-4 標準中的 Security 防護)。同時，在 Keycloak 中記錄了 Access

Log，以及記錄了相關的資訊，如 Client (場域)、User (使用者)、IP Address 以及關於請求響應的詳細訊息，以此儲存為 Log 記錄。倘若在未來發生重大資安事件時，可透過審查該 Log 紀錄，及時迅速的查明出現資安事故的具體原因，以此作為漏洞管理的重要依據，便可達到 IEC62443-2-4 裡的收集日誌紀錄，並且日誌紀錄裡包括了成功和無效的登陸等等的資訊。

在系統架構層面，為了符合 IEC-62443-2-4 SP.09.01，已進一步將各個 OT 設備對應的服務進行拆分，落實分離式架構的設計，使其各自獨立負責單一任務，避免因其中一個服務出錯而影響其他的服務，出現超載負荷、程式故障的問題，也方便日後再進行開發、維護和佈署。再者，以資料安全性角度而言，由於每個 Database 也是基於單一的場域，當有攻擊者盜取了某個場域的資料，另外兩個場域的資料可以免於被竊取的災難，有分散風險的作用。如圖 16 所示，各 OT 設備擁有各自的 API 與 DB，甚至互動 (Web、GUI) 服務，所有使用者再透過整合入口網站來存取，且僅能存取已被授權的合法範圍設備資料。

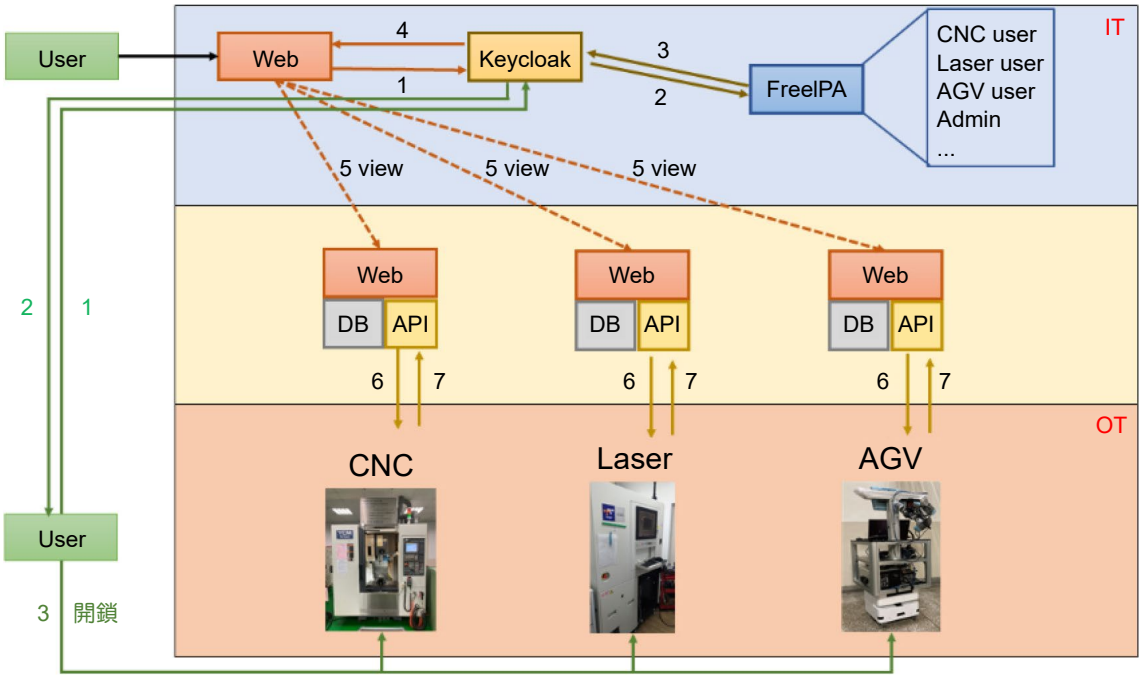

圖 16. 分離式系統架構。系統中 OT 設備系統各自獨立運作，互不影響。

參考文獻

1. Paul Loh Ruen Chze, Kan Siew Leong, Ang Khoon Wee, Elizabeth Sim, Kan Ee May, Yong Jun Jie , Hing Siew Wing, “Secured IoT Gateway For Smart Nation Applications”, 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), 25-29 June (2018).
2. Nigel Poulton, *The Kubernetes Book*, Amazon (2021).
3. Amit M Potdar, Narayan D G, Shivaraj Kengond, Mohammed Moin Mulla, *Procedia Computer Science*, **171**, 1419 (2020).
4. Wetter, D. (2021). Docker-Security. OWASP Docker-Security Top 10. Please refer to the website: https://github.com/OWASP/Docker-Security
5. Paul Loh Ruen Chze, Kan Siew Leong, Ang Khoon Wee, Elizabeth Sim, Kan Ee May, Yong Jun Jie , Hing Siew Wing, “Secured IoT Gateway For Smart Nation Applications”, 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), 25-29 June (2018).

6. Yuan Ko, “Architecture of three Federated learning”, Disassembly. Please refer to the website: https://medium.com/disassembly/architecture-of-federated-learning-a36905c1d225
7. Recurrent Neural Network (LSTM) with Keras Framework. Please refer to the website: https://github.com/Parasgr7/Google-Stock-Price-Prediction#recurrent-neural-networklstm--with-keras-framework
8. H. Brendan McMahan, Eider Moor, Daniel Ramage, Seth Hampson, Blaise Aguera y Arcas, *In Artificial Intelligence and Statistics*, 1273 (2017).
9. H. Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, Blaise Aguera y Arcas, “Communication-Efficient Learning of Deep Networks from Decentralized Data”, *the 20 th International Conference on Artificial Intelligence and Statistics (AISTATS)*, **54**, (2017).
10. You Jun Kim, Choong Seon Hong, “Blockchain-based node-aware dynamic weighting methods for improving federated learning performance”. *2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS)* IEEE. September 18-20 (2019,)
11. Vale Tolpegin, Stacey Truex, Mehmet Emre Gursoy, Ling Liu, “Data poisoning attacks against federated learning systems”, *In European Symposium on Research in Computer Security, September* 14-18 (2020).
12. Wenqi Wei, Ling Liu, Yanzhao Wu, Gong Su, Arun Iyengar, “Gradient-leakage resilient federated learning”, *2021 IEEE 41st International Conference on Distributed Computing Systems (ICDCS)*, .IEEE, July 7-10 (2021,)

作者簡介

陳彥霖先生為國立陽明交通大學電控工程博士，現為國立臺北科技大學資訊工程特聘教授。
Yen-Lin Chen received his Ph.D. in Electrical and Control Engineering from National Yang Ming Chiao Tung University. He is currently a Distinguished Professor in the Department of Computer Science and Information Engineering at National Taipei University of Technology.

楊士萱先生為美國密西根大學電機與計算機科學博士，現為國立臺北科技大學資訊工程教授。
Shih-Hsuan Yang received his Ph.D. in Electrical Engineering and Computer Science from University of Michigan, USA. He is currently a Professor in the Department of Computer Science and Information Engineering at National Taipei University of Technology.

陳金聖先生為國立陽明交通大學機械工程博士，現為國立臺北科技大學自動化所特聘教授。
Chin-Sheng Chen received his Ph.D. in Mechanical Engineering from National Yang Ming Chiao Tung University. He is currently a Distinguished Professor in the Graduate Institute of Automation Technology at National Taipei University of Technology.

何昭慶先生為國立臺灣科技大學電機工程博士，現為國立臺北科技大學製造科技研究所教授。
Chao-Ching Ho received his Ph.D. in Electrical Engineering from National Taiwan University of Science and Technology. He is currently a Professor in the Graduate Institute of Manufacturing Technology at National Taipei University of Technology.

林志哲先生為國立成功大學機械工程博士，現為國立臺北科技大學自動化所教授兼所長。
Chih-Jer Lin received his Ph.D. in Mechanical Engineering from National Cheng Kung University. He is currently a Professor and Director in the Graduate Institute of Automation Technology at National Taipei University of Technology.

王正豪先生為國立台灣大學資訊工程博士，現為國立臺北科技大學資訊工程教授。
Jeng-Haur Wang received his Ph.D. in Department of Computer Science and Information Engineering

from National Taiwan University. He is currently a Professor in the Department of Computer Science and Information Engineering at National Taipei University of Technology.

曾釋鋒先生為國立陽明交通大學機械博士，現為國立臺北科技大學機械工程副教授。
Shih-Feng Tseng received his Ph.D. in Mechanical Engineering from National Yang Ming Chiao Tung University. He is currently an Associate Professor in the Department of Mechanical Engineering at National Taipei University of Technology.

張世豪先生為英國利物浦約翰摩大學計算與數學科學博士，現為國立臺北科技大學資訊工程助理教授。
Shih-Hao Chang received his Ph.D. in Computing and Mathematical Sciences from the University of Liverpool in the United Kingdom. He is currently an Assistant Professor in the Department of Computer Science and Information Engineering at National Taipei University of Technology.

劉佳明先生現為國立臺北科技大學資訊工程博士班學生。
Chia-Ming Liu is currently a Ph.D. student in the Department of Computer Science and Information Engineering at National Taipei University of Technology.

余兆偉先生為國立臺北科技大學資訊工程博士，現為國立臺北科技大學資訊工程博士後研究員。
Chao-Wei Yu received his Ph.D. in Computer Science and Information Engineering from National Taipei University of Technology. He is currently a Postdoctoral Researcher in the Department of Computer Science and Information Engineering at the National Taipei University of Technology.