具工控資訊安全之智慧製造系統研究

Study on Smart Manufacturing System with Industrial Control Information Security

姚賀騰、郭秉寰、賴伯洋
Her-Terng Yau, Ping-Huan Kuo, Po-Yang Lai

該研究成果主要圍繞資訊安全建設與智慧製造的結合展開。本研究中智慧製造技術包括刀具磨損預測和顫振識別，並利用機器學習和資料分析實現更高的處理精度和資料預測。利用網路防護的視角，構建一套資訊安全架構，建立包括 VPN、防火牆、處理資料的伺服器等多層防護機制的防護體系，監控資料流程。通過帳號、系統、通訊、整合資訊流等，研究防護和漏洞掃描、導入資訊和通訊資料包分析等技術和機制，逐步探索從傳統方法到最新的機器學習和深度學習等與智慧生產線相關的先進資訊安全技術，利用漏洞掃描和處理品質等資訊安全測試方法，驗證生產線開發的各種資訊安全演算法的正確性和安全性。

The research results mainly focus on the combination of information security construction and smart manufacturing. The smart manufacturing technology in this study includes tool wear prediction and chatter recognition and uses machine learning and data analysis to achieve higher processing accuracy and data prediction. Using the perspective of network protection, build a set of information security frameworks, establish a protection system including VPN, firewall, server for data processing and other multi-layer protection mechanisms, and monitor data flow. Through the account, system, communication, integrated information flow, etc., research technologies and mechanisms such as protection and vulnerability scanning, import information and communication data package analysis, and gradually explore advanced technologies related to smart production lines, from traditional methods to the latest machine learning and deep learning. Information security technology uses information security testing methods such as vulnerability scanning and processing quality, to verify the correctness and safety of various information security algorithms developed by the production line.

一、目標

利用維運技術 (operational technology, OT) 及資訊技術 (information technology, IT) 之技術結合，使整個場域在達成具備智慧製造[1] 的高精密度加工與數據分析時，也能使重要資料受到保護。

二、介紹

因應工業 4.0 的到來，傳統加工製造業也迎來了新的改革。現今許多工具機具備自動化加工能力，也讓許多加工問題受到更多關注，像是刀具磨耗[2] 與顫振[3] 問題，在自動化生產的過程中這些健康診斷的數據分析是不能忽視的。以往這些問題都是由老師傅的經驗決定，但隨著感測器能偵測到的數據越來越多、電腦的運算能力越來越強大，我們已能運用機器學習演算法處理與分析這些資料，並達成補償回授及問題預測的實際應用。近年來，廣泛應用網路使電腦發明後就存在的資安議題變得很嚴苛。在智慧製造的範疇中，感測器的數據、機台的資料，或利用演算法得出的數據，它們都是重要且很具影響力的資料，保護這些資料不受到竊取或修改是不容忽視的問題。儘管在資安上的付出仍可能受到攻擊，但我們應持續維護與強化相關防護，讓攻擊者因代價過高而放棄。近年來物聯網 (IOT) 與智慧製造逐漸盛行，在國內業界利用聯網與自動化技術提高生產與製造效率和降低成本。但聯網也伴隨著資安問題的威脅，讓駭客有機會透過連網機制入侵製造場域。相關業者於執行數位化與網路化的升級之後，再次在資安上面對新的問題。陸續發生的案例都說明了國內各大產業迎來了智慧化後的資安問題。根據 IBM「2020 資安關鍵防護策略」，臺灣因為資安議題所造成的營利損失就高達新台幣 8,100 億元，這快要是臺灣 5% 的國內生產總值 (Gross Domestic Product, GDP)。由此可見，在智慧製造場域中加入資安機制進行資訊系統防衛是一件刻不容緩的課題。

本校國立中正大學前瞻製造系統頂尖研究中心 (AIM-HI) 積極將掌握的關鍵自主技術產業化，建立一條具資安環境之智慧模擬生產線。目前已經建置完成之產線如圖 1 所示。本研究在既有自動化製造產線上，加入資安方法與設備，發展安全的網路與通訊環境，進而整合出具安全之智慧製造加工系統，達到由單機到整線智慧化與安全之目的，呼應工業 4.0 精神與本國發展自主技術場域之目標。目標是超前佈署，解決未來台灣智慧製造場域會面臨的資安危機，並發展台灣在地化的工控資訊安全之智慧製造產線。

圖 1. 國立中正大學智慧化加工產線。

三、資安防護架構圖建置

本研究設計資安防護架構如圖 2，可以很明確的釐清 IT 及 OT 區域的資料流向情形，此架構圖也清楚了表示防護機制的應用在可能的網路入侵處進行監控過濾及阻斷。

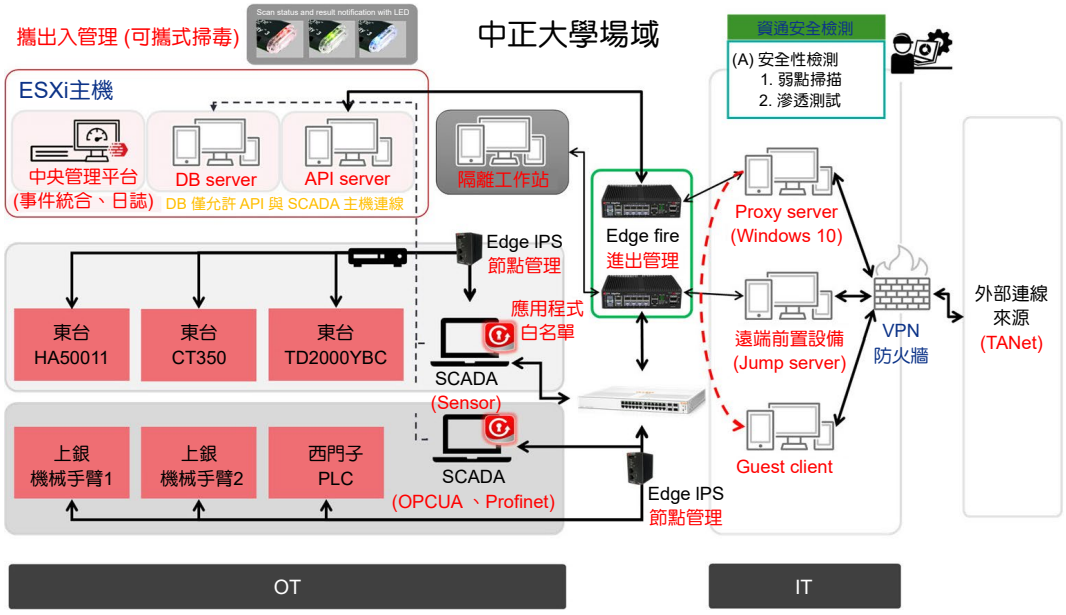

圖 2. 資安防護架構圖。

在技術方面智慧製造的技術在第四章及第五章的技術會建立在架構圖中的 OT 區域，在第四章的資安技術會建立在架構圖的 IT 區域。在智慧製造技術落實的同時進行資安的全面防護。

四、工控系統資安防禦建置

本研究針對 IT/OT 場域進行資安防禦建置。在場域中，會遇到的資安問題主要分為三種：駭客透過網路入侵場域、機邊設備夾帶病毒或惡意程式、以及惡意人士非法入侵。因此本研究針對以上三種問題進行資安防禦。

1. Database Server

在場域中，會由機邊設備將機台資料與感測器資料上傳至資料庫，Database Server 建置於 OT 場域中 ESXi 主機上，使用的資料庫程式為 MySQL。MySQL 不僅建置方便快速，且能管理使用資料庫用戶的存取權，可達成資料安全防護上分層管理。而在資料的保存上，保留線上查詢紀錄 30 天 (離線 90 天)，以便日後發生資安問題時可了解損害範圍。在個別用戶規範上，能達到依據特定身分存取特定範圍的資料，將權限最小化。經過 10 天不間斷測試，資料庫能經起每秒 1500 個以上查詢指令。各資料表欄位圖 3、圖 4 所示。

	資料表	動作	資料列數	類型	編碼與排序
☐	CT350	瀏覽 結構 搜尋 新增 清空 刪除	1	InnoDB	utf8_general_ci
☐	HA50011	瀏覽 結構 搜尋 新增 清空 刪除	1	InnoDB	utf8_general_ci
☐	TD2000YBC	瀏覽 結構 搜尋 新增 清空 刪除	1	InnoDB	utf8_general_ci
	3 張資料表	總計	3	InnoDB	utf8_general_ci

圖 3. 資料庫中儲存不同機器資訊之資料表。

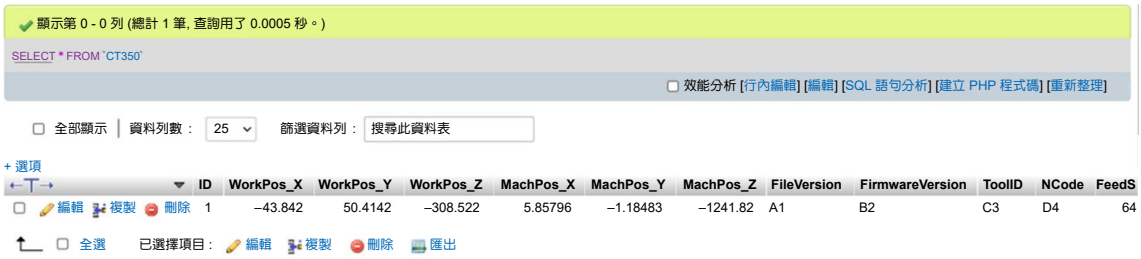

圖 4. 資料表中儲存之資料欄位。

2. 防火牆

在面對網域外的連線管理，本研究使用 pfsense5 作為防火牆來管理。pfSense 是一套免費開源的防火牆及路由系統，以 FreeBSD 系統為核心，可以結合 VPN 來對網域外的連線做存取管理。此外，還使用了 pfsense 的其他功能，例如：監看被防火牆規則阻擋下來的流量、透過路由功能與防火牆規則實現白名單機制 (如圖 5)。

圖 5. pfsense 內部防火牆規則設置實現白名單機制。

3. WireGuard VPN[6]

WireGuard 為一款開源的 VPN 程式，使用者透過管理員提供的合法憑證即可連線進入網域內。使用憑證皆由管理員進行配發，為一使用者對一 IP 的方式，便於權限控管。WireGuard 運用 Curve25519 進行金鑰交換，ChaCha20 用於加密，Poly1305 用於資料認證，BLAKE2 用於雜湊函式運算。工作原理為交握成功後，內部 kernel 會建立各自的通道 (tunnel) 將數據加密後發送給對方，接收者在經過解密後訪問目的地 IP (如圖 6)。

4. Proxy Server[7]

為了確保 DB server 內的資料安全，因此限定所有透過 VPN 抓取機器資料的使用者僅能透過 Proxy server 做資料讀取，作業系統為 ubuntu，且使用 Python 內的 flask 套件做到 Proxy server 的功能。主要功能為做為一個代理伺服器，橋接 API server 與 VPN user (如圖 7)，達到資料庫資料與使用者實體隔離。

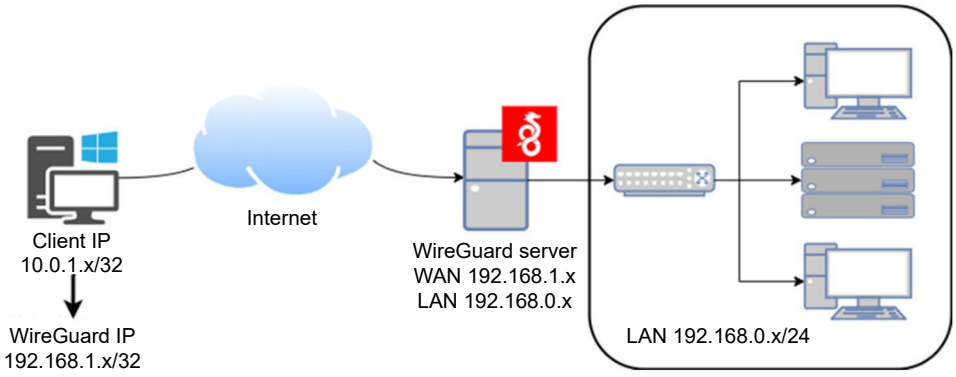

圖 6. WireGuardy 資料流向圖。

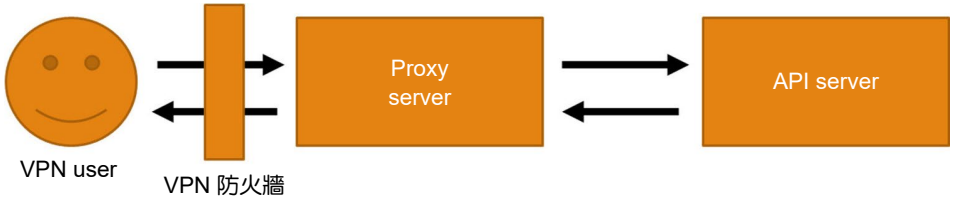

圖 7. Proxy server 資料流動架構圖。

5. Jump Server

為了方便管理員從遠端操縱場域內電腦設備進行管理，同時又能達到場域內的安全，因此建置了 Jump server 來當作管理員經由 VPN 進入場域內管理設備的跳板機。目前建置了兩台 Jump server，分別管理 DB server 與 API server，作業系統皆為 Windows 10。管理員可經由存取這兩台 Jump server 的 VPN 憑證，再經由 RDP 或 SSH 功能透過隔離工作站遠端管理 DB server 與 API server (如圖 8)。

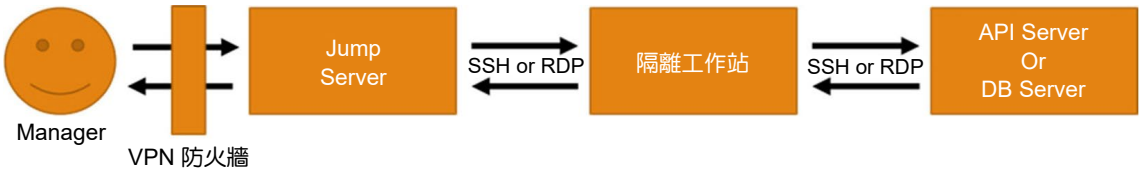

圖 8. Jump server 資料流動架構圖。

6. Guest Client

使用者透過 VPN 進入網域後，權限最低的訪客會連接到 Guest client，Proxy server 會主動提供符合 Guest client 權限的資料 (如圖 9)。再經 Guest client 傳送資料給權限較低的訪客。

7. EdgeFire

EdgeFire 是工業用防火牆，透過網路分段和隔離將網路分為不同的控制區域，以保護關鍵生產設備線上威脅防禦防火牆，同時提供虛擬補丁 (virtual patch) 機制。防火牆可保護弱系統，阻絕利用已經發生的網路攻擊。防火牆可在監控和防護兩種模式之間切換，大幅提高

圖 9. Guest Proxy 資料流動架構圖。

安全性及保持生產效率。透過分析封包內資訊，防火牆能偵測出是否為惡意流量以阻隔攻擊的發生。

8. 機邊設備資安防護

在機邊設備防護上，本研究使用可攜式掃毒棒與應用程式白名單來進行防護，當場域中需增加機邊設備時，須先經由掃毒棒確認設備並無夾帶病毒。並且進行應用程式白名單的管理，確保惡意程式無法在場域內執行。

五、刀具磨耗預測[4]

在智慧製造關鍵技術當中，刀具磨耗被視為健康診斷的標準之一。故 OT 領域中的研究目的之一是開發透過人工智慧預測刀具磨耗之模型。首先，為蒐集模型建模與訓練的資料，在銑床上進行切削實驗，並將三軸加速規裝設在主軸上蒐集震動訊號。刀具磨耗值則是透過電子顯微鏡與本研究所開發之線上刀具磨耗量測系統進行量測與紀錄。接著將資料進行預處理後，導入模型進行訓練。刀具磨耗預測系統實驗架構如圖 10 所示。

1. 震動訊號預處理

在使用加速規擷取震動訊號時，因機台特性與環境雜訊的影響，使訊號包含著大量雜訊。為了降低雜訊影響，本研究根據刀具通過頻率使用低通濾波器進行濾波。低通濾波器可將容許低頻訊號通過，並減弱高於截止頻率的的訊號，以此增強訊號的特徵，震動訊號過濾前後的情況如圖 11 所示。

2. 線上刀具磨耗量測系統

本研究也開發一套線上刀具磨耗量測系統，目的是為了協助建立刀具磨耗預測技術。一般之刀具磨耗量測需藉由拆卸刀具至顯微鏡下進行量測，但此舉將影響刀具加工的狀態與連續性，且操作上較為費時。此裝置開發可解決前述問題，進而提升預測模型之準確度與縮短量測時間。在影像檢測上，我們使用 Canny 邊緣檢測技術與 Hough 轉換來輔助計算刀具磨耗值，線上刀具磨耗量測示意圖如圖 12 所示。

3. 刀具磨耗預測模型建立

在建構模型時，首先導入震動訊號作為模型輸入、刀具磨耗值作為輸出，將資料彙整成數據集後，在切割成訓練集與驗證集。接著選用隨機森林回歸 Random Forest Regression (RFR) 演算法作為模型的架構進行訓練。最後使用 k-fold cross-validation 進行交叉驗證，確保模型訓練效果。模型建構流程圖如圖 13 所示。

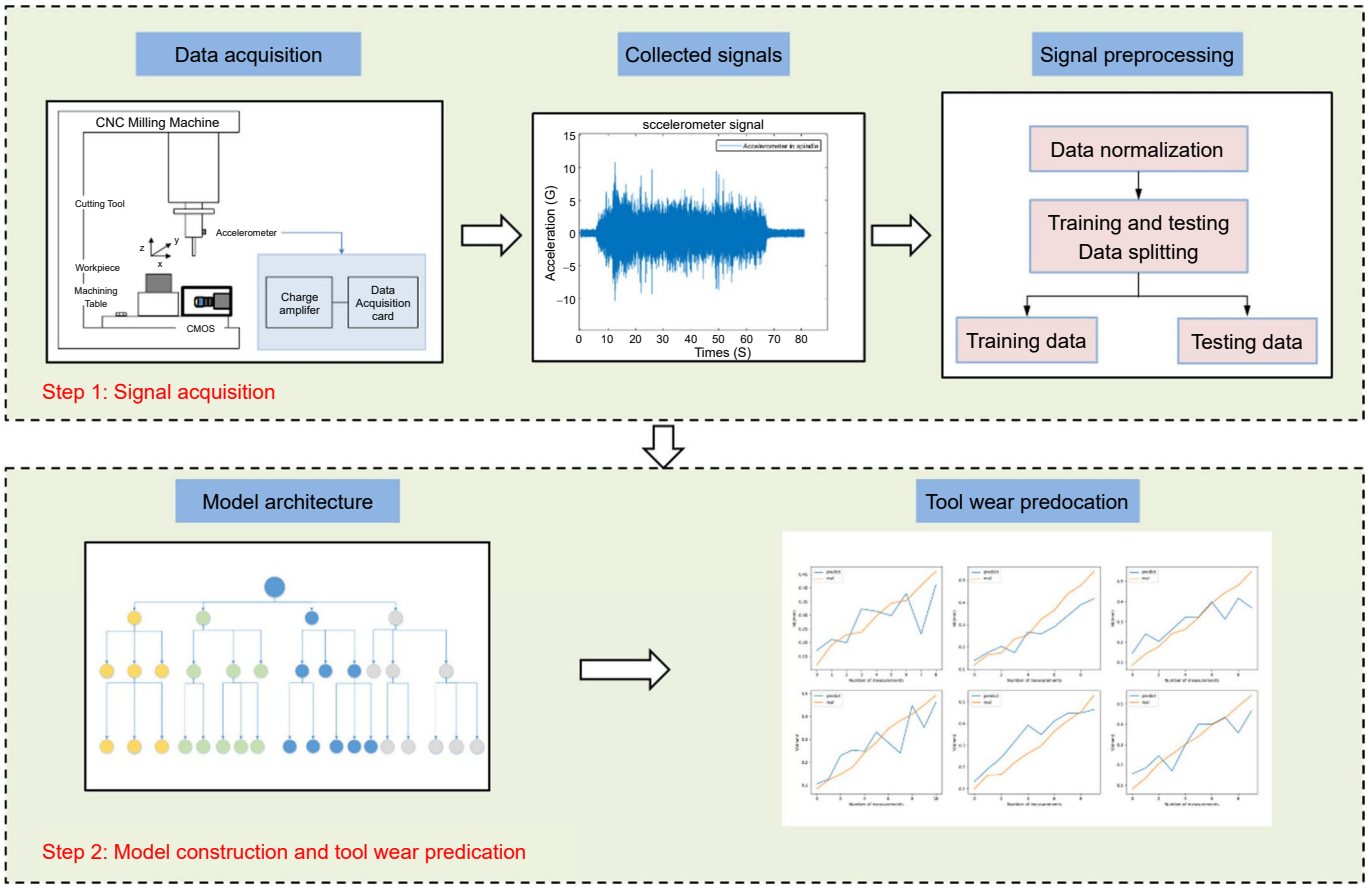

圖 10. 刀具磨耗預測系統實驗架構[4]。

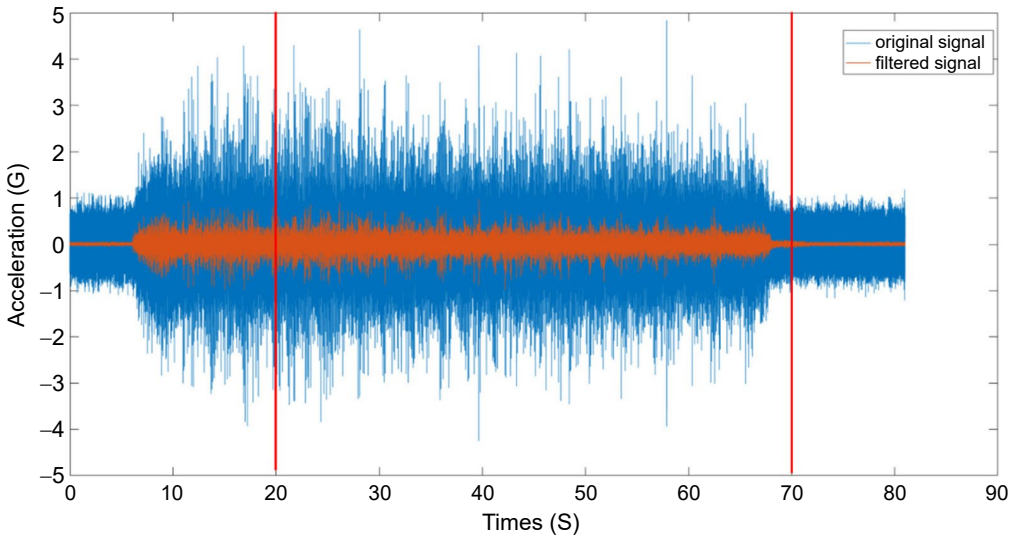

圖 11. 濾波後的震動訊號圖[4]。

4. 顫震識別系統開發[3]。

刀具顫振是刀具在切削過程中因刀具磨損、脆性斷裂或激發共振頻率所導致。此現象會導致加工品質下降，進而影響智慧產線的運行。本研究使用分數階卷積神經網路來進行刀具

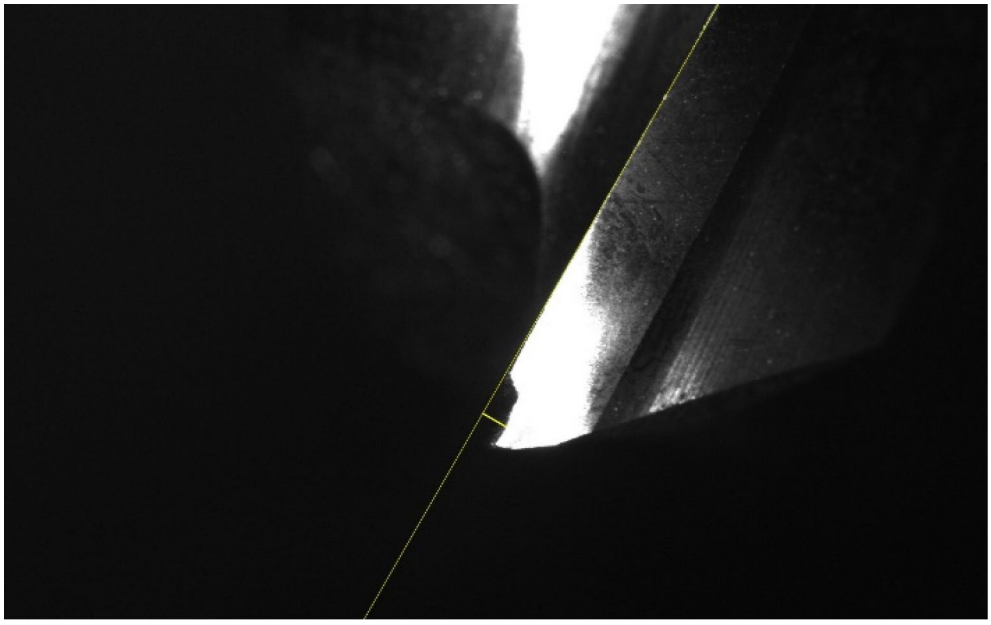

圖 12. 刀具磨耗量測拍攝[4]。

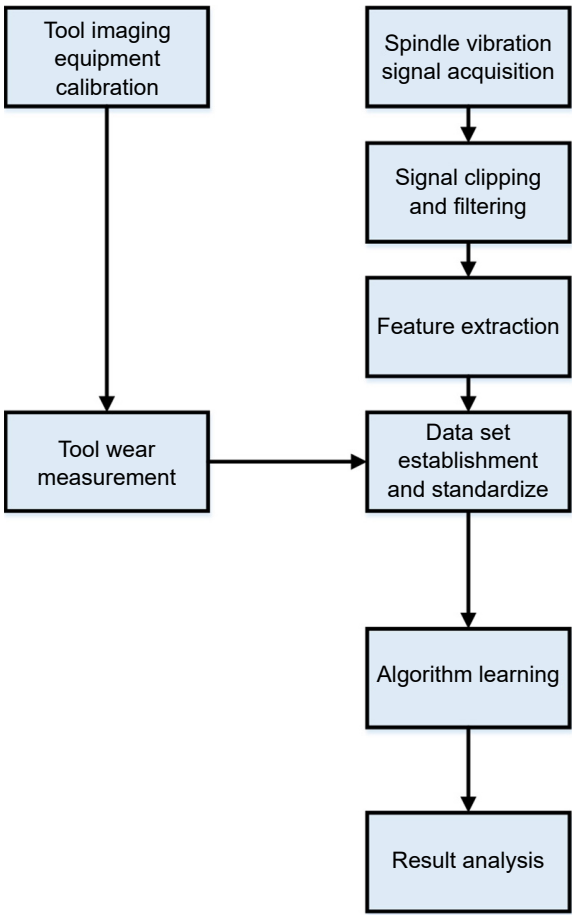

圖 13. 模型建構流程圖。

顫震識別。首先使用加速規擷取機台加工時的震動訊號，並對訊號進行處理，轉變為具有混沌動態誤差映射特徵之二維圖像。再以分數階卷積神經網路進行訓練與驗證，以此判斷顫振之發生。在分數階混沌同步動態誤差訊號處理[1] 方面，先預處理一維震動訊號。萃取訊號之特徵與拆解使特徵個別獨立，並取出較低維度的資訊。利用訊號處理方法達到強化訊號可視性之目標。輸入對於混沌理論來說影響幅度很大，透過混沌系統讓加工時之微小振動變化產生比較容易辨別之特徵，以分數階混沌系統動態誤差映射分佈圖 (chaotic dynamic error map) 做為識別特徵。同步動態誤差映射方程式如式 (1) 所示：

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{bmatrix} = \begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} + \begin{bmatrix} -x_2 x_3 \\ x_1 x_3 \\ \frac{1}{3} x_1 x_2 \end{bmatrix} \tag{1}$$

其中式 (1) 中 a、b 及 c 為參數權重，參數權重在 $a > 0$、$b < 0$ 及 $0 < a < (-b + c)$ 時代表系統具有奇異吸引子之特性。將分數階 Grunwald-Letnikov (G-L) 微積分模型，如式 (2)，與 Chen-Lee 混沌系統相互合併，可以非常有效的將特徵提取能力提升，讓輸出的形式特徵更加明顯且獨立，而 G-L 分數階微積分模型如下式所示。

$$D^{\sigma}(x^m) \approx \frac{\Gamma(m+1)}{\Gamma(m-\alpha+1)} x^{m-\sigma} \tag{2}$$

一般整數階微分行為是在 σ 為 1 時，在 $0 < \sigma < 1$ 時為分數階微分之行為。為了要求得分數階 Chen-Lee 混沌動態誤差，把式 (1) 中運用式 (2) 的計算，可得分數階 Chen-Lee 混沌系統動態誤差方程式如下式所示。

$$\begin{bmatrix} D^{\sigma} x_1 \\ D^{\sigma} x_2 \\ D^{\sigma} x_3 \end{bmatrix} \approx \begin{bmatrix} a' & 0 & 0 \\ 0 & b' & 0 \\ 0 & 0 & c' \end{bmatrix} \begin{bmatrix} {x_1}^{1-\sigma} \\ {x_2}^{1-\sigma} \\ {x_3}^{1-\sigma} \end{bmatrix} + \begin{bmatrix} \frac{-\Gamma(1) x_2 x_3 {x_1}^{-\sigma}}{\Gamma(1-\sigma)} \\ \frac{\Gamma(1) x_1 x_3 {x_2}^{-\sigma}}{\Gamma(1-\sigma)} \\ \frac{\Gamma(1) x_1 x_2 {x_3}^{-\sigma}}{3\Gamma(1-\sigma)} \end{bmatrix} \tag{3}$$

六、相關成果展示

此研究成果已透過可視化介面開發如圖 14，將研究成果的數據及資安監控技術架設在本研究開發之網頁程式中。利用此可視化界面可清楚看到個工具機運轉時之數據如圖 15，磨耗情形及顫振狀況。後續將會把開發之技術彙整到此介面，讓整個智慧生產線能在這個介面上一目瞭然。可視化界面的應用也讓我們離自動化生產又邁進了一大步。相信在未來的工廠應用中都會逐漸趨向自動化生產技術及場域可視化的顯示方式。

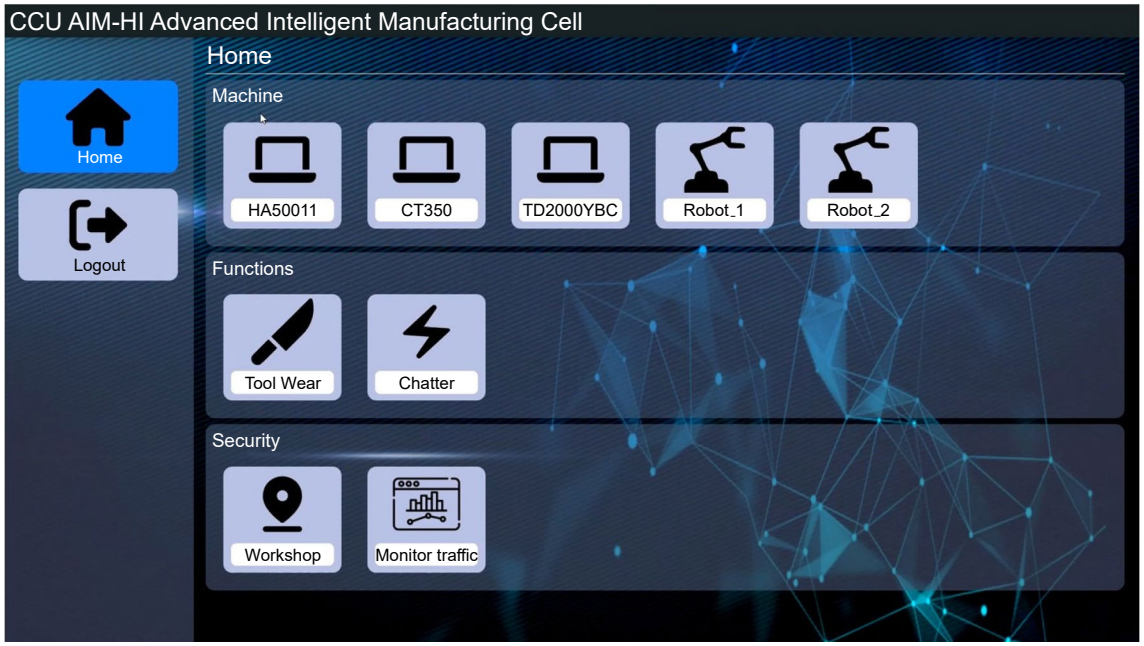

圖 14. 可視化界面。

圖 15. 工具機實際數據詳情。

七、結論

智慧製造系統的開發與資訊安全維護密不可分。運用上述的智慧製造技術與資安維護系統，對智慧化生產有著顯著的進步。刀具磨耗預測與顫振識別能有效地對工具機進行健康診斷，讓智慧化產線產出之工件維持高精度。隨著智慧製造的技術與資料資訊化，這些數位資產對於製造業者來說尤為重要。有了上述的資安技術，一些機器的數據、機器學習訓練後的權重資料，和資料正確性會有一定的保障。隨時間的推進，物聯網與資訊技術的持續發展會

導致生更多的資安議題，工業界必須持續地加強防護及更新，才能使資安技術實際落實。工業界在享受智慧製造帶來的數據決策效益時，也應持續精進資訊防護技術，才能確保整個場域的資訊安全程度。

參考文獻

1. Her-Terng Yau, Shang-Yi Wu, Chieh-Li Chen and Yu-Chung Li, *IEEE Transactions on Industrial Electronics*, **63** (6), 3824 (2016).
2. Ping-Huan Kuo, Chia-Yu Lin, Po-Chien Luan and Her-Terng Yau, *IEEE Sensors Journal* **22** (21), 20257 (2022).
3. An-Hong Tian, Cheng-Biao Fu, Xiao-Yi Su and Her-Terng Yau, *Journal of Low Frequency Noise, Vibration and Active Control* **38** (3-4), 953 (2019).
4. 林家宇, 姚賀騰, 基於時間延遲相平面重構之卷積神經網路於刀具磨耗預測之線上檢測研究. (2022).
5. P. SenthilKumar, M. Muthukumar, “A Study on Firewall System, Scheduling and Routing using pfsense Scheme”, Dec 14-15, *2018 International Conference on Intelligent Computing and Communication for Smart World (I2C2SW)*, 17 (2018).
6. Benjamin Lipp, Bruno Blanchet, Karthikeyan Bhargavan “A Mechanised Cryptographic Proof of the WireGuard Virtual Private Network Protocol”, June17-19, 2019 IEEE European Symposium on Security and Privacy,(2019).
7. Zhi-Li Zhang, Yuewei Wang, D.H.C. Du, *IEEE/ACM Transactions on Networking* **8** (4), 429 (2000).

作者簡介

姚賀騰先生為國立成功大學機械工程研究所博士，現為國立中正大學機械系教授。

Her-Terng Yau received his Ph.D. in Mechanical Engineering from National Cheng Kung University. He is currently a Professor in the Department of Mechanical Engineering at National Chung Cheng University.

郭秉寰先生為國立成功大學電機工程研究所博士，現為國立中正大學機械系副教授。

Ping-Huan Kuo received his Ph.D. in Electrical Engineering from National Cheng Kung University. He is currently an Associate Professor in the Department of Mechanical Engineering at National Chung Cheng University.

賴伯洋先生現為國立中正大學機械工程所研究助理。

Po-Yang Lai is currently a Rresearch Aassistant in the Department of Mechanical Engineering at National Chung Cheng University.