「儀器資訊安全」專題介紹

Special Issue Introduction of "Instrumentation Cyber Security"

客座主編－蔡孟勳教授
國立臺灣大學機械工程學系特聘教授

智慧製造的推動可望提升製造業的生產效率與附加價值，是企業轉型的助力。然而，智慧化的同時也帶來了一些潛在的資安風險，像是工業自動化及控制設備受到像勒索病毒等惡意軟體的威脅。緣此，本期以「儀器資訊安全」作為專題，介紹製造業、企業導入智慧製造所產生的問題與因應的資安強化技術。

專刊內容包含「從 IEC 62443 看儀器應具備的資訊安全功能」，說明連網的儀器，可根據 IEC 62443-4-2 七項基本要求來評估儀器應有的資訊安全功能，藉以判斷儀器是否能防止惡意的攻擊。「基於 API 解析及運用深度學習的工業自動化及控制系統惡意軟體偵測機制」則聚焦在針對智慧製造場域之端點防護提出惡意軟體的偵測機制，可避免惡意程式透過變種來躲過相關偵測，有效降低智慧場域內端點設備的資安威脅。

過去，運營科技 (operational technology, OT) 主要在隔離和相對獨立的環境中執行，著重於工業控制系統的操作和程序控制面向。資訊科技 (information technology, IT) 則著重於計算機與網路通用面向。一旦 OT 設備連上網路後，OT 場域將面臨和 IT 相同的資訊安全問題，然而，現有 IT 資安解決方案並無法完全適用於 OT 環境，故在不影響生產線營運與品質確保的情況下需發展 OT 環境所需的創新資安解決方案，以即時偵測、防護與應變於工控環境中成為目前急需解決的資安問題。本期專題中「IT/OT 資安技術與標準應用於航太級光學元件產線」、「符合 IT 與 OT 資安規範之半導體製程具可擴充性微隔離場域之資安系統架構設計」、「具工控資訊安全之智慧製造系統研究」、「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」，四篇文章分別以加入 IEC62443 系列標準之資訊技術系統的安全標準為基礎，於不同的場域，建立具有 IT-OT 整體考量之網路安全功能，以確保關鍵製程與環境參數資料的安全性與正確性。

台灣為 OEM/ODM 代工大國，為國內外產業指標大廠之重要供應鏈。盼透過此專刊，在作者群的介紹下，激發讀者們創新的研究想法與方向，共同投入研發與積極合作，以提升台灣製造業資安管理、推動智慧製造，適應外部市場各式需求。