供應鏈資訊安全管理強化

教戰手則

主辦單位：經濟部工業局　　執行單位：工業技術研究院

目錄

一、 智慧製造產業資安問題盤點 1

二、 跨廠區管理需求案例解析 7

(一) 群創光電 7

三、 設備連網遠端連線需求案例解析 15

(一) 新揚科技 15

(二) 銘異科技 24

四、 IT/OT 混合環境下 OT 創新解決方案需求案例解析 33

(一) 新漢 33

(二) 泓格科技 41

五、 結論與建議 50

圖目錄

圖 1、企業資安發展程度.....1
圖 2、製造業資安阻力與困難.....3
圖 3、資安戰情儀表板.....11
圖 4、資訊資產系統.....12
圖 5、智慧網管系統.....12
圖 6、企業資安成熟度持續升級.....14
圖 7、資安防護佈署導入.....17
圖 8、端點白名單防護.....18
圖 9、容錯機制提供不中斷服務.....19
圖 10、資安戰情管理.....21
圖 11、資安事件偵測與通報機制.....21
圖 12、資安成熟度提升.....23
圖 13、資安導入建議做法.....27
圖 14、OT 資安戰情中心.....30
圖 15、自動化資安通報系統.....30
圖 16、OT 場域佈署 20 個誘捕設備.....31
圖 17、企業資安評級結果.....32
圖 18、產線資安硬體防護架構.....36

圖 19、產線導入 OT 資安設備收集機台資料 36
圖 20、跨廠區整合企業資安戰情監控 38
圖 21、資安戰情室系統(威脅情資分析、設備機台資安狀態).....38
圖 22、企業資安成熟度提升.....40
圖 23、資安水準雷達圖.....43
圖 24、通信加密服務器硬體.....44
圖 25、IDS 入侵偵測系統 45
圖 26、安全威脅模擬系統.....46
圖 27、智慧工廠資安整合平台 47
圖 28、工控網路安全資安通報設備 48
圖 29、工廠資訊網路安全強化部署成果 49

一、 智慧製造產業資安問題盤點

臺灣身為 OEM/ODM 代工大國，為國內外產業指標大廠之重要供應鏈，乘著數位轉型腳步來提升產能與品質之際，工廠設備、系統開始連上網路，也同步開啟物聯網情境下的資安潛在風險。然企業資安的發展程度並未跟上腳步，大約 95%的企業(包含多數製造業)都是資安入門生，缺乏資安意識，或是對資安有認知卻不曉得資安如何下手，連基本資通安全流程或管理規章都不具備，極易遭受攻擊；僅 5%的企業具備標準作業流程與企業規章，符合如 ISO 27001 國際資安標準，但仍難擋進階持續性滲透駭客攻擊(APT)。

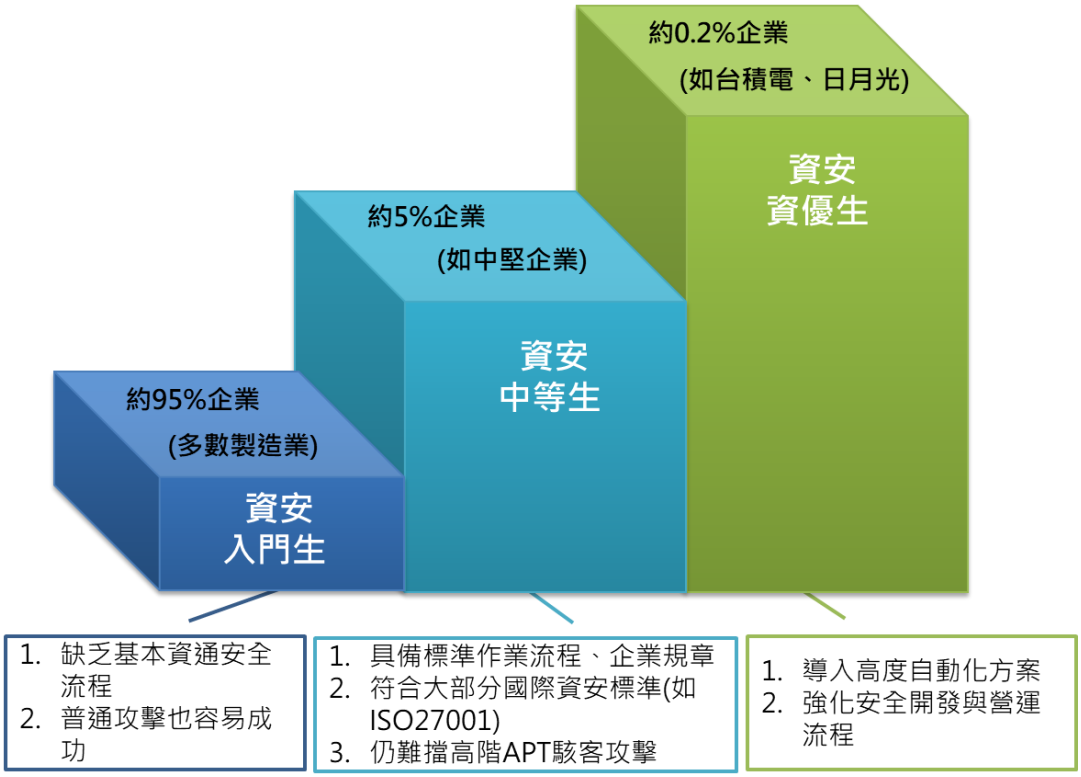


圖 1、企業資安發展程度

聚焦在台灣製造業推動資通安全相關業務的阻力與困難，統計國

內 200 人以上的製造業結果，前三大挑戰分別是內部技術能量不足(41.2%)、公司對於資安投資報酬率缺乏了解(40.0%)、內部員工缺乏資安意識(33.8%)等。以本計畫關聯性產業來看，重點高科技產業、機械設備製造業與其他製造產業的分析如下：

■ 重點高科技產業主要阻力與困難

- 內部員工缺乏資安意識 (38.2%)
- 公司對於資安投資報酬率缺乏了解 (37.6%)
- 內部技術能量不足 (37.0%)

■ 機械設備製造業主要阻力與困難

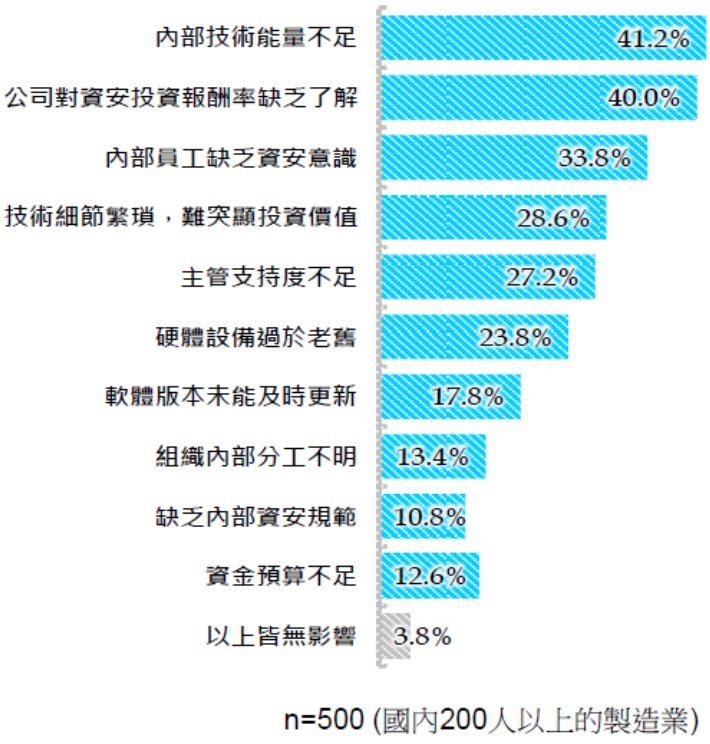
- 內部技術能量不足 (43.4%)
- 公司對於資安投資報酬率缺乏了解 (42.2%)
- 內部員工缺乏資安意識 (33.7%)

■ 其他製造產業主要阻力與困難

- 內部技術能量不足 (43.5%)
- 公司對於資安投資報酬率缺乏了解 (40.4%)
- 技術細節繁瑣，難以突顯投資價值(29.8%)

以往製造業重視生產線產能，設備/產線人員數較高，相關資訊/資管人員數則很少，甚至身兼資安人員職責，在人力與能力都缺乏之下更不會有專責的資安團隊來維運公司資安治理，且企業對於資安佈

署高達八成以上僅以防火牆、端點安全防護為主，約六成有加以佈署安全郵件閘道，多數企業其他資安產品幾乎不考慮，資安防禦能量當然不足；另外資安投資的回報往往無法量化，公司老闆經常性詢問提案採購的資安設備或解決方案可以增加多少資安防護力，IT 部門乃至配合的資安設備供應商幾乎都無法提出讓公司老闆滿意的答案，對資安投資報酬率的缺乏了解，造成每年資安預算編列皆會被砍。



資料來源：工研院產科國際所

圖 2、製造業資安阻力與困難

但隨著產業數位轉型，勒索軟體攻擊、惡意軟體滲透、釣魚攻擊等資安攻擊問題日益嚴重，2017 年，美默克藥廠遭勒索軟體攻擊，損失 87.9 億元；同年 6 月，日本田汽車同樣遭受勒索軟體入侵，延遲千輛汽車出貨；2018 年，美波音公司電腦遭攻擊，產線暫停生產；同年

8 月，全球最大晶圓代工廠－台積電半導體機台為病毒感染，全台工廠停機三日；同年 11 月，合晶上海 EPI 磊晶矽晶圓廠，亦遭病毒攻擊，產線停擺；2019 在卡巴斯基發現有駭客透過華碩的更新伺服器，為華碩電腦安裝後門，造成眾多華碩電腦受害；2020 與 2021 年勒索軟體攻擊肆虐，國內關鍵基礎設施與製造產業等陸續遭受攻擊事件，因為 IT 無法運作造成營運停擺。有鑑於資安事件層出不窮，身為高科技研發製造重鎮且為各國際大廠供應商的臺灣，各大企業夥伴不得不重視導入資安防禦的重要性。

無論企業是因為內部資安技術能量不足、內部資安意識不高或不知道該如何落實資安、及缺乏對於資安投資報酬成效的了解導致公司老闆不願投入更多資安預算，製造業的資安成熟概況普遍落後於其他產業(如：金融業)，可將產業資安問題與需求盤點分析為下列三類：

(一) 跨廠區管理需求

高科技製造業(如：半導體晶圓製造、高科技面板廠)相較於多數製造業實屬資安優等生，對於資安能量的防禦部署投入更多及更完善，每年千萬元等級以上的資安預算規劃，然而防護面向太大沒有百分之百的絕對安全，仍然會有被攻擊的可能性。這類產業的共通樣態是製造工廠遍及北中南各廠區甚至跨國廠區，設備多且產線複雜、自動化

程度高且設備連網，由於製造工廠建造與營運多年、廠區新舊產線混用，需要防護管理的設備機台數量繁多，眾多設備資訊量僅靠人力監管、應變、分析而沒有足夠自動化工具/機制輔助，一旦發生資安事件，從問題被偵查發現，到根因識別排除，到應變處置恢復，恐需要花費相當可觀的時間造成公司營運影響層面極廣。故面對跨廠區管理需求的企業，高度資產可視化、網路資訊行為可視化等是協助資安人員/高階長官快速發現、掌控、應變、排除事件的不二法門。

(二) 設備連網遠端連線需求

臺灣身為 ODM/OEM 代工大國、國際大產供應鏈重要角色，為持續爭取大廠客戶訂單，製造業迎向數位轉型設備機台連上網路是勢在必行，但面對產業轉型資安腳步卻跟不上，資安防護不知道該如何下手，對員工的資安教育訓練與資安人員的投資，或是對資安事件的應變處置計畫也都欠缺。2018 年台積電產線資安事件因為人員疏失未遵守標準 SOP 進行新機上線前隔離掃毒，造成產線停擺損失高達 50 多億元，即便是高科技大廠也有因人員資安意識不足而引起的資安風險；就算是工廠實體隔離，利用 USB 進行 IT 與 OT 間的資訊交換仍是常態，廠內受感染的行動可攜式裝置依然潛藏資安危機。臺廠在國際市場趨勢下逐漸接受到大廠客戶稽核管理要求，為了生產營運的品質管理，需開啟遠端連線讓客戶可即時審視產能品質狀況，且因

為疫情影響及未來趨勢所趨，開始需要開啟遠端連線讓供應商調校機台參數或維護，甚至公司員工/主管需遠端登入系統進行操控，此時智慧工廠門戶大開不再只是過往實體隔離就可進行全面控管的局面，資安風險會大幅提升。為爭取客戶訂單並建立安心品牌形象，面對資安更需嚴正以待，需由內而外全面檢視網路系統架構與部署資安防護堡壘。

(三) IT/OT 混合環境下 OT 創新解決方案需求

隨著智慧工廠、工業 4.0 概念崛起，自動化設備有了與過去截然不同的改變，過去的自動化設備多為獨立運作，而現今因應智慧化生產管理、設備即時監測等多元需求，各類廠房環境大量進行雲端與實體設備間的虛實整合，產線各環節運作透過連網而互通，工廠內佈建超過 50%具備 IP 功能的設備，帶來極大的便利性，同時卻也帶來更多資安攻擊之突破口。產業端的資訊技術（IT）和營運技術（OT）已逐漸融合，實體隔離早已不敷使用，且 IT 與 OT 混合讓資安管理更不易，面對工控領域的特殊需求使用公開或私有通訊協定，使得工廠潛在風險大增，但現有 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的資安問題。

跨廠區管理需求案例解析

群創光電

二、 跨廠區管理需求案例解析

(一) 群創光電

1. 資安導入評估準則

企業數位轉型的發展，讓高科技製造業導入智慧製造，利用先進製造技術和物聯網、大數據、雲計算和人工智慧(AI)，透過數據及科學的方法，除了讓生產管理更精準，更需要最小化資安攻擊可能，以降低損害產生，提升企業績效與競爭優勢。

群創光電為營運多年的科技製造業，在台灣有 14 個廠區，面對老舊工廠，遇到製造業的資安通病 — 機台設備作業系統老舊、無法更新(或更新不容易)造成漏洞不能及時修補，要升級可能遭遇到設備供應商已關廠、或是天價的升級費用，造成工廠數位轉型的資訊網路環境複雜，資安風險提高。

面對資安攻擊肆虐的局面，一般企業高階主管談論起資安一致認知很重要，真正實作資安導入需要經費投入時，資安往往是被優先排除的前幾名；傳統製造業向來重視的是生

產穩定與產能的量化，資安投資的 KPI 不容易和營運效益綁定。

群創光電有鑑於 2018 年台積電事件造成的大規模營運損失，企業敲響警鐘，逐漸意識到工廠資安風險問題；2019、2020 及 2021 年勒索病毒駭進關鍵基礎設施及製造業等資安事件頻傳；群創光電相較於多數製造業，更進一步對於資安能量的防禦加強部署。

群創光電為面板產業龍頭之一，此次資安強化由企業高層主管主導資安升級計畫，MIS 和工廠打造工控環境資安合規標準(IEC 62443)，全面導入台灣 14 大廠區，由管理面、技術面及推廣面縱深防禦強化工廠關鍵機台資安應變與持續營運的能力，相較於多數製造業，對於資安能量的防禦部署已投入更多，每年至少 3,000 萬元的資安投資下限，然而製造工廠遍及北中南各廠區，設備機台數量多產線複雜，眾多設備資訊量僅靠人力監管、應變、分析，防護面向太大沒有百分之百的絕對安全，一旦發生攻擊影響層面極廣。

為了有效溝通企業內部與各廠區應具備資安防禦，需轉換對上企業主管、對下內部員工的溝通方式，用簡單清晰的

高度視覺化介面將資安的能見度提高，公司上下溝通順暢，大家都看得懂、聽得懂資安，才會更有感覺哪裡有資安漏洞，哪裡有不足之處可以優化改善。

2. 資安強化作法

首重在公司的資安治理策略制定與推動，包含資安專責組織制度推動、資訊資產盤點管理、風險評估等；以及視覺化資安戰情平台建置，包含機台網路安全區隔與防護、機台資安事件客製化管理、智慧網管系統集中管控等。相關做法論述如下。

- 資安專責組織制度：明文制定公司的資訊安全政策並公佈，並設置專責的資訊安全組織與人員分工，指派專責的資訊安全長而非僅是兼任，並針對公司 IT/OT 資訊安全事件制定通報機制與應變處置流程辦法。

- 資產盤點管理:於計畫內針對老舊關鍵機台進行資安風險盤點，以分級分類資產設備進行資安指標設立與精進資安防護力道。針對高風險會影響到正常營運的關鍵機台設備，需評估整體軟硬體升級汰換，若無法升級汰換則評估增設在機台前加掛「次世代防火牆」，阻絕已知的漏洞攻擊和

及時的病毒防護，讓可能的攻擊行為無法於工廠生產網路擴散出去。

- 風險評估：採用經濟部工業局所推動的企業資安評級工具進行資安成熟度自我評估，了解公司資安缺口並可參考建議改善措施擬定資安升級步驟，完成資安控制措施，如對已知攻擊的防護、對病毒入侵的防護、部署防火牆實施關鍵機台網路區隔及安全防護。

- 關鍵機台資安戰情平台：收集各 FAB 情資往 Datacenter 端送，包含防毒 log、IPS log、防火牆 log、AD log 等，分析正規化 log 作為資安攻擊事件判別基準，並建置集中處理的智慧網路與效能監控系統，包含有線和無線用戶紀錄、連線軌跡，整體結合資訊安全團隊、資產盤點、資安事件分析統計與管理流程、即時告警機制，打造可視化資安事件分析查詢戰情儀表板。該資安戰情平台統計的資安威脅事件分別為 IPS/IDS 入侵偵測防禦事件、Malware 病毒與惡意程式事件、黑名單事件，依照事件危害等級分為嚴重風險(Critical)、高風險(High)、中風險(Medium)、低風險(Low)四級。

- 而整合在戰情室的資訊資產系統，自動掌握資訊資產最新資訊、完整性及異常變更狀態，收集伺服器、儲存設備、個人電腦、不斷電系統、網路、通訊、監視系統等類別資產，確實了解整體數量及機齡狀況，提早預先安排規劃，減少老舊系統所帶來的資安風險。

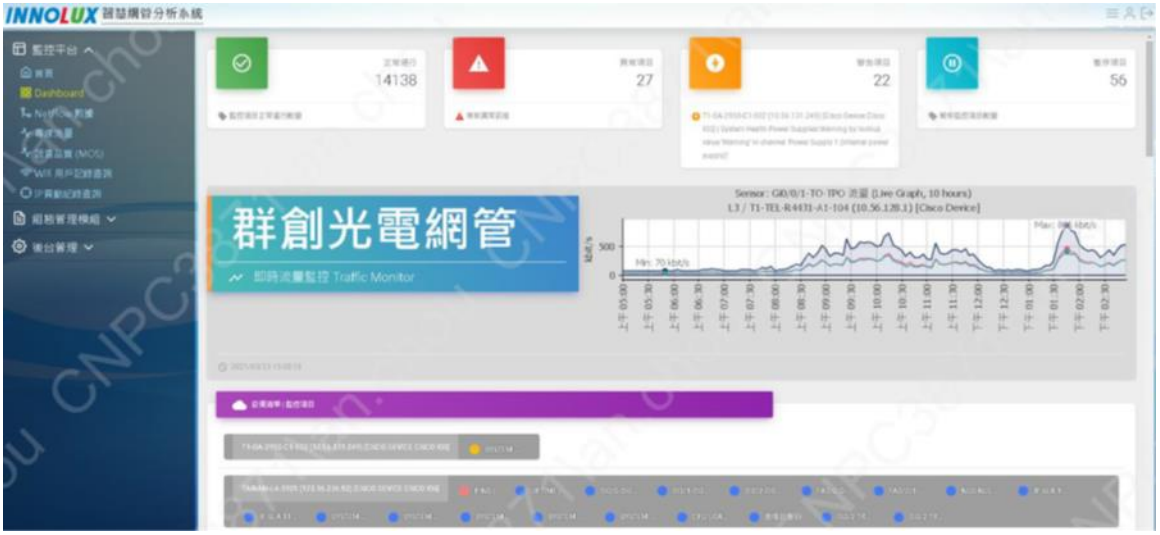
- 智慧網管分析系統是持續監控各個廠區的 IT 基礎設施，包含網路設備、伺服器、防火牆等設備，一旦有設備發生硬體故障或是效能障礙，會立即產生告警並通報管理員，確保各廠區運作順暢。

資料來源：群創光電

圖 3、資安戰情儀表板

資料來源：群創光電

圖 4、資訊資產系統



資料來源：群創光電

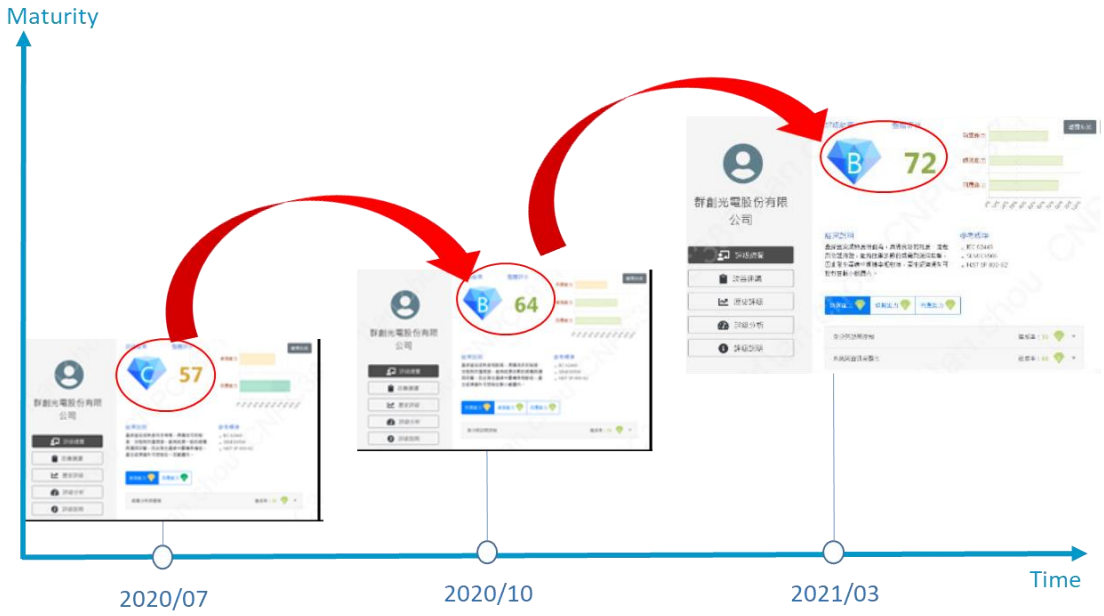
圖 5、智慧網管系統

3. 成果效益

為了能主動有效快速回應資安事件，建置了整套資安戰情系統，收集所有資訊安全相關資料（IPS、次世代防火牆、DDoS 及防毒等相關），利用生產製造中心統計資安事件，快速偵測、抵禦及修補漏洞，主動找出可疑資安事件，0.5 小時內要識別判斷並將受感染機台隔離封鎖，為確保工廠營運順暢，未來也將從老舊高風險關鍵機台擴大到監管工廠機台導入主動資安防護。

群創光電透過資安戰情室三大系統相互輔助提升資安應變能力，7*24 運用 AI 大數據分析，主動找出可疑資安事件，減輕大量人員日常的分析工作及降低人為 MO(Miss Operation)機率，透過跨廠區資安控管與可視化資安平台，讓主管與工程師都能清楚看懂資安問題破口與不足之處，也藉由各廠區 IT 與 OT 資訊彙整呈現，形成各廠間的良性競爭，高層主管自主意識到並比較各廠資安防護能力，主動提高投入資安之意願與預算，並要求跨部門合作資安強化，達到資安有效溝通。該計畫透過資安評級工具進行內部風險評估，執行期間資安成熟度從 C 等級提升至 B 等級，參考了評級結果建議從識別、防護、偵測、回應及復原五大能力中表現較

弱的識別、防護及偵測等能力優先採取強化策略，包含進行資產盤點管理、風險評估管理、獨立資安長與成立資安團隊、完善資安事故應變處理流程及打造資安戰情室主動偵防資安事件等，後續仍會每年至少投資 3,000 萬預算來自主強化資安方案，針對資安評估缺口持續精進資安防護面向，預計資安成熟度 2022 年可達 A 等級。



資料來源：群創光電

圖 6、企業資安成熟度持續升級

設備連網遠端連線需求

案例解析

新揚科技
銘異科技

三、 設備連網遠端連線需求案例解析

(一) 新揚科技

1. 資安導入評估準則

新揚科技是臺灣唯一能獨立研發和掌控製程參數的專業FPC 材料領導企業，從 2017 年開始轉型智慧工廠，從設備連線、數據收集，到生產可視化、整廠資訊整合，串聯廠區各項生產資訊並建立可視化管理平台。新揚致力發展導入低介電無膠銅箔基板，低介電覆蓋膜，低介電純膠等相關之低介電材料，提供客戶在高頻/高速 5G 傳輸應用之最佳解決方案獲美國兩收機大廠將其納入設計採用量產重要的材料供應製造商，5G 高端產品的供應鏈已完成布局。然面對國際大廠客戶的機敏資料保護，客戶對供應商的資訊安全能力有一定程度要求，為爭取大廠訂單，供應鏈的資安防禦能力需提前部署。

智慧工廠聯網的確帶來許多效益如精確資產管理、提升機台稼動率、快速的趨勢分析、有效庫存管理、主動式資料擷取傳輸與存取、透明的行銷策略等，過往新揚科技為了讓產線主管可即時掌握生產狀況監控，或為了讓設備廠商能更新軟體程式與故障排除，進階的為了讓大廠客戶可隨時查看

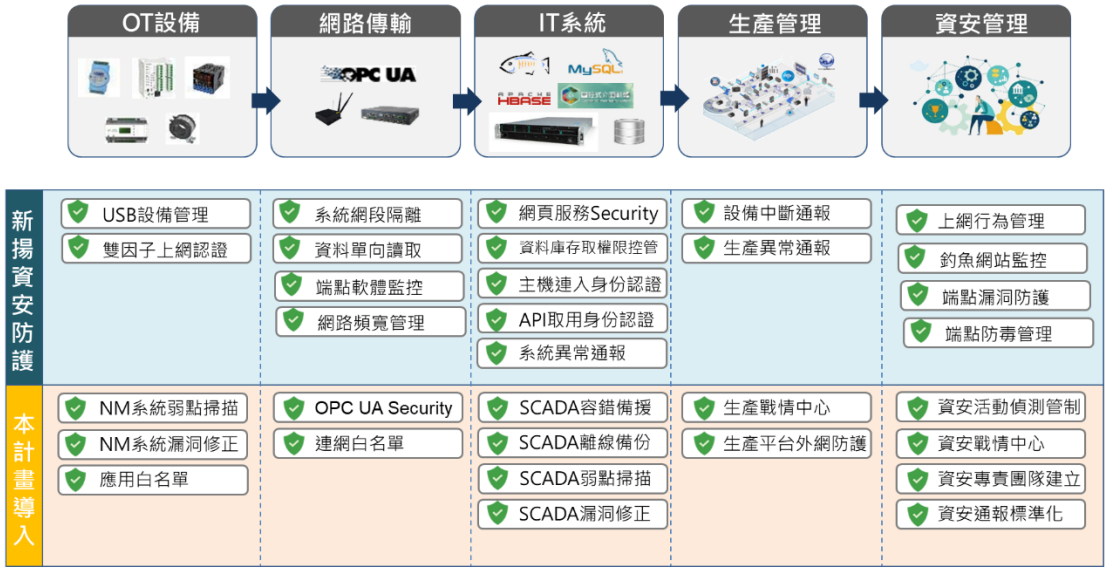
生產進度與良率表現，開啟了外部遠端連線的需求，但隨著廠內設備資訊皆可經由網路上傳、資料皆透過網路蒐集整合於雲端伺服器內使用，大量資料在智慧工廠與網際網路間進出，資安風險的議題便浮上檯面，而邁向數位轉型之路，資安意識與資安防護能量相對較薄弱的製造產業，需更加正視 IT 與 OT 的資訊安全保護避免受駭客/病毒的攻擊，以滿足客戶端與供應端對資訊交換與資訊安全的要求。

故新揚科技依據製程重要性及成本效益，制定風險管理策略，規劃從產線設備面、SCADA 系統面、資料傳輸管理面進行安全補強，打造 PCB 軟板產線成為具資安防護的智慧製造系統，以持續獲得大廠客戶信賴，取得訂單。

2. 資安強化作法

新揚科技在 IT 系統防護層面已有較多著墨，對於網站、主機系統有採取一些身分管控的機制，IT 設備的防毒與漏洞管理亦有實施，對於員工上網行為或社交工程攻擊、釣魚網站監控也都有管理。然 OT 與 IT 之間的資訊無法相互回饋或整合，亦無網路隔離或資安防護策略，容易造成 OT 資訊分散沒有妥善分析利用，IT 系統資安防護又各自獨立，當發生

資安事件時相當容易橫向擴散，異常事件的處理與排除僅靠現場人員回報，缺乏資安專業能力下無法及時應變處置。故需要打造資安防護的 IT 與 OT 整合平台，從產線設備端點防護、OT 資料安全擷取與傳輸、系統容錯穩定運行、異常偵測與追蹤等面向確保整廠資訊安全防護。



資料來源：新揚科技

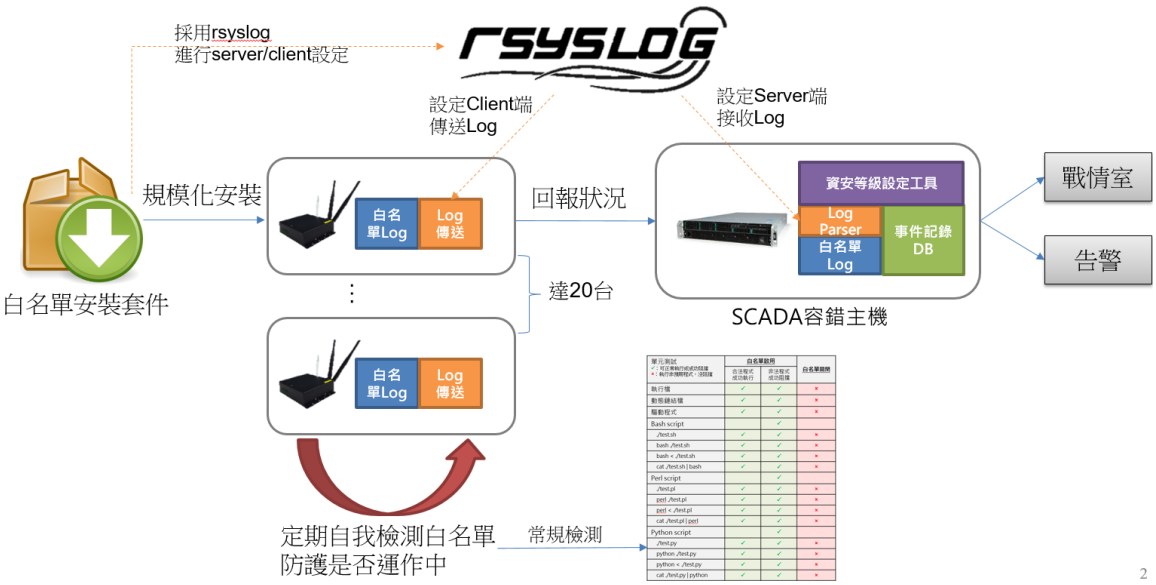
圖 7、資安防護佈署導入

■ 產線設備端點防護系統

利用工具針對工控設備與系統服務定期進行漏洞挖掘檢測，透過資安實測推動我國產業落實安全開發流程的觀念進入產品管理流程，透過資安檢測服務提供檢測報告、風險評估、提供修補建議等資訊，並佐以檢測人員進行弱點確認以及進行深度探索未知弱點是否存在，透過此方式維持檢測品

質並避免傳統需要大量人物力之檢測方式，進而確保智慧工廠內工控設備以及系統服務之安全防禦能力。

進一步佈署應用程式白名單機制，以正面表列方式確保所有可被執行之程式皆為名單內之程式內容，同時整合檔案完整性檢測避免惡意攻擊者任意仿冒特定執行檔執行，主動防護端點設備，並整合相關資訊匯集至資安戰情模組以進行異常監控與及時告警。



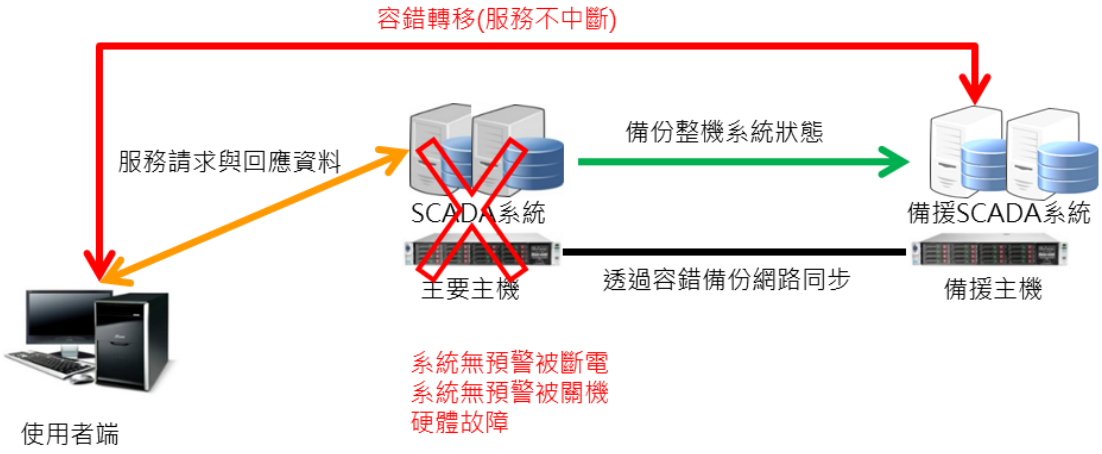
資料來源：新揚科技

圖 8、端點白名單防護

■ 系統容錯備援

為確保營運不中斷，廠內 SCADA 系統導入容錯備援機制，主要主機與備援主機間有容錯備份網路相連，當容錯服務啟動時，主要主機上的容錯程式將會持續地收集 SCADA

系統狀態並備份至備援主機，防止生產監測系統在受到攻擊時服務中斷而遺失重要的生產資料造成產線停擺；同時系統導入離線備份機制，防止因災難或受到勒索病毒攻擊時，重要生產資料與系統無法復原。



資料來源：新揚科技

圖 9、容錯機制提供不中斷服務

■ 資料安全傳輸

廠內已建置工業 4.0 標準通訊協定，而針對資料安全加密部份，則仍需補足符合工業 4.0 標準規範。故建置 OPC UA Security 安全傳輸機制，進行全廠生產資料安全傳輸，保證生產資料無法被非法取得而外流。OPC UA 安全性概念包括三個級別：使用者安全性、應用程式安全性和傳輸安全性。使用者安全性的機制在設置建立連線時會為使用者授予訪問權限及角色；用程式級安全性也是通信會話的一部分，包括交

換 X.509 憑證，在安全通道建立期間交換的應用程式實例證書用於驗證應用程式，可由 OPC Foundation 認證的受支持的 UA 安全配置文件定義 UA 應用程式支持的安全機制；傳輸級安全性則可用於在通信會話期間對每條消息進行簽名和加密，簽名可確保消息完整性並加密防止竊聽。

■ 資安戰情管理

透過戰情中心建置整合工廠生產資訊與資訊安全資訊，以異常事件判別設定模組、資安活動紀錄分析模組、資安異常事件通知模組、資安事件紀錄模組完備工廠資訊監控功能。新揚於場域內的工控設備建立應用程式白名單，經過設定將 log 同步至 SCADA 容錯主機上，在 SCADA 主機上預先建立異常事件判別設定功能，經過資安活動記錄分析模組後，進行資安異常事件通知，發送資安威脅 Email，最後將資安事件儲存在資料庫中。

資料來源：新揚科技

圖 10、資安戰情管理

資料來源：新揚科技

圖 11、資安事件偵測與通報機制

3. 成果效益

新揚科技透過該計畫全面盤點智慧工廠，從設備端、系統端以及資料傳輸端部署資安策略，成為國內 FCCL 軟板產線中，具資安防護的智慧製造系統的示範廠，在推動機聯網平台升級之際，將生產資訊與資安串聯，實現廠區 IT 與 OT 高度整合之智慧工廠資訊安全系統，由內而外強化自身資安等級由 E 等級晉升到 B 等級，從表現較弱的識別能力、防禦能力、偵測能力、回應能力著手部署規劃，包含盤點資產弱點、成立專責資安團隊、制定資安治理政策、建立資安事件通報與應變機制、主動式白名單防護、產線 Log 資訊收集分析等，並進階加強 SCADA 系統容錯備援機制，保護生產資訊不毀損、營運不中斷。藉由資安升級步驟的落實，新揚科技可具備較完整的資訊安全防護，避免生產資訊外流與阻隔駭客與病毒攻擊造成的停線危機，也因此可提供國際大廠完

善的機敏資料保護能力，取得國際信賴成功布局國際大廠策略性的材料合作夥伴。

資料來源：新揚科技

圖 12、資安成熟度提升

(二) 銘異科技

1. 資安導入評估準則

銘異科技為全球第一硬碟機零組件OEM/ODM代工供應商，考量全球供貨樣態逐漸轉向少量多樣、品質要求一致，自 2006 年成立自動化事業群開始發展自動化機台設備，起初以解決企業內部生產需求為主，然自動化技術越趨穩定，2011年開始拓展版圖幫助客戶打造自動化設備。在萬物聯網、大數據與 AI 等技術的潮流下，過去封閉式的生產機台隨著智慧工廠的推波助瀾，設備開始串連至網路平台，萬物聯網已經成為無可避免的趨勢，但也意味著資料進出流竄的複雜性和潛在的高風險。

銘異科技在協助客戶導入整線自動化與佈建連網設備時，深感 OT 端的資安防護重視程度遠不及 IT 端，這將會是企業的隱憂，成為駭客攻擊的目標。IT 端的資訊安全防護可隨著軟體的更新即時升級，相較於 OT 設備，為維持產能無法隨時停機做系統更新修補資安漏洞，且產線設備老舊也難以佈署資安防護方案，OT 端人員亦缺乏資安防護意識與經驗，使得駭客更易瞄準其為攻擊對象。另外智慧工廠中有些自動化

設備來自國外(如：日本)設備供應商，為保護自身智財不會將設備內部連網架構、設備組態設定等資訊公開給客戶甚至全部加密，機台設備的後續維護，是需開啟網路連線讓設備供應商遠端進入機台操作或更新軟體，供應商亦不允許客戶任意安裝資安防護軟體否則拒絕保固，這些議題都凸顯了 OT 設備連網會引來資安威脅。

面對駭客日新月異的入侵手法，製造業需超前佈署資安防護避免企業遭受資安攻擊所造成的營運重大損失，故銘異科技自 2019 年開始找尋並規劃合適的資安解決方案，最終決定由企業內部開始全面進行資安健檢與資訊資產盤點，並收集 OT 機台設備資訊進行分析監控，以進行早期預警、持續監控、通報應變與協處的風險管理策略。將從自身智慧工廠做起，建立 OT 雲端資安戰情中心，主動資安情資收集比對與自動通報應變，建立完整智慧製造資安解決方案；後續會構築 OT 資安聯防體系，串聯自動化設備客戶一起加入，透過資安情資分享以及資安通報，協助客戶即時獲得第一手消息進行 OT 資安升級防護，以供應鏈資安聯防體系整體強化智慧製造資安，讓製造業在整線自動化與智慧製造相關設施導入工廠時資安防護不再是單打獨鬥。

2. 資安強化作法

銘異科技欲以推動產線自動化整合資安解決方案的完整智慧製造資安解決方案為目標，故結合自動化事業部門與資訊部門共同成立資安專責團隊推動此計畫，藉由建立雲端資安戰情中心,鏈結自身與客戶共同進行資安監控與資安通報,打造 OT 資安聯防體系。由於缺乏 IT 與 OT 整合的資安防禦方法，無法主動偵測與即時告警關鍵設備遭受攻擊的情況，導致無法提供包含資安監控的整線自動化完整方案，加上缺乏專業能力與人力來進行 OT 監控與應變，事件發生單靠人工通報亦無法有效通報，故在資安強化做法規劃從全面資安健檢與資產盤點來檢視智慧工廠現況，再藉由收集場域設備機台的封包資訊建置資安監控中心，同時建立 OT 資安監控規則以利導入 AI 分析技術進行識別，後設立誘捕系統，吸引駭客視其為弱點破口進行攻擊，收集攻擊手法與途徑，最後為驗證資安防護方法是否有效可引進第三方攻防測試驗證。

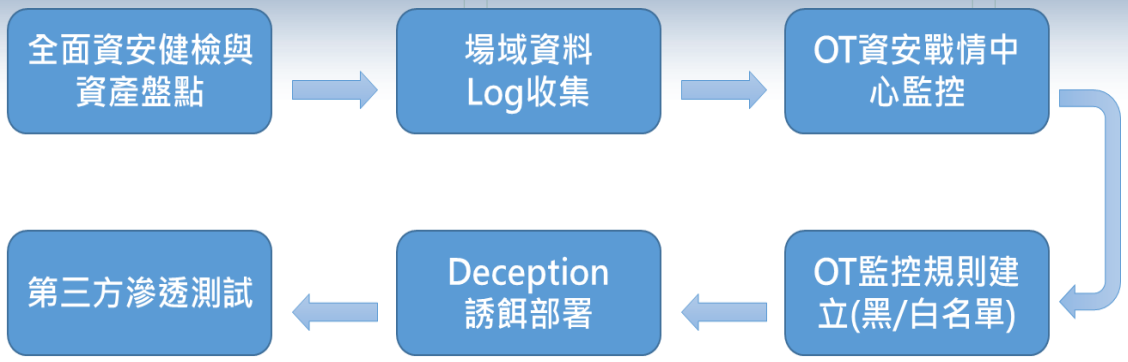


圖 13、資安導入建議做法

於全面資安健檢檢視網路拓樸架構與重要主機系統擺放位置，發現 IT 與 OT 並無隔離機制，當 IT 設備被駭客入侵時，OT 環境缺乏邊界防護也無 OT 設備自主的防禦機制，容易成為下一階段被攻擊目標，故可透過資產盤點與風險評鑑後的等級(低、中、高)進行網段切割與區域邊界防護，以強化 OT 端保護。

而過去面對 IT 威脅偵測無法與即時情資比對，威脅告警不即時、威脅回應不即時，無持續性的資料 log 收集與關聯規則分析與更新，相關人員需手動增加關聯規則才能確保情資比對，且須人工操作在各系統的 raw data 中分析找出威脅的蛛絲馬跡，再著手調整資安管理策略，這些非自動化方式使得符合重大情資的網路封包無法被主動阻斷，使得弱點電腦成為被入侵的門戶。故亟需收集產線機台的封包資料，引進國內外資安情資建構開放式資安戰情大數據中心，比對收

集的資料封包與戰情大數據，以關聯規則分析可能的威脅異常並告警。

當資安事件發生時，過去皆靠人員由各項軟硬體設備所紀錄之訊息手動進行資安事件資料彙整，且可能只能發現該終端設備的資安問題，無法回朔資安事件根因，造成無法徹底解決資安問題，另資安事件的處理亦沒有事件管理與流程追蹤機制，事件的處理可能因為逾期而未發現，也缺乏事件處理後的紀錄，無法成為企業內部資安知識的累積資產。故除了需自動進行告警分析，也需建立資安事件單進行處理人員及優先處理順序指派，並有完整的威脅調查報評估確認影響範圍、影響電腦設備，及建立事件處理與流程追蹤，結案後可形成企業資安知識資產。

銘異科技於產線自動化整合資安解決方案的示範執行首重雲端 OT 安全監控防護平台的建立以及智慧資安主動防護與自動化通報系統建置。

■ 雲端 OT 安全監控防護平台

情資數據庫建置，可將 OTX 情資匯入資安戰情大數據，當收集公司內部資安設備的網路封包與日誌，將其與資安威

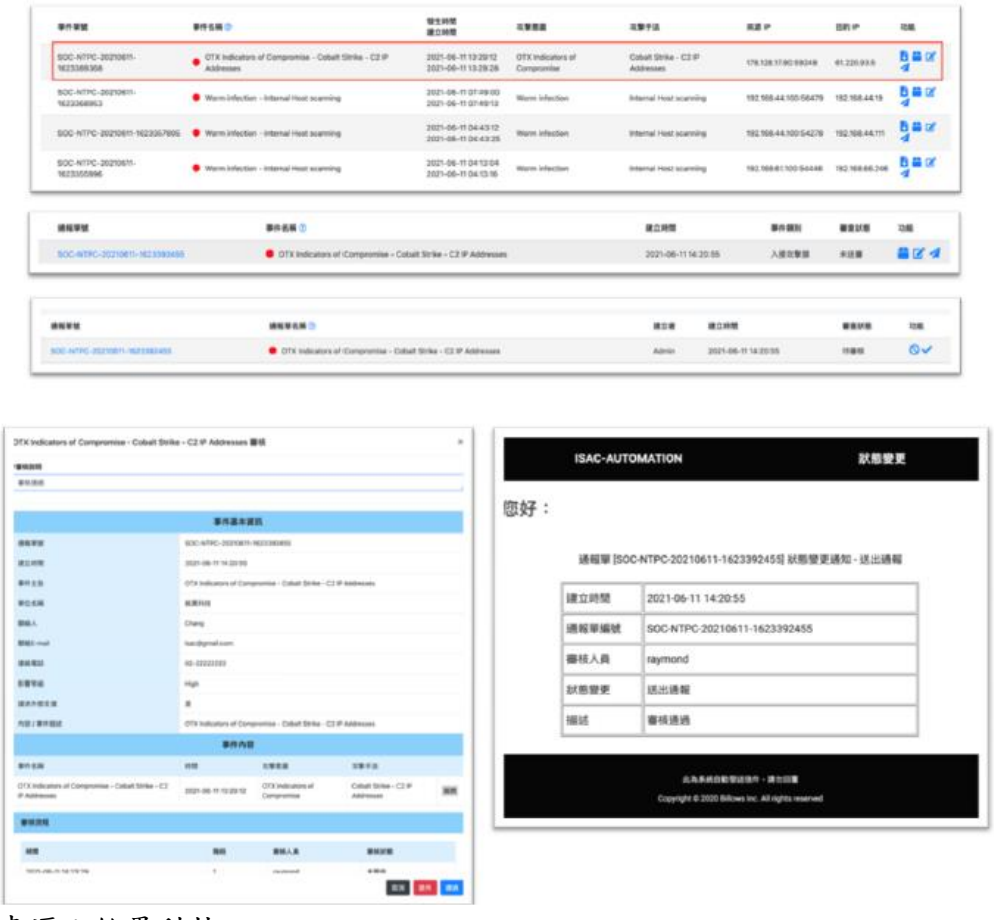
脅情資互相比對，若比對符合時，則進行後續告警通知或者透過命令發送，提供設備進行主動式阻斷；開發戰情中心儀表板串接資料收集器與關聯分析模組，每小時自動更新一次資安監控中心之情資比對資料庫，當判斷有資安事件發生時，則透過資安通報 Web Service 進行資安通報平台的資料串接，以視覺化的方式，提供資安人員得以有效的運用資安戰情資訊，做出資安防護的最有效決策。

■ 智慧資安主動防護與自動化通報系統

透過收集、發現、分析、通報及應變等一系列循環的動作來執行自動化資安情資通報，整合防火牆設備將收集到的黑名單情資資訊透過 API 更新防火牆設備中的 blocklist，再導入誘捕系統模擬設備行為，吸引駭客攻擊，再將駭客攻擊行為進行分析，進而達到威脅回應防禦與攻擊阻斷的目的。

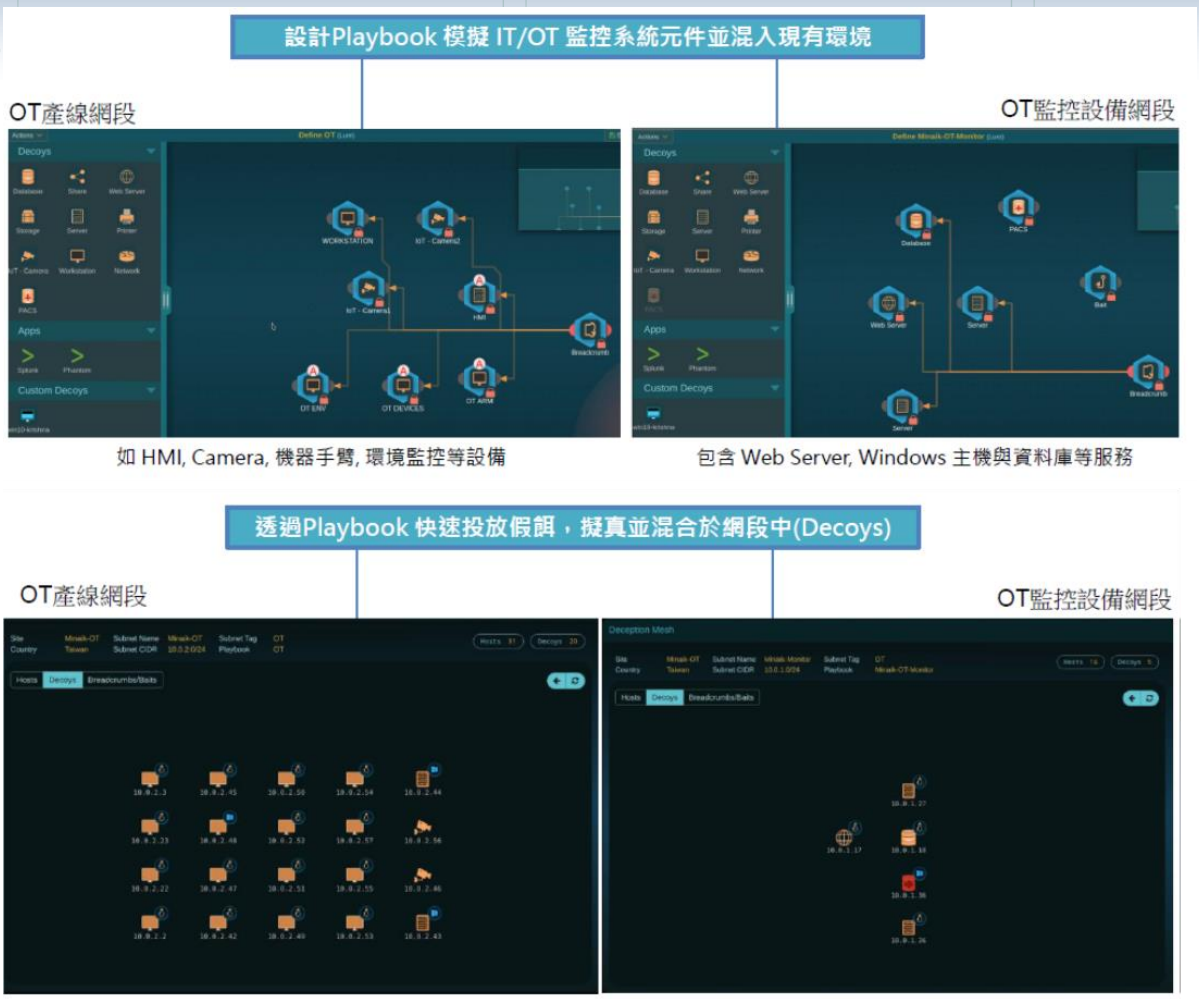
資料來源：銘異科技

圖 14、OT 資安戰情中心



資料來源：銘異科技

圖 15、自動化資安通報系統



資料來源：銘異科技

圖 16、OT 場域佈署 20 個誘捕設備

3. 成果效益

面對日益複雜的攻擊手法及威脅態勢，企業對待網路安全的態度也開始有重大轉變，因為網路資安和威脅正在迅速成為許多組織的最大商業風險，因此目前許多企業已開始透過與資安服務提供商合作，以提高威脅、漏洞的處理能力。銘異科技透過此計畫導入資安強化方案執行，資安成熟度從 D 等級提升至 B 等級，將識別、防護、偵測、回應、恢復五

大能力中表現較弱的識別能力、防護能力、偵測能力與回應能力視為重點改善項目，於計畫執行期間從資產盤點、風險評估管理、情資分析運用、戰情中心建立、自動通報應變系統建立等著手，整體部署資安防護面向，從原本協助製造業客製化整線自動化設備規劃的廠商，成功轉型成為提供客戶整線自動化設備規劃建置加上資安監控服務整合解決方案之供應商。該全方位的自動化設備資安解決方案可協助客戶在面對數位轉型之際所遭遇的資安威脅壓力與人力或專業能力不足以應對，有了解決的方法，並可藉由製造業生態圈資安情資聯防體系，共同抵禦無所不在的資安攻擊。

資料來源：銘異科技

圖 17、企業資安評級結果

IT/OT混合環境下OT創新解決方案需求案例解析

新　　漢
泓格科技

四、 IT/OT 混合環境下 OT 創新解決方案需求案例解析

(一) 新漢

1. 資安導入評估準則

新漢是工業 4.0 解決方案的領導廠商，致力於協助企業做數位轉型，從設備自動化到整廠產線自動化，提供工業 4.0 一站式服務。深耕工業電腦和製造產業近 30 年，發現到台灣有相當完整的智慧製造產業鏈，這含括客戶端需求面與供應面，面對市場趨勢逐漸朝產品特性少量多樣、設備連網 IoT 智能化，新漢深刻瞭解到工業物聯網安全屬性不同於 IT 環境的資安可隨時軟體更新升級，智慧製造場域面對的是產線設備老舊、作業系統無法更新、設備品牌眾多、通訊協議各異、產線不能中斷營運等問題，面對日益升高的網路攻擊和潛在威脅，安全性不足的工業設備和網路環境可能遭駭客攻擊而造成營運停擺，或者遭入侵竊取企業或客戶的敏感資料。

而資安事件頻傳造成營運停擺，故現今客戶對於智慧製造產線資安的要求也越趨嚴苛；以新漢為例統計，若產線停擺，平均一天就是二千萬元以上產能的損失，在這 IT 與 OT 逐漸融合的智慧工廠，原有的 IT 資安解決方案並不適用於

OT 環境，需以建立符合 OT 需求的資安防護方案為重點目標。新漢現有的 iAT2000 雲智化監控戰情系統是打造工業 4.0 的整廠解決方案，透過智慧閘道器可收集各品牌控制器資料納入 iAT 2000 系統的監控，面對工控資安的威脅，新漢積極尋求在不影響產線營運的需求下發展產線資安強化方案，並能整合資安監控資訊至 iAT 2000 系統。基於此智慧製造場域的資安需求，新漢於 2017 年成立椰棗科技新創子公司，專為客戶導入工業 4.0 而投入的資安新事業，結合新漢在工業電腦以及工業 4.0 整體解決方案的雄厚基礎上，成功推出 eSAF 資安平台。

2. 資安強化作法

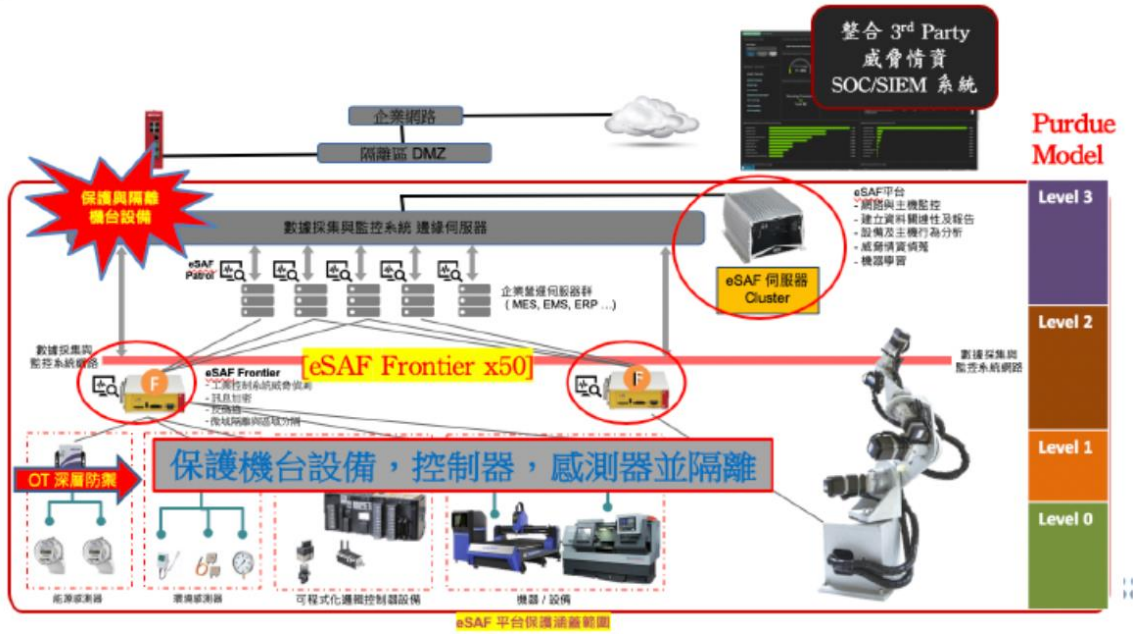
深知 IT 與 OT 網路混合後，產線系統存在許多過時的作業系統與硬體，底層的控制器、感測器、連網設備機台皆無自我保護能力，也缺乏對於整廠 OT 場域資安監測整合的機制，故規劃針對原本資安防護能力不足的機連網工廠環境強化產線資安，並加強重要產線系統韌性，也整合既有的工控防火牆與工廠相關的資安設備監控機制，透過資安戰情室完整呈現工廠 IT 與 OT 的資安防護。下面針對產線資安強化與資安監測戰情系統說明。

■ 產線資安強化

先針對場域內工控機台設備(包括:產線系統、機台設備、IoTGW、感測器、作動器、智慧電表等)完整盤點並進行網路架構調整，針對老舊產線資訊系統越需加強防護避免系統停擺，然後於產線內進行資安設備部署。新漢佈署了 50 台 eSAF OT 資安防護設備橫跨林口華亞廠與板橋三民廠，進行跨廠區即時監控、分析與保護每部機台的資安狀況，並將產線設備進行微隔離以精準偵測與保護，避免廠區內的連網設備橫向感染攻擊。另為了保護重要產線系統，考量老舊設備是製造業常態，將透過重新調整架構把重要系統導入虛擬化 VMWare HA 做到容錯與高可用度資安保護。除了於每台設備機台前部署 eSAF Frontier 收集監控資料，亦建置 2 台 eSAF Platform Manager 以 HA 備援，將收集到的資料可儲存超過 1 年以上。

資料來源：新漢

圖 18、產線資安硬體防護架構



資料來源：新漢

圖 19、產線導入 OT 資安設備收集機台資料

■ 資安監測戰情系統

部署於產線的 OT 資安設備會將機台事件收集並上傳完整設備日誌到資安監控系統，比對威脅情資資料庫(收錄超過 60 種以上威脅情資來源)，以威脅情資和資安事件分析系統持續性監控和分析，以自動分析有效降低過往人力操作負擔、降低人工誤判、加快資安事件處理應變。該資安監測整合了相關產線資安設備的日誌與分析，包括 IT 和 OT 垂直整合防護，內容包含網路完整性的查核、資安事件的管理、資安監督，並可以偵測可程式化邏輯控制器(PLC)的命令，以及與其他資安系統整合，包含日誌檔伺服器、AD 伺服器、安全性資訊與事件管理(SIEM)等。

資安戰情室整合至新漢 iAT2000 企業戰情系統，以跨場域呈現包含總部、三民廠和華亞廠三地的 IT 和 OT 資安事件，會以紅黃綠燈方式即時呈現主機及環境監控的安全狀態，將安全等級劃分為 1-10 級，1-6 級顯示為安全，以綠色表示，7-8 級為警示，以黃燈表示，9-10 以上為危險，以紅色顯示。以直覺化方式讓管理者一眼看出問題所在，即時反應。

資料來源：新漢

圖 20、跨廠區整合企業資安戰情監控

資料來源：新漢

圖 21、資安戰情室系統(威脅情資分析、設備機台資安狀態)

3. 成果效益

透過示範場域的開發，新漢發展出整廠自動化整合產線資安強化的 OT 專屬解決方案，讓過去沒有資安防護能力的設備機台、感測器、控制器等皆能受到保護，並將整廠 IT 與 OT 的資安事件整合並結合威脅情資分析，打造完整的智慧工廠資安戰情室，以清晰可視的呈現方式讓快速迎來數位轉型設備連網的製造產業，減緩遭遇工控資安威脅與應變處理的壓力。於智慧製造資安導入推行過程中，資安成熟度也從 E 等級躍升至 B 等級，從識別、防護、偵測、回應、恢復能力皆採取了資安升級策略，包含工廠內完整設備盤點、風險評估並加強重要系統的韌性保護、導入 OT 專用資安設備、收集完整設備日誌、情資分析比對、資安戰情室監控、系統備援等，持續會擴大部署 OT 資安設備，將跨廠區產線全面納管。新漢結合 iAT 2000 企業戰情系統與 eSAF 資安平台的解決方案，亦將帶動產業鏈學習複製，協助製造業在整廠數位化、自動化轉型之際亦附加資安防護的能力。

資料來源：新漢

圖 22、企業資安成熟度提升

(二) 泓格科技

1. 資安導入評估準則

泓格科技致力於提供完整的工業自動化解決方案，積極發展可程式自動化控制器、工業通訊產品等，其被廣泛應用在國內外工控與自動化領域中。在本身具備智慧工廠的基礎下，泓格亦有協助客戶進行機聯網環境建置，但考量到現今 IT 與 OT 環境融合下，面對生產場域中高複雜度的軟、硬體資產和網路架構，工廠資訊安全的問題更應重視。智慧工廠資安環境建構與導入會面臨到幾個問題，包括：缺乏同時熟悉 IT 與 OT 的人才，傳統 IT 資安解決方案並不適用於 OT 場域；多半的工控網路設備缺乏認證與加密保護，易受駭客入侵；遇到入侵事件，一般需人工建立機制解析封包，曠日費時，應變處置不即時；另外可能遇到客戶對 OT 資安的要求，需依循國際資安標準來維護產線安全環境。故面對機聯網環境，需要有工廠網路資安強化與防護技術整合的解決方案。

此案規劃對泓格湖口二廠的智慧工廠導入資安強化，該工廠是自動化設備生產醫療用 TPU 材料，是新廠建置並且所有工廠機台設備皆連網，故會從打底補強做起，工廠資訊網

路全面風險評估檢視威脅，根據弱點項目進行改善提升；而針對工控網路的安全，需發展網路威脅自動化偵測系統，以有效阻擋攻擊行為；發展可視化的智慧製造資安整合平台，針對入侵威脅能即時經由系統告警並進行資安通報(可透過手機簡訊、Email、通訊軟體通報)。

2. 資安強化作法

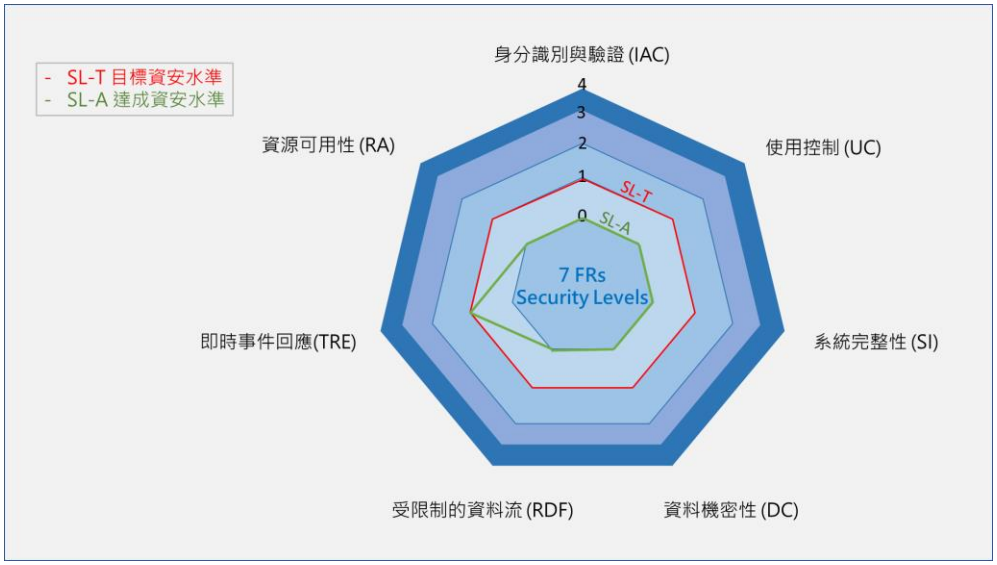
考量工控網路環境的資訊安全問題，泓格科技優先納入智慧工廠資安強化服務導入，包含工廠資訊網路的威脅掃描、根據 IEC 62443-3-3 進行安全強化佈署與導入。納入工控網路安全專用的防護技術或產品開發，包含網路惡意攻擊資料收集與解析技術、工控網路威脅智慧偵測系統、工控網路安全威脅模擬系統。納入智慧製造資安整合平台開發，包含智慧工廠視覺化安全平台開發、資安通報機制。

■ 資安強化服務導入

(1) 工廠資訊網路威脅掃描：透過全面盤點與檢視工廠產線潛藏資安風險，包含網路架構安全弱點檢視、有線/無線網路惡意活動檢視、使用者端與伺服器端電腦惡意程式檢視等

作業，根據盤點結果實施相關改善控制措施，以提升網路與資訊系統安全防禦能力。

(2) 根據 IEC 62443-3-3 進行安全強化佈署與導入：首先完成 IEC 62443-3-3 系統基本資安需求控制項查核，評估產線系統具備的資安水準，並根據資安水準雷達圖顯示的七大項系統基本資安需求差距，持續精進改善控制措施，以協助工廠符合 OT 網路安全國際標準要求、提升工業連網環境之防護能力；另鑒於工控網路設備缺乏加密保護，故開發工控網路通信加密服務器，完成 OPC UA Server 與 Modbus Master 通訊功能，以提升資料傳輸安全性。



資料來源：泓格科技

圖 23、資安水準雷達圖

資料來源：泓格科技

圖 24、通信加密服務器硬體

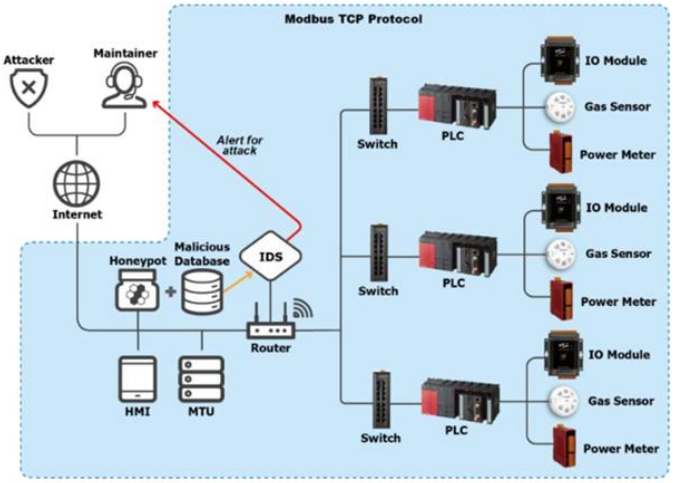
■ 工控網路安全防護技術或產品開發

(1) 網路惡意攻擊資料收集與解析：建立 Modbus 實體密罐與自動擷取網路惡意封包功能，以建置惡意攻擊資料庫。可辨識 6 種惡意攻擊封包：Data Scan、Slave ID Scan、Function Code Scan、The Point Scan、Unauthorized Modification、DoS。藉此收集 AI 入侵偵測系統所需的惡意威脅訓練資料集。

(2) 工控網路威脅智慧偵測系統：建立深度學習 LSTM 分類器模型，採 Bagging 方法從訓練資料集隨機抽取樣本訓練多個 LSTM 模型。該自動入侵偵測系統攻擊偵測正確率

達 90%以上，可協助工廠網路設備安全防護，並達到即時通報與應變之效。

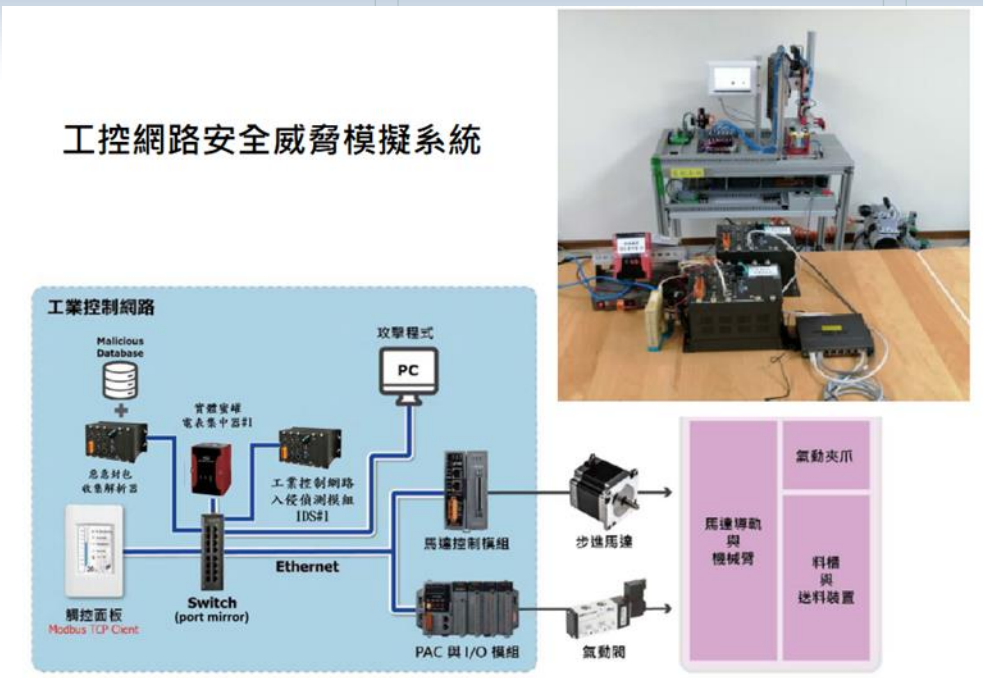
工控網路威脅智慧偵測系統



資料來源：泓格科技

圖 25、IDS 入侵偵測系統

(3) 工控網路安全威脅模擬系統：因考量入侵偵測系統不能直接於產線上驗證，故開發一威脅模擬系統來驗證功能。該工控網路安全威脅模擬系統具備執行料件裝配自動控制程序功能以及 Modbus TCP 網路通訊控制功能，可執行 6 種網路攻擊驗證入侵偵測系統的有效性。



資料來源：泓格科技

圖 26、安全威脅模擬系統

■ 智慧製造資安整合平台開發

(1) 智慧工廠視覺化安全平台：將工廠網路拓樸與設備清單、入侵偵測資安威脅即時警報與歷史警報、主動推播資安危脅警報等功能與視覺呈現整合於智慧工廠整合安全平台，以提供工廠網路安全管理介面，方便管理者快速掌握工控網路資訊。

資料來源：泓格科技

圖 27、智慧工廠資安整合平台

(2) 資安通報機制：建立主動推播資安威脅告警機制，以利管理者可即時接收資安事件通報並快速處理排除。該工控網路安全資安通報功能，具備 3 種告警模式，包含手機簡訊、Email 告警、Line 即時通訊軟體告警，並串聯發生資安事件設備鄰近的攝影機擷取鏡頭畫面，輔以判別資安事件發生的相關影響原因。

資料來源：泓格科技

圖 28、工控網路安全資安通報設備

3. 成果效益

為強化現有智慧製造場域之資安防護能力，泓格科技透過工廠資訊網路威脅掃描與資訊網路安全強化部署與導入，識別現有產線工業控制系統及資安防護設備之潛在弱點與威脅，針對不足之資安控制項進行調整改善；而為強化場域資安能量，也積極進行工控網路安全專用的防護技術開發，該案衍生多項新產品，包含工控網路通信加密服務器、工控網路安全資安通報設備、工控網路威脅智慧偵測系統。藉此強化自我產線資安防護能力外，同時自我期許成為台灣產業資安風氣推手。

資料來源：泓格科技

圖 29、工廠資訊網路安全強化部署成果

於計畫執行期間，資安成熟度表現從 D 等級提升到 B 等級，分別針對識別、防禦、偵測、回應能力予以加強，包含全面工廠資訊網路威脅掃描與資產盤點、遵循 IEC 62443-3-3 資安控制項進行風險評估及建議改善、發展工控網路安全威脅偵測機制、主動推播的資安威脅告警機制等，整體提升泓格智慧工廠的安全性降低停機風險，並打造產線設備資料安全傳輸環境，確保生產品質。此外，公司也成立專責資安管理團隊及對外服務團隊，在資訊安全產品的研發人員質/量能量、建立跨領域產業應用、智慧製造與智慧聯網資安技術上皆有所提升。

五、 結論與建議

物聯網示範案例於計畫執行期間配合施行企業資安評級，結果顯示各示範案例資安升級皆有提升至 B 等級，各案於執行期間亦持續參考評級結果擬定資安升級策略。故建議智慧製造在規劃資安導入之際與評估已投入的資安部署策略/方案有效性，可先進行企業資安成熟度自評，該套工具收錄全球超過 10 套知名國際標準指引(NIST、IEC62443、ISO27001、SEMI、CIS、UK NCSC 等)，超過 300 條結合 IT 與 OT 的資安防護指引，提供國內智慧製造場域主進行風險自我診斷，先了解自身資安現況與弱點項目，並根據評級結果探究企業需求與採納建議改善事項規劃資安持續升級步驟。示範案例的使用回饋摘要如下：

- 企業資安評級系統幫助我們公司快速掌握資安缺口，進行標竿管理。執行計畫過程中省下許多規劃的時間。(新漢)
- 企業資安評級工具提供工廠環境完整資安指引，能夠幫助企業找到過去沒有想到資安部署方向，有利於資安長期升級規劃。(群創)

示範案例的推動也連帶引導企業完善資安管理的制度或策略，衍生許多效益：

- 建立專責的資安團隊與資安主管，培植核心技術人才與自主能量，

提升公司自主資安管理的技術層次。

- 建立完整的資安事件通報與應變管理程序，並定期進行演練作業，達到快速資安事件應變處置能力。
- 建立主動式資安防禦解決方案，打造智慧工廠對內強固資安體質、對外有效偵測與阻擋惡意攻擊。
- 重視員工的資安意識提升與資安教育訓練，針對不同職務需求給予訓練課程安排，提升公司整體資安意識並讓專責同仁更有能力應對各種資訊安全事件。

該智慧製造資安強化教戰手則彙編成功案例的資安導入經驗與做法，目的要藉此協助同領域產業在邁入數位轉型，需積極部署資安防護能量之際，可學習效仿示範案例的思維規劃與執行策略。該手則編製完成，會於 ACW 跨域資安強化產業推動計畫網站(https://www.acw.org.tw/) 線上發佈，讓想了解智慧製造資安強化如何執行的對象查閱參酌；亦可於研討交流活動會輸出成冊，讓廠商進行資安經驗分享之時可同步發送手冊擴散宣傳應用，除了新興物聯網資安示範推動計畫項內的推廣交流活動，亦配合跨域資安強化產業推動計畫與智慧沙崙物聯網資安實驗計畫的推動執行，根據合適分享議題邀請物聯網示範案廠商擔任講師，除了透過資安導入經驗分項並搭配

手冊瀏覽，引導並協助其他同領域業者能學習他人經驗與做法，進一步了解公司真實需求狀況與擬訂資安升級策略及順序，更加妥善編列資安預算投入執行並獲得相對應執行成效，落實帶動整體產業鏈提升資安防衛能力；另可將手則依據產業問題與個別廠商拆分內容，提供給原示範案例廠商，使其可將資安導入成果作為公司宣傳的元素，向其國內外潛在客戶展示臺灣產業在產業資安化具備之技術能量，深化客戶對其信賴與肯定，提升臺灣製造業角逐國際之競爭優勢。