

DECEMBER 2022

12

no.43

AIR

AI
+
IR

智慧自動化產業期刊
Journal of Automation Intelligence and Robotics



智慧製造 X 資安

TAIROA

TAIPEI
Automation
2023

台灣機器人與 智慧自動化展

Taiwan Automation Intelligence and
Robot Show

台北國際 自動化工業大展

Automation Taipei

2023/8/23 (三) - 26 (六)

台北南港展覽館1&2館



立即預登參觀

徵展項目 Exhibit Profile



智慧製造相關 Smart Manufacturing

• 工業自動化設備 • 工業機器人技術 • 智慧工廠(工業自動化軟體應用)



製造設備 Industrial Supply

• 五金工具 • 廠房設備 • 機床暨工具機設備



關鍵零組件 Key Components



AI人工智慧 Artificial Intelligence



智慧服務 Smart Services



服務型機器人 Service Robot

展覽報名 Exhibit Inquiry

攤位有限，立即洽詢

社團法人台灣智慧自動化與機器人協會

陳怡樺#14

TEL: (04)2358-1866

FAX: (04)2358-1566

Email: service@tairoa.org.tw

展昭國際企業股份有限公司 Chan Chao Int'l Co., Ltd.

黃姝嫻#122、方強#153

TEL: +886-2-26596000

FAX: +886-2-26597000

Email: automation@chanchao.com.tw





TAIROA B2B 台灣智動領域 供應商平台

金屬加工 | 電子零組件 | 半導體 | 紡織 |
航太 | 能源 | 教育娛樂 | 醫療照護 |
物聯網 | 系統整合 | 機器人



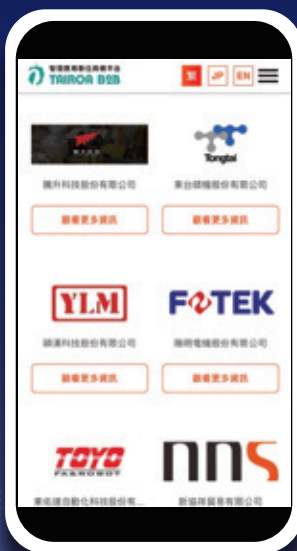
掃描尋找最佳自動化夥伴

NEW OPPORTUNITIES FOR BUSINESS

→ 產品分類搜尋



→ 檢索結果



→ 供應商公司簡介/產品總覽





市場焦點 Market Focus

12

經濟與景氣指標

資料來源：台灣經濟研究院、國家發展委員會、中華經濟研究院
資料整理：社團法人台灣智慧自動化與機器人協會

24

資安西遊記- 製造業資安的取經之旅

工研院產科國際所 林威佐

28

打造資通安全的台灣

國家實驗研究院科技政策研究與資訊中心
周媛韻 佐理研究員、王宣智 副研究員

產業脈動 Industry Trend

32

智慧製造的IoT 安全防護

緯謙科技股份有限公司 葉卯陽 總經理

34

智慧工廠資安 導入實戰經驗談

泓格科技股份有限公司 趙英傑 研發處長

產業脈動 Industry Trend

42

淺談智慧製造的資安防患與因應

TXOne Networks 鍾銘輝 市場研究團隊

48

華碩雲端雲原生、數位韌性
引領企業建構新世代經營 DNA

華碩雲端股份有限公司 數位轉型事業處暨技術服務處
潘育群總經理

56

智慧製造資安痛點與因應策略

中華資安國際股份有限公司 劉叡 鑑識暨健診部 經理

66

從無到有 打造智慧製造之資安防線
以某上櫃特用化學中小企業為例

聚和國際股份有限公司 總經理室暨資訊中心 王邦峻 協理

70

智能製造廠商可能面對的
資安威脅與防禦方式（應用層篇）

Sky Yu, Senior Security Solutions Architect-APAC Lead, Edgio

74

有效防禦勒索軟體 構建企業資安新思維

杜浦數位安全

78

跨網路資訊傳輸的零信任作法

達友科技股份有限公司
林皇興 副總經理 / CISSP/國際資安師證照

82

上市製造業公司
將安全性機制標準化案例分享

Akamai

86

Are Cybersquatters Going After
the Car Manufacturing Sector?

WhoisXML API Inc

產學研究&技術趨勢
Technology Research & Insight

88

自動化檢測類產線之LC、
異質機器手臂與AI視覺辨識間
Modbus-TCP通信協定設計

龍華科技大學機械工程系
蘇展弘、洪誌謙、王信宗、沈志陽、丁鯤、林欣穎

94

移印製程提昇之相關因素研究

萬能科技大學車輛工程系助理教授 周國達教授
翊揚能源科技公司工程師 王士榮

活動焦點 Special Events

104

AI視覺人才暑期特訓營
優質即戰力企業最愛

發那科的實習生活
國立臺灣科技大學 何慶軒

新亞洲儀器的實習生活
國立台北科技大學 詹承偉

110

用智慧科技導入指引重檢企業供應鏈
韌性與評估改善方式

社團法人台灣智慧自動化與機器人協會

118

2022第二屆機器人智動系統優質獎
發掘優秀人才，開發創新產品，
產業動起來！

社團法人台灣智慧自動化與機器人協會

122

服務型機器人創意實證
推進多元場域應用

社團法人台灣智慧自動化與機器人協會

好書推薦 Bookrecom

126

領導者的試煉

亞當·布萊安特 (Adam Bryant)
凱文·沙爾 (Kevin Sharer)



產業行事曆 Industrial Calendar

128

2023國際參訪及展覽資訊一覽表

社團法人台灣智慧自動化與機器人協會 整理

129

自動化與機器人協會
112 年度課程資訊

社團法人台灣智慧自動化與機器人協會 整理

實現您的智慧工廠

HIWIN 為工業 4.0 提供高附加價值的整體解決方案
全方位系列產品，實現您的智慧工廠。

HIWIN®



智慧自動化關鍵零組件
Key components for
Intelligent Automation



機電整合解決方案
Mechatronic Integration
Total Solution



智慧製造整合方案
Smart Manufacturing
Total Solution



加工產業的轉型升級
Machine Users to Upgrade
and Improve Productivity



上銀科技全球營運總部

上銀科技股份有限公司
HIWIN TECHNOLOGIES CORP.
台中市40852精密機械園區精科路7號
Tel : (04) 2359-4510
Fax: (04) 2359-4420
www.hiwin.tw
business@hiwin.tw



關係企業

大銀微系統股份有限公司
HIWIN MIKROSYSTEM CORP.
台中市40852精密機械園區精科中路6號
Tel : (04) 2355-0110
Fax: (04) 2355-0123
www.hiwinmikro.tw
business@hiwinmikro.tw



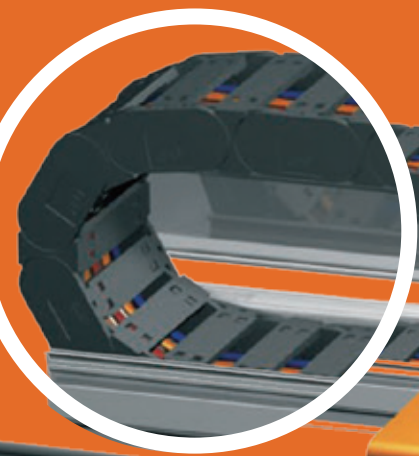
全球銷售暨服務據點

德國 www.hiwin.de	日本 www.hiwin.co.jp	美國 www.hiwin.us	義大利 www.hiwin.it
瑞士 www.hiwin.ch	捷克 www.hiwin.cz	法國 www.hiwin.fr	新加坡 www.hiwin.sg
韓國 www.hiwin.kr	中國 www.hiwin.cn	以色列 www.mega-fabs.com	

Keep Working...

readychain®
全裝配拖鏈系統

triflex R®
三維拖鏈管線包



igus.com.tw



台灣易格斯有限公司 40850台中市南屯區工業區24路35號5樓 電話:04-2358-1000 www.igus.com.tw

igus ReBeL®

具有四到六個自由度的 ReBeL® 工業和服務機器人



igus.com.tw



台灣易格斯有限公司 40850台中市南屯區工業區24路35號5樓 電話:04-2358-1000 www.igus.com.tw

六大”撇步”助企業邁向混合雲端

作者 | Epicor 亞洲區域副總裁鄧永泉

根據恩柏科(Epicor) 2022年行業見解報告^[1]，有 93% 具有某些雲端解決方案，且絕大多數的企業都採用混合式解決方案。新冠疫情驅使台灣企業比以往更加尋求科技解決業務營運挑戰。疫情亦反映，製造業缺乏能夠推動數位創新的基礎設施、安全和網絡架構能力。

雲端運算技術能提供實際的解決方案，使製造商更靈活應對新環境，透過在雲端部署額外伺服器、儲存及網絡資源，亦能快速擴展以滿足流量需求高峰。

但採用公有雲端最大的考量是控制權問題。雖然企業的內部部署的伺服器、儲存及網絡或能提供更好的控制權，可是需要聘請合適的人才管理，成本就變得非常昂貴，而預算限制亦使企業未能靈活應對市場需求。

目前有不少製造商都把混合雲端運算模式視為未來的發展趨勢，因為混合雲端能將本地部署運算的安全性及控制，以及公有雲端基礎設施的可擴展性和創新空間的特性相結合。使用時才付費，能省花費金錢在不再需要的資源上。有分析指出，混合雲端的需求正在飆升，複合年增長率高達 21%，到 2025 年全球市場規模將達 1.72 億美元。

雖然市場混合雲端運算的需求大增，但每家企業的需要及架構卻不同，混合雲端遷移策略亦必須根據企業需要量身訂造，以下六大”撇步”可確保您的混合雲端運算遷移旅程更順暢。

一）調查企業系統環境

目前企業每天可能運行數以百計的商業應用程式，但並非每個程式都需要遷移到雲端運行。企業必須了解自身運行的程式，根據其重要性、遷移到雲端的難易程度、以及程式遷移後能為企業帶來的效益，來決定各種應用程式的雲端遷移之旅。

二）捨難取易

其次，企業要清楚是否願意將最寶貴的知識產權，以及有關客戶關係的詳細資料轉移到並非自身擁有的基建設施上。例如在雲端環境為病人處理醫療數據，或進行知識產權相關的工程設計可能並不容易，當中涉及的隱私協議（如 HIPAA 對病患者機密性規則）的要求就非常嚴格。與其將困難的應用程式放上雲端，不如先從簡單的應用程式遷移做起，例如在雲端運行機器學習演算法。此做法可以為企業開創混合雲端應用案例，同時免卻業務風險或因法規帶來的障礙。

三）繪製關係架構圖

通常企業的各種應用程式都會共享數據庫，如果不清晰了解及整理好程式間的依賴及連結關係，將難以把應用程式遷移到雲端。要計劃遷移時，需要讓那些深入了解應用程式及其依賴關係的人員參與進來，除了能讓遷移更順利，更可以建立各主要參與者對遷移雲端的信心。

四）可考慮開放程式 (Open Source)

如果企業考慮將系統改為不同的應用程式、模組或數據庫的基建架構，可評估使用開放替代方案。開放軟體在質素方面已進步不少，尤其在雲端環境中就更為領先。目前最受歡迎的開放應用程式都比較穩定，並且得到大量活躍用戶支持。而開放軟體更有助節省程式的使用授權費用成本。

五）以人為本的流程

企業必須謹記，再領先的技術要能發揮出來，必須也要有人才和高效營運的配合，在遷移時必須考慮兩者情況以計劃藍圖。務必要讓您的員工充滿信心，畢竟遷移應用程式時，或會改變日常工作流程，並影響您的資訊科技員工。一般而言，人們都抗拒改變，建議可向員工分享發展藍圖，讓他們了解您的想法與全盤計劃，讓加強他們對當中流程的擁有權。這個也是坦誠對話和建立信任的良機，畢竟員工或不願意放棄他們多年來開發的應用程式和用戶群的控制，因為這與他們的身份和專業知識有關。

遷移到全新的雲端世界，同時讓資深員工有機會掌握「新技巧」，例如無數次重置密碼等瑣事，如果雲端服務供應商可將其自動化，將有助提高工作效率。

切記！遷移到雲端是一種合作關係，如果您的團隊沒有參與的話，最終只會以失敗收場。

六）定期審視遷移情況

當遷移完成後，最理想是定期評估混合雲端 tech stack（技術堆棧 - 做產品時選擇的開發工具與程式語言）的情況，看看它是否最能滿足您的需求。如果發現技術堆棧中仍有不少陳舊的本地系統，或之前行之有效的整合策略開始停滯不前時，就是時候審視您的雲生態系統，並聘請數據整合服務供應商。他們或能夠制定更順利且有效的計劃。

企業的未來取決於公司的靈活度及快速反應，未來大數據將繼續爆炸式增長，市場預測 2023 年，大數據市場規模將達到 1030 億美元，當中就需要強大、易於擴展，並且靈活按需要計費的運算能力。

雲端可以提高資安

製造商對雲端安全性一直存有顧慮。在一項研究發現，



有 72% 的企業將數據丟失風險視為是否使用 SaaS ERP 解決方案的主要決定因素。實際上，ERP 供應商的雲端通常比內部部署 ERP 擁有更高的安全性。數據安全性對製造商而言是一項複雜、具有挑戰性且花費昂貴，然而在商業競爭中的貢獻卻非常小。在恩柏科 (Epicor) 2022 年行業見解報告也有提及，在過去幾年之間，企業已快速地採用雲端 ERP；時至今日，絕大多數的企業皆已認同此類解決方案能帶來眾多優勢。事實上，有 90% 的企業對於使用雲端解決方案這件事感到安心。

相比之下，ERP 供應商的雲端服務商卻必須將數據的安全性視為當務之急，並斥以鉅資。ERP 供應商的合作伙伴的數據中心提供了可靠且極具成本效益的數據安全功能，這些功能以前僅使用於大型公司，而且價格不菲。這種轉移說明了眾多專家對雲端的安全性的認可，可見安全性已成為雲端的主要優勢，而非薄弱環節。

採用混合雲端運算方式，不單有安全認可的資安，還可助您透過數位轉型的力量來發揮您的優勢，但企業就必須有一套量身訂造的策略，才能把握現在邁向未來。



掃二維碼查看更多資訊

¹資料來源:
<https://www.epicor.com/zh-tw/resources/library/corporate/industry-insights-report/>

作者簡介

鄧永泉為現任 Epicor 亞洲區域副總裁，從事企業資源規劃軟體產業超過 30 年，對於亞洲區製造業和物流配送業的發展及數位轉型，見解精闢獨到，尤其能助高管人員作出明智決策。



台灣智動化檢測驗證聯盟，由社團法人台灣智慧自動化與機器人協會標準委員會成立，為促進台灣產業發展，建立機器人及智慧自動化安全管理機制宣傳之平台。整合並串聯相關設備之製造、進口、系統整合、使用者、檢測驗證等產學研單位，加速擴大宣傳標準及檢測驗證之重要性，提升台灣智慧自動化與機器人產業競爭力。

聯盟任務

- 蒐集並推廣智動化產業相關國際標準、區域標準及產業標準。
- 成為智動化產業相關安全標準諮詢管道。
- 作為諮詢及媒合平台，推動智慧自動化設備檢測驗證媒合需求。
- 依據特定標準、安全規範、產品設計等業者需求，辦理教育訓練。
- 辦理或推動實驗室能力一致性測試，提升檢測驗證能力。
- 協助政府推動機器人及智慧自動化設備，強化本質安全與推動產業自主管理機制。
- 其他經聯盟成員建議之。

會員資格

- 產業、政府、學術及研究單位。
- 驗證機構及測試實驗室：須符合 IAF 及 ilac 體系或其他同等單位所認可之機構。
- 機器人及智慧自動化相關設備使用者。

洽詢窗口

社團法人台灣智慧自動化與機器人協會 標準組
40852臺中市南屯區精科路26號4樓

Dennis 04-23581866#32 dennis@tairoa.org.tw
Cathy 04-23581866#33 cathy@tairoa.org.tw



▲熱烈招募，歡迎入會

出刊者 社團法人台灣智慧自動化與機器人協會
地址 40852台中市南屯區精科路26號4樓
電話 +886-4-2358-1866
傳真 +886-4-2358-1566

發刊時程 每季一期
本期出版日期 民國111年12月號
發行期數 期刊，全彩印刷
發行數量 1,000-3,000本/期
發行區域 國內及國外重要機器人與智動化展覽
發行對象 社團法人台灣智慧自動化與機器人協會全體會員、工具機暨零組件業、物流傳動業、汽機車與自行車業、食品製造廠、紡織、電機電子業、五金業等設備或零組件製造商、研發單位及學術機構等，發行對象遍及產業供需體系，國內外展覽會。

編輯單位 社團法人台灣智慧自動化與機器人協會
Taiwan Automation Intelligence and Robotics Association
地址 40852台中市南屯區精科路26號4樓
4F., No.26, Jingke Rd., Nantun Dist., Taichung City 408, Taiwan (R.O.C.)
10059台北市新生南路一段50號6樓603室
Rm. 603, 6F., No.50, Sec. 1, Xincheng S. Rd., Zhongzheng Dist., Taipei City 100, Taiwan (R.O.C.)
聯絡專線 (04)2358-1866、(02)2393-1413
傳真 (04)2358-1566、(02)2393-1405
電子郵件 service@tairoa.org.tw
網址 www.tairoa.org.tw
美術編輯 九禾廣告媒體整合行銷公司 J&M MEDIA CORPORATION 04-22965959
投稿說明 (一) 歡迎各界提供智慧製造/機器人相關產業趨勢及技術文章，來稿採用匿名審查制度，由本出版單位編輯部與相關學者專家審核之。
(二) 凡接受刊登之文章，本出版單位得視編輯之需要，決定刊登的版面配置與形式。
版權所有 非經同意請勿轉載。本刊內文文責由作者自負，文章著作權由本刊享有，欲利用本刊內容者，須徵求社團法人台灣智慧自動化與機器人協會同意或書面授權。



經濟與景氣指標

景氣概況本次發布日期為11月25日；臺灣採購經理人指數本次發布日期為12月1日

資料來源：台灣經濟研究院、國家發展委員會、中華經濟研究院
資料整理：社團法人台灣智慧自動化與機器人協會

觀察近期國際經濟情勢，10月主要經濟體領先指標與製造業採購經理人指數(PMI)續呈走低態勢，且依經濟合作暨發展組織(OECD)的經濟展望報告表示，由於俄烏戰爭引發的能源衝擊繼續刺激通膨，全球經濟將在明年進一步放緩，2023年全球經濟成長表現有很大程度上來自於亞洲新興市場經濟體，而美國和歐洲則急劇減速。

國內製造業方面，全球經濟受到通膨及升息影響，終端市場需求疲弱，廠商持續進行庫存調整，設備投資意願趨向保守觀望，故製造業廠商對當月與未來半年景氣看法多呈悲觀與持平，不過廠商對景氣看壞程度較上月調查相比略為改善。服務業隨著國境開放，民眾已漸習慣與病毒共存，消費人潮回流，使餐旅業者看好當月與未來半年景氣表現。此外，10月金融市場表現持續疲弱，券商經紀手續費收入與自營獲利減少，且壽險保費收入下滑，加上產險業仍處虧損狀態，故證券業與保險業者大多看壞當月景氣表現。營建業方面，10月續呈下滑主要來自於營造業與不動產業對當月均顯悲觀，建築工程業者因房市不景氣，工程承攬情況仍未

好轉，加上不動產業者面臨金融市場表現疲弱、房貸利率走高、國內外經濟下行壓力仍大，致使房市交易件數萎縮的情況日趨顯著所致，故營建業有超過一半比例的廠商看壞當月景氣表現，且對未來半年景氣看法續呈保守。根據調查結果，10月製造業、服務業與營建業營業氣候測驗點均呈下滑態勢。

美國國際情勢方面，美國商務部經濟分析局(BEA)發布2022年第三季美國經濟成長數值；第三季GDP成長年增率(yoy)為1.8%，與第二季數值持平。美國經濟在內需市場表現方面，第三季的民間消費與民間投資成長年增率，分別為2.0%與2.3%。而同一時間的外需表現上，美國的商品與勞務出口及進口成長年增率則分別為11.3%與7.5%。此外IHS Markit與EIU皆於11月發布美國於2022全年的經濟成長率預測，分別是1.8%與1.7%；分屬較前一個月預測值上修0.1與0.2個百分點。

有關美國就業市場表現方面，根據美國勞動統計局公布資料，美國於2022年10月的失業率為3.7%，較前一個月失業率增加0.2個百

分點；此外10月美國非農就業人口增加26.1萬人，就業市場表現仍佳。物價方面，美國2022年10月消費者物價指數(CPI)年增率為7.7%，較前月數值下滑0.5個百分點。扣除食品與能源價格的核心CPI年增率則為6.3%，較前月數值下滑0.3個百分點。美國通膨壓力仍大，聯準會(Fed)已於2022年11月3日升息3碼，亦即自3月以來總共已經升息15碼；聯邦基金利率來到3.75-4.0%區間。美國就業市場表現佳，而通膨壓力仍大，因此預計Fed持續於12月升息的機率高。

至於美國經濟近期的景氣展望方面，參考美國供應管理研究所(Institute of Supply Management, ISM)公佈美國的2022年10月製造業採購經理人指數(PMI)為50.2點，較前一個月數值下滑0.7點。另外ISM公佈的2022年10月服務業PMI為54.4點，較前一個月指數下滑2.3點。美國兩項PMI數值雖仍高於50點以上，但是皆屬持續下滑，亦即美國景氣呈現由擴張趨向緊縮態勢。

日本方面，日本內閣府公布2022年第3季國內生總值(GDP)第1次速報值顯示，扣除物價影響後的實質GDP年增率為1.8%，較第2季增加0.1個百分點，主要是因民間消費、民間企業設備投資較分別由第2季增加1.2、3.7個百分點來到4.3%及4.1%水準。財務省公布2022年10月進口金額為11兆1,638億日圓，較2021年同期年增53.5%，為連續21個月的正成長；出口額為9兆15億日圓，較2021年同期年增25.3%，為連續20個月的正成長。IHS Markit引用JIBUN BANK日本製造業採購經理人指數(PMI)，受到全球通膨及主要貿易夥伴經濟疲軟，新訂單出現連續4個月衰退，致生產衰退，製造商減少投入品採購，致10月PMI指數來到50.7點，較9月減少0.1點，為連續第21個月在榮枯線之上。

中國方面，2022年10月全國規模以上(主要業務收入在2,000萬元及以上的工業企業)工業增加值年增率為5.0%，較9月減少1.3個百分點，其中製造業、電力、熱力、燃氣及水生產業及供應業及採礦業增加值分別成長5.2%、4.0%及4.0%；10月社會消費品零售額達4兆271億人民幣，年減0.5%，為6月份以來首度轉為負成長，其中商品零售成長0.5%，餐飲收入年減8.1%；1-10月固定資產投資(不含農戶)成長5.8%，其中民間固定投資成長1.6%。另海關總署公布2022年10月貿易額達5,115.9億美元，較2021年同期衰退0.4%，其中出口衰退0.3%，進口衰退0.7%；1-10月貿易年增率為7.7%，其中出口成長11.1%、進口成長3.5%，前三大出口地區為美國(16.5%)、歐盟(15.8%)及東協(15.5%)，出口合計占比達47.8%。

在生產與商業活動方面，受到需求減少，致生產、新訂單及從業人員等活動降低，10月PMI指數為49.2%，較9月減少0.9個百分點，以企業規模來看，大、中、小型企業PMI分別較9月減少1.0、0.8及0.1個百分點來到50.1%、48.9%及48.2%。非製造業活動指數來到48.7%，較9月減少1.9個百分點。

國內情勢方面，首先在對外貿易，儘管塑化與基本金屬等傳產貨類終端買氣續疲，且光學器材外銷減幅持續擴大，然受惠於高效能運算、車用電子、資料中心等創新科技需求仍受支撐，加上國際品牌智慧手機新機拉貨效應，抵消部分減幅，10月出口年增率從上月衰退5.33%轉為至衰退0.46%，連續兩個月衰退。在主要出口產品方面，受到積體電路及資通產品需求上升，令電子零組件出口年增率再度轉為雙位數成長，資通與視聽產品出口年增率由負轉正。再者，光學器材因消費性電子產品需求疲弱，客戶持續消化庫

存，出口年減41.96%，基本金屬、化學品、紡織品隨終端消費動能低迷，減幅分別高達27.64%、18.54%、23.52%；進口方面，受惠於資本設備購置推升，加上手機進口大增，令資本設備與消費品進口年增率由負轉正，10月進口年增率成長從上月衰退2.57%轉為成長5 8.22%。累計今年1至10月出口較去年同期成長11.96%，進口成長16.94%，總計2022年1至10月出超金額為437.19 億美元，衰退17.35%。

國內生產方面，因終端消費需求疲弱，庫存調整持續，以及設備投資意願保守，業者採取減產策略調節產能，致使10月化學原材料業、基本金屬業分別年減22.15%、21.14%，連續五個月呈現雙位數衰退，機械設備業亦年減少10.76%。在電子零組件業方面，儘管消費性電子產品需求下滑，客戶進行庫存調整影響，然受惠於國際品牌新機拉貨，加上高效能運算等晶片需求暢旺，令電子零組件業生產指數由負轉正，年增2.09%。10月工業生產指數年減3.56%，連續兩個月呈現衰退態勢，總計2022年1至10月工業生產較去年同期增加2.58%，其中製造業增加2.71%。

一、景氣對策信號

111年10月為18分，較上月增加1分，燈號續呈黃藍燈。9項構成項目中，機械及電機設備進口值由綠燈轉呈紅燈，分數增加2分，貨幣總計數M1B由綠燈轉呈黃藍燈，分數減少1分；其餘7項燈號不變。個別構成項目說明如下：

- 貨幣總計數M1B變動率：由上月6.7%減至5.5%，燈號由綠燈轉呈黃藍燈。
- 股價指數變動率：由上月-17.0%減

內需消費方面，儘管百貨業者週年慶活動陸續登場，有助於推升買氣，然受到上年同月振興方案高基期影響，使得10月百貨公司營業額僅年增0.10%，量販店營業額年增率甚至轉為負成長。其他綜合商品零售業則受惠於邊境管制放寬，出入境旅客人潮增加，帶動免稅店業績成長，年增20.68%，連續五個月呈雙位數成長，故10月整體零售業營業額年增率從上月7.84%縮小至2.05%，累計1至10月零售業營業額較上年同期相比增7.86%。

勞動市場方面，因工作場所業務緊縮或歇業而失業的人數較上月減少，2022年10月失業率3.64%，較上月下降0.02個百分點，不過受到去年比較基期偏高，故10月失業率較上年同月下降0.19個百分點，總計2022年1至10月失業率平均為3.69%，較上年同期下降0.33個百分點。在薪資方面，2022年9月總薪資為52,503元，較2021年同月增加0.82%，9月經常性薪資為44,417元，較2021年同月增加2.39%，若以全年平均情況觀察，在扣除物價上漲因素後，2022年前三季實質經常性薪資為41,369元較 2021年同期衰退0.07%。

- 至-21.6%，燈號續呈藍燈。
- 工業生產指數變動率：由上月上修值-4.3%增至-2.9%，燈號續呈藍燈。
- 非農業部門就業人數變動率：由上月-0.06%減至-0.2%，燈號續呈藍燈。
- 海關出口值變動率：由上月7.1%增至8.1%，燈號續呈綠燈。

- 機械及電機設備進口值變動率：由上月6.1%增至17.3%，燈號由綠燈轉呈紅燈。
- 批發、零售及餐飲業營業額變動率：由上月上修值4.4%減至4.1%，燈號續呈綠燈。
- 製造業銷售量指數變動率：由上月上修值-6.7%減少至 -7.3%，燈號續呈藍燈。
- 製造業營業氣候測驗點：由上月下修值84.6點減至84.2點，燈號續呈藍燈。

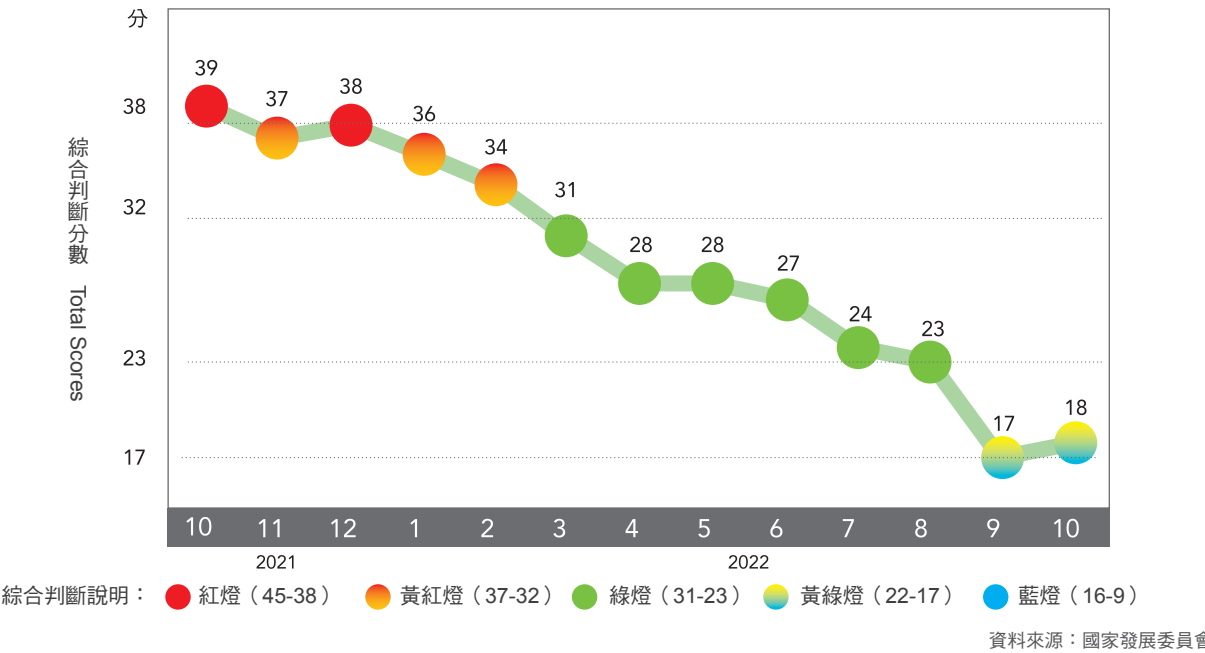


圖1. 近一年景氣對策信號走勢圖

景氣對策訊號		2021年			2022年											
		10月	11月	12月	1月	2月	3月	4月	5月	6月	7月	8月	9月		10月	
													燈號	%	燈號	%
綜合判斷	燈號	●	●	●	●	●	●	●	●	●	●	●	●		●	
	分數	39	37	38	36	34	31	28	28	27	24	23	17		18	
貨幣總計數M1B		●	●	●	●	●	●	●	●	●	●	●	●	6.7	●	5.5
股價指數		●	●	●	●	●	●	●	●	●	●	●	●	-17.0	●	-21.6
工業生產指數		●	●	●	●	●	●	●	●	●	●	●	●	-4.3 _r	●	-2.9
非農業部門就業人數		●	●	●	●	●	●	●	●	●	●	●	●	-0.06	●	-0.2
海關出口值		●	●	●	●	●	●	●	●	●	●	●	●	7.1	●	8.1
機械及電機設備進口值		●	●	●	●	●	●	●	●	●	●	●	●	6.1	●	17.3
製造業銷售量指數		●	●	●	●	●	●	●	●	●	●	●	●	-6.7 _r	●	-7.3
批發、零售及餐飲業營業額		●	●	●	●	●	●	●	●	●	●	●	●	4.4 _r	●	4.1
製造業營業氣候測驗點		●	●	●	●	●	●	●	●	●	●	●	●	84.6 _r	●	84.2

註：1. 各構成項目除製造業營業氣候測驗點之單位為點（基期為95年）外，其餘均為年變動率；除股價指數外均經季節調整。
2. r為修正值。

資料來源：國家發展委員會

圖2. 一年來景氣對策信號

二、景氣指標

領先指標

領先指標不含趨勢指數為95.63，較上月下降0.97%（詳表1、圖3）。

7個構成項目經去除長期趨勢後，僅實質半導體設備進口值較上月上升；其餘6項較上月下滑，分別為：外銷訂單動向指數、股價指

數、製造業營業氣候測驗點、實質貨幣總計數M1B、工業及服務業受僱員工淨進入率、建築物開工樓地板面積。

表1. 景氣領先指標

項 目	111年 (2022)						
	4月	5月	6月	7月	8月	9月	10月
不含趨勢指數	101.53	100.53	99.45	98.44	97.50	96.57	95.63
較上月變動 (%)	-0.81	-0.99	-1.07	-1.02	-0.95	-0.96	-0.97
構成項目 ¹							
外銷訂單動向指數 ²	99.92	99.51	99.06	98.60	98.14	97.68	97.21
實質貨幣總計數M1B	99.95	99.70	99.47	99.24	99.04	98.83	98.63
股價指數	100.24	99.90	99.52	99.12	98.72	98.28	97.84
工業及服務業受僱員工淨進入率 ³	100.39	100.28	100.15	100.01	99.86	99.67	99.48
建築物開工樓地板面積 ⁴	100.84	100.63	100.31	100.06	99.90	99.78	99.68
實質半導體設備進口值	99.64	99.72	99.85	99.99	100.14	100.26	100.39
製造業營業氣候測驗點	99.85	99.34	98.85	98.40	98.00	97.64	97.29

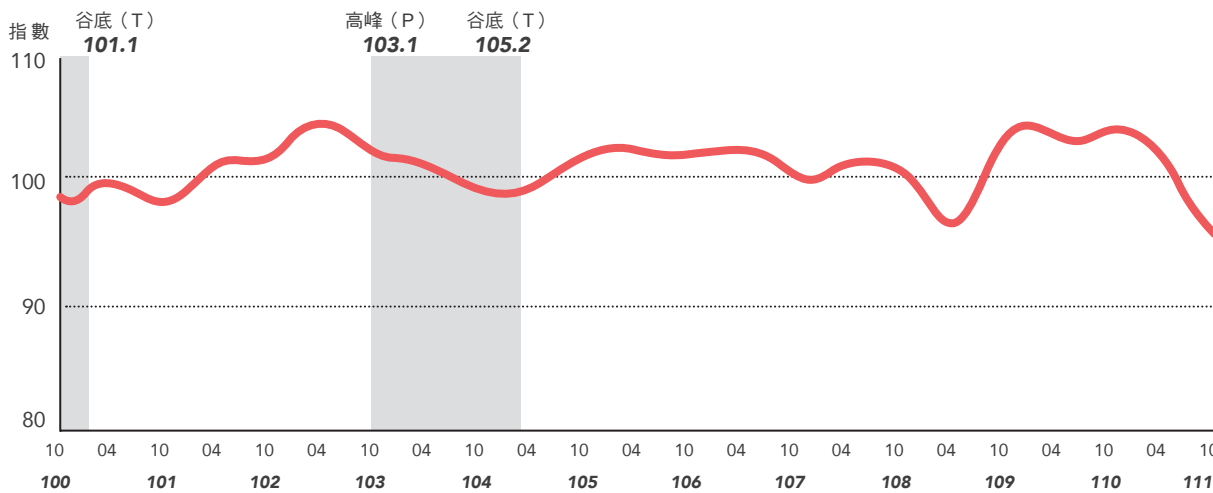
註：1.本表構成項目指數為經季節調整、剔除長期趨勢，並平滑化與標準化後之數值。以下表同。

資料來源：國家發展委員會

2.外銷訂單動向指數採用以家數計算之動向指數。

3.淨進入率=進入率-退出率。

4.建築物開工樓地板面積僅包含住宿類（住宅）、商業類、辦公服務類、工業倉儲類4項統計資料。



註：陰影區表景氣循環收縮期，以下圖同。

資料來源：國家發展委員會

圖3. 領先指標不含趨勢指數走勢圖

同時指標

同時指標不含趨勢指數為95.05，較上月下降1.34%（詳表2、圖4）。

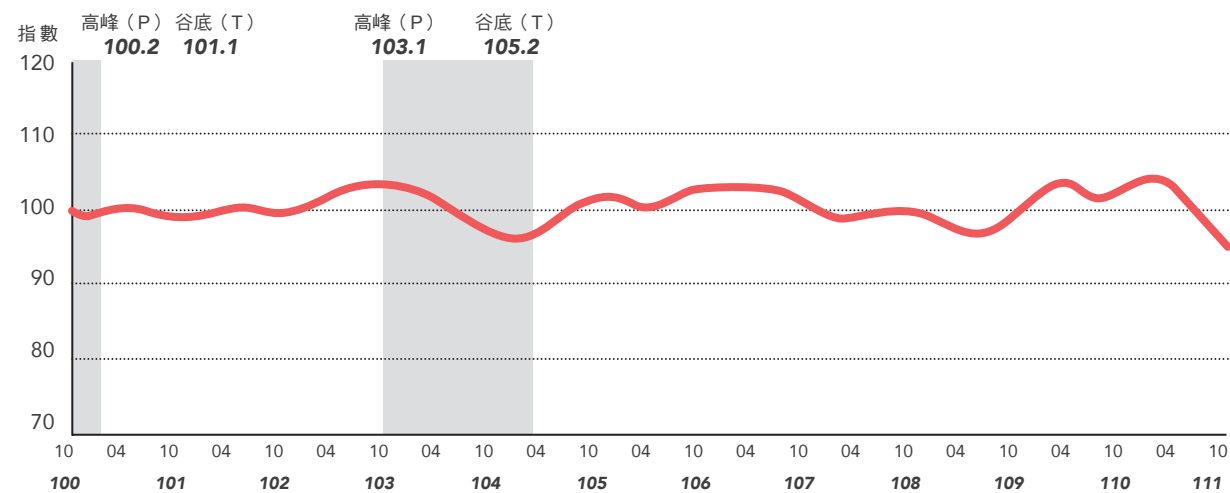
7個構成項目經去除長期趨勢後，僅非農業部門就業人數較上月上升；其餘6項較上月下滑，分別為：工業生產指數、製造業銷售量

指數、實質海關出口值、實質機械及電機設備進口值、批發、零售及餐飲業營業額、電力（企業）總用電量。

表2. 景氣同時指標

項 目	111年 (2022)						
	4月	5月	6月	7月	8月	9月	10月
不含趨勢指數	102.66	101.67	100.47	99.13	97.72	96.35	95.05
較上月變動 (%)	-0.67	-0.97	-1.18	-1.33	-1.43	-1.41	-1.34
構成項目 ¹							
工業生產指數	100.47	100.17	99.80	99.34	98.79	98.17	97.55
電力(企業)總用電量	100.25	100.13	100.03	99.90	99.66	99.37	99.07
製造業銷售量指數	100.34	99.89	99.39	98.84	98.26	97.65	97.04
批發、零售及餐飲業營業額	101.38	100.98	100.52	100.03	99.60	99.24	98.92
非農業部門就業人數	99.94	99.76	99.64	99.58	99.59	99.65	99.73
實質海關出口值	101.66	101.25	100.65	99.92	99.20	98.58	98.05
實質機械及電機設備進口值	100.58	100.36	100.04	99.65	99.22	98.79	98.40

資料來源：國家發展委員會



註：陰影區表景氣循環收縮期，以下圖同。

資料來源：國家發展委員會

圖4. 同時指標不含趨勢指數走勢圖

落後指標 落後指標不含趨勢指數為102.76，經回溯修正後較上月下降0.39%（詳表3、圖5）。

5個構成項目經去除長期趨勢後，2項較上月上升，包括金融業隔夜拆款利率、失業率；其餘3項較上月下滑，分別為：全體金融機構放款與投資、製造業存貨價值、製造業單位產出勞動成本指數。

表3. 景氣落後指標

項 目	111年 (2022)						
	4月	5月	6月	7月	8月	9月	10月
不含趨勢指數	102.59	103.09	103.43	103.57	103.46	103.16	102.76
較上月變動 (%)	0.55	0.48	0.33	0.14	-0.10	-0.30	-0.39
構成項目 ¹							
失業率 ¹	100.60	100.56	100.53	100.53	100.55	100.58	100.61
製造業單位產出勞動成本指數	100.27	100.83	101.31	101.65	101.84	101.89	101.88
金融業隔夜拆款利率	99.97	100.05	100.14	100.23	100.32	100.42	100.52
全體金融機構放款與投資	100.46	100.07	99.63	99.18	98.72	98.24	97.75
製造業存貨價值	101.42	101.73	101.99	102.16	102.21	102.20	102.15

註：¹失業率取倒數計算。

資料來源：國家發展委員會

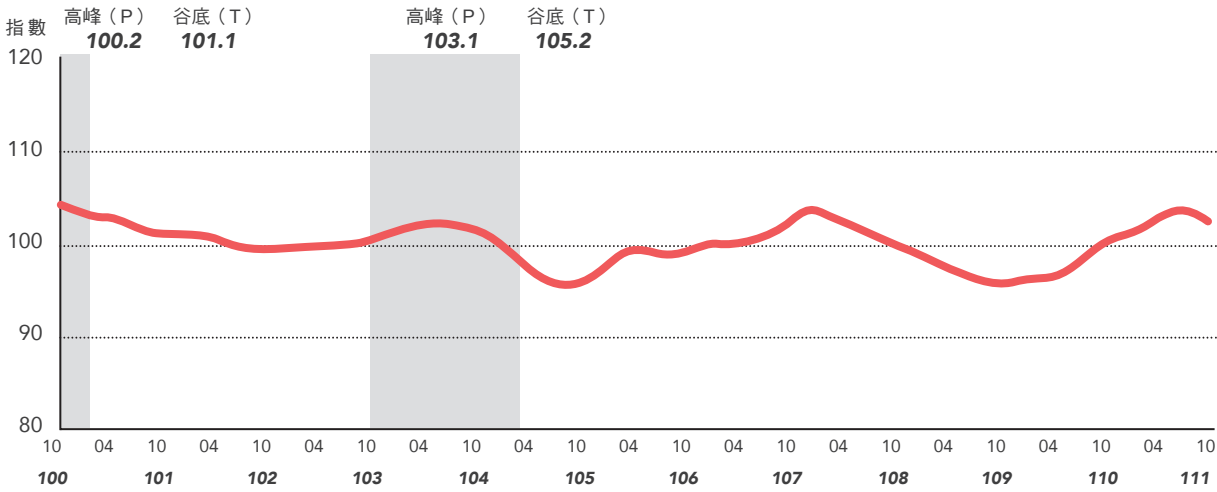


圖5. 落後指標不含趨勢指數走勢圖

資料來源：國家發展委員會

三、製造業採購經理人指數(PMI)

2022年11月經季節調整後之台灣製造業採購經理人指數（PMI）已連續5個月緊縮，本月指數回跌1.5個百分點至43.9%。

- 五項組成指標中，新增訂單、生產與人力僱用緊縮，供應商交貨時間下降，存貨緊縮。

- 領先反應景氣動態之新增訂單指數已連續8個月緊縮，惟緊縮速度未再大幅走跌，指數微跌0.9個百分點至41.9%。

- 經季調後之生產指數回跌1.8個百分點至42.8%，連續第5個月緊縮。

- 製造業之未來六個月展望指數回升0.5百分點至25.3%，連續第7個月緊縮。

- 2022年11月四大產業回報PMI緊縮，依緊縮速度排序為電子暨光學產業（39.4%）、

電力暨機械設備產業（40.0%）、基礎原料產業（44.7%）與化學暨生技醫療產業（45.1%）。食品暨紡織產業（52.6%）與交通工具產業（51.3%）則轉為回報PMI擴張。

- 六大產業全數回報未來六個月展望呈現緊縮，依緊縮速度排序為電力暨機械設備產業（15.4%）、電子暨光學產業（22.5%）、交通工具產業（27.1%）、基礎原料產業（29.1%）、化學暨生技醫療產業（31.4%）與食品暨紡織產業（35.2%）。

2022年11月四大產業回報PMI緊縮，依緊縮速度排序為電子暨光學產業（39.4%）、電力暨機械設備產業（40.0%）、基礎原料產業（44.7%）與化學暨生技醫療產業（45.1%）。食品暨紡織產業（52.6%）與交通工具產業（51.3%）則轉為回報PMI擴張。

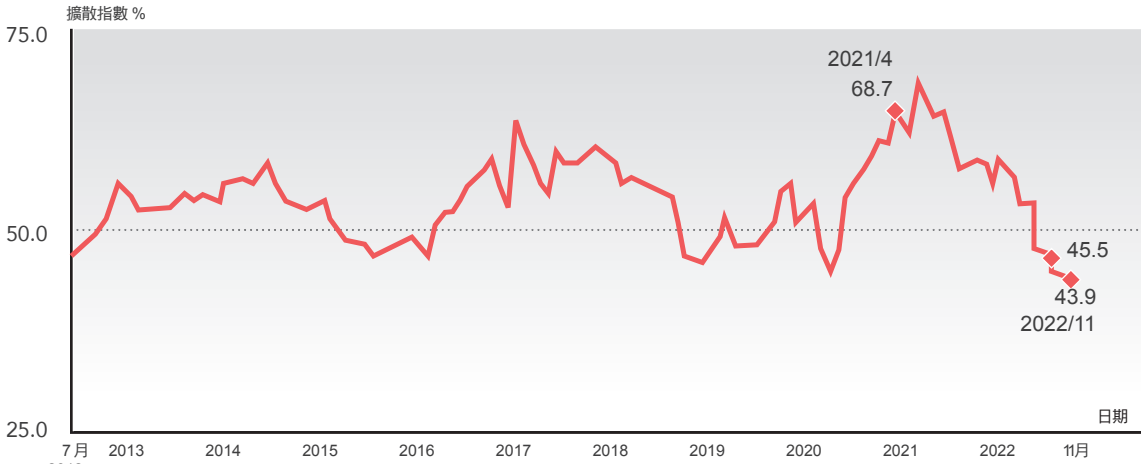


圖6. 臺灣製造業PMI時間序列走勢圖

資料來源：中華經濟研究院

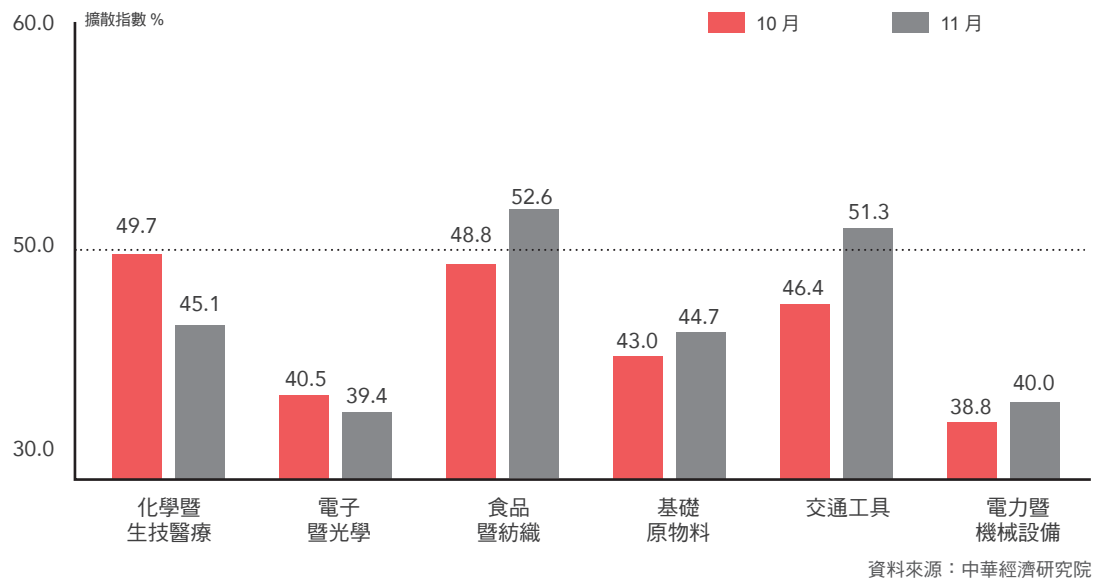


圖7. 產業別PMI示意圖

表4. 2022年11月臺灣製造業採購經理人指數

單位：%

	產 業 別												
	2022 11月	2022 10月	百分點變化	方向	速度	趨勢連續月份		化學暨生技醫療	電子暨光學	食品暨紡織	基礎原物料	交通工具	電力暨機械設備
臺灣製造業PMI	43.9	45.2	-1.5	緊縮	加快	5		45.1	39.4	52.6	44.7	51.3	40.0
新增訂單數量	41.9	42.8	-0.9	緊縮	加快	8		41.4	34.0	59.3	40.7	50.0	29.5
生產數量	42.8	44.6	-1.8	緊縮	加快	5		37.1	36.9	53.7	46.5	58.3	37.2
人力僱用數量	48.3	48.9	-0.6	緊縮	加快	4		47.1	44.7	57.4	50.0	52.1	46.2
供應商交貨時間	42.7	44.3	-1.6	下降	加快	5		47.1	42.2	44.4	40.7	47.9	39.7
存貨	43.6	46.5	-2.9	緊縮	加快	3		52.9	39.3	48.1	45.3	47.9	47.4
客戶存貨	49.9	50.1	-0.2	過低	前月為過高	1		50.0	51.6	53.7	44.2	47.9	50.0
原物料價格	45.9	45.1	+0.8	下降	趨緩	5		41.4	43.9	64.8	45.3	52.1	46.2
未完成訂單	32.0	33.7	-1.7	緊縮	加快	6		41.4	29.9	48.1	26.7	43.8	24.4
新增出口訂單	35.5	33.5	+2.0	緊縮	趨緩	7		48.6	34.0	44.4	29.1	43.8	30.0
進口原物料數量	35.0	34.9	+0.1	緊縮	趨緩	6		45.7	30.7	50.0	33.7	41.7	33.3
未來六個月展望	25.3	24.8	+0.5	緊縮	趨緩	7		31.4	22.5	35.2	29.1	27.1	15.4
生產用物資(平均天數)	43	44	-	-	-	-		41	42	46	48	42	39
維修與作業耗材(平均天數)	35	38	-	-	-	-		36	32	40	41	35	32
資本支出(平均天數)	71	68	-	-	-	-		65	67	104	63	79	69

資料來源：中華經濟研究院

四、非製造業經理人指數 (NMI)

2022年11月末季調之台灣非製造業經理人指數（NMI）僅維持1個月的持平（50.0%）隨即轉為擴張，指數回升2.2個百分點至52.2%。

八大產業中，七大產業NMI呈現擴張，依擴張速度排序為住宿餐飲業（62.5%）、資訊

暨通訊傳播業（58.1%）、教育暨專業科學業（54.6%）、營造暨不動產業（51.6%）、金融保險業（51.2%）、零售業（51.2%）與運輸倉儲業（50.5%）。批發業（41.9%）則持續回報NMI呈現緊縮。

• 四項組成指標中，商業活動與新增訂單轉

為擴張，人力僱用擴張，供應商交貨時間上升。

• 商業活動與新增訂單（新增簽約客戶或業務）皆由緊縮轉為擴張，二指數分別回升5.0與4.9個百分點至51.3%與51.4%。

• 未完成訂單（工作委託量）已連續4個月緊縮，惟本月指數回升5.0個百分點至45.1%。

• 服務收費價格指數已連續30個月呈現上升（高於50.0%），惟本月指數回跌3.3個百分點至53.2%。

• 存貨觀感已連續7個月過高（高於50.0%，高於當前營運所需），指數在9月攀升至2018

年12月以來最高（55.5%）後，本月指數續跌0.4個百分點至54.7%。

• 未來展望已連續8個月緊縮，惟指數回升3.8個百分點至37.4%。

• 八大產業中，七大產業回報未來六個月展望呈現緊縮，各產業依緊縮速度排序為批發業（24.0%）、營造暨不動產業（29.0%）、金融保險業（32.6%）、運輸倉儲業（35.2%）、教育暨專業科學業（41.7%）、零售業（42.9%）與資訊暨通訊傳播業（47.1%）。住宿餐飲業已連續6個月回報未來六個月展望呈現擴張，指數為75.0%。

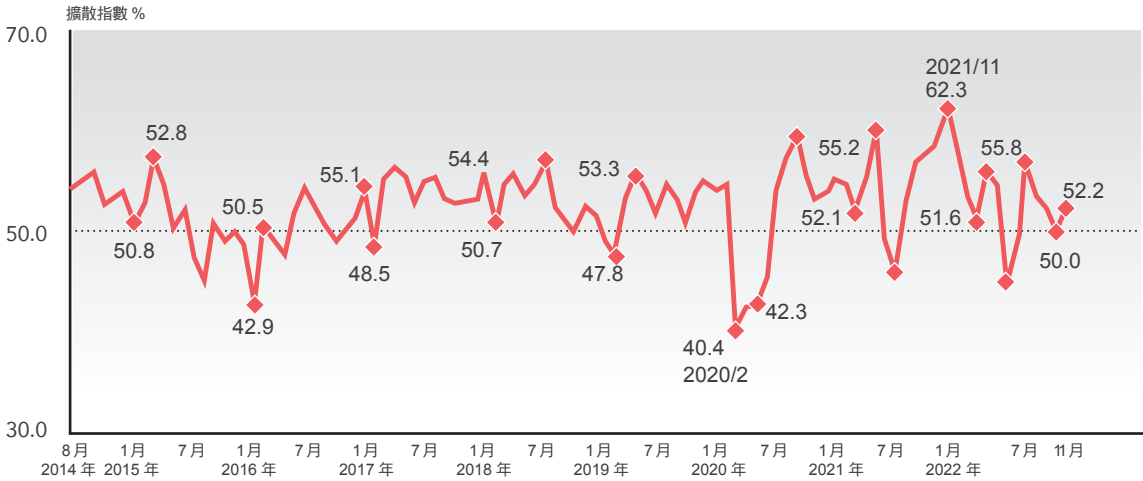


圖8. 臺灣非製造業NMI時間序列走勢圖

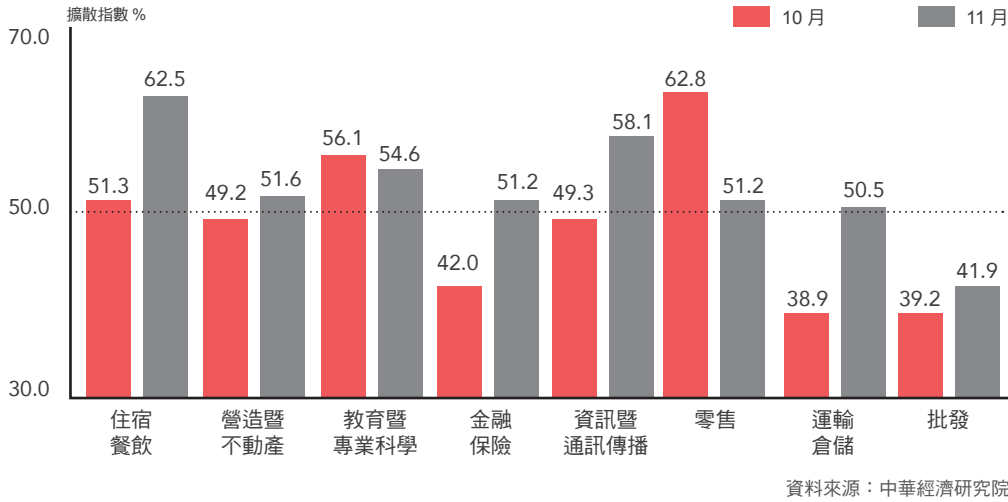


圖9. 產業別NMI示意圖

表5. 2022年11月臺灣非製造業採購經理人指數

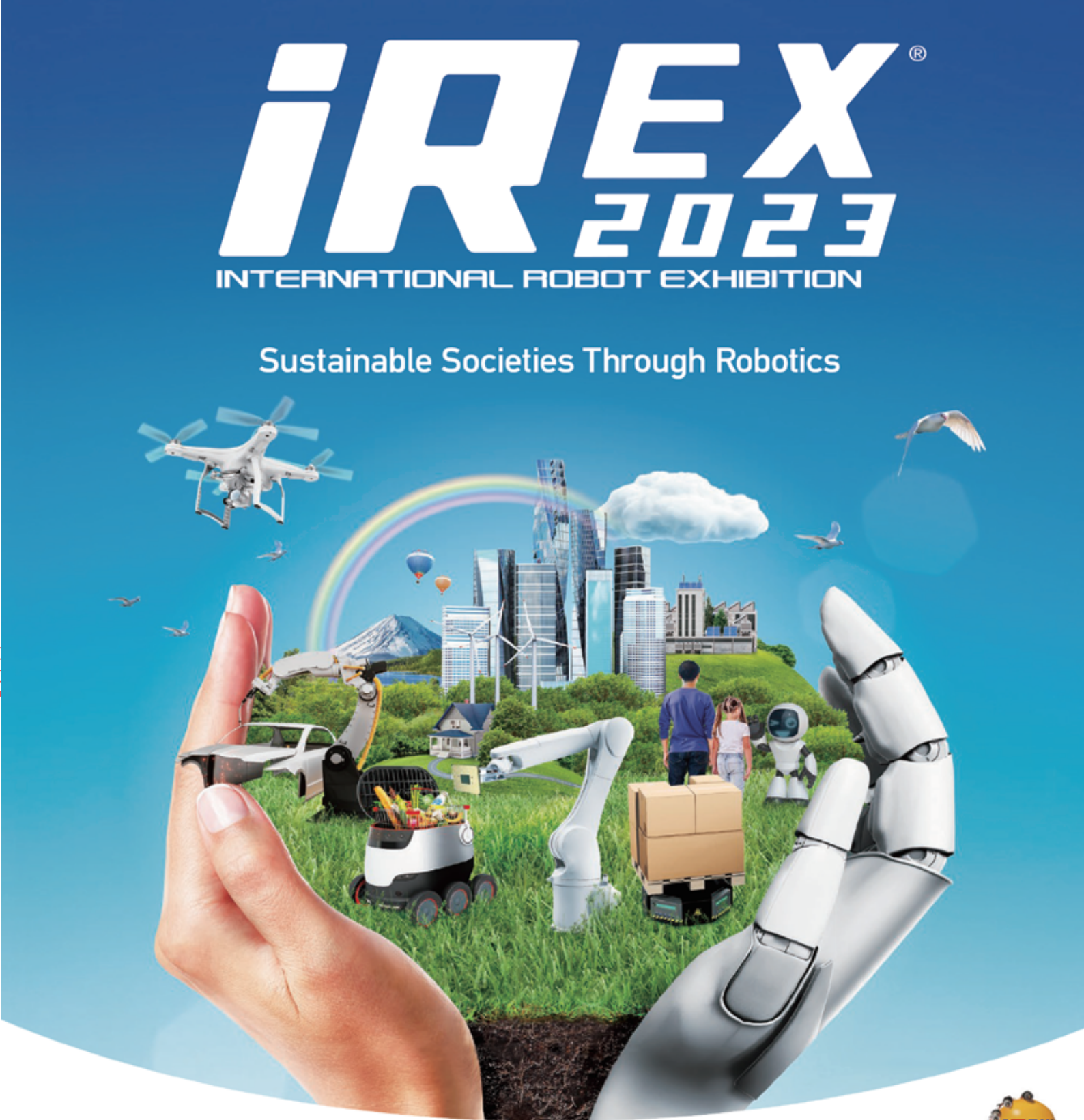
單位：%	產業別												
	2022 11月	2022 10月	百分點 變化	方向	速度	趨勢 連續月份	住宿 餐飲	營造暨 不動產	教育暨 專業科學	金融 保險	資訊暨 通訊傳播	零售	運輸 倉儲
臺灣NMI	52.2	50.0	+2.2	擴張	前月為持平	1	62.5	51.6	54.6	51.2	58.1	51.2	50.5
商業活動	51.3	46.3	+5.0	擴張	前月為緊縮	1	62.5	43.5	55.0	60.5	61.8	54.8	42.6
新增訂單	51.4	46.5	+4.9	擴張	前月為緊縮	1	62.5	45.2	63.3	488	61.8	50.0	46.3
人力僱用	53.1	53.0	+0.1	擴張	加快	6	70.8	51.6	53.3	47.7	52.9	50.0	63.0
供應商交貨時間	53.1	54.0	-0.9	上升	趨緩	37	54.2	66.1	46.7	47.7	55.9	50.0	44.0
存貨	52.6	53.5	-0.9	擴張	趨緩	5	54.2	58.1	51.7	44.2	58.8	40.5	59.3
採購價格	63.3	67.3	-4.0	上升	趨緩	83	79.2	54.8	63.3	69.8	67.6	71.5	61.1
未完成訂單	45.1	40.1	+5.0	緊縮	趨緩	4	62.5	35.5	50.0	40.7	50.0	45.2	35.2
服務輸出/出口	41.5	41.8	-0.3	緊縮	加快	10	83.3	40.0	40.0	42.9	50.0	10.0	26.9
服務輸入/進口	50.3	48.5	+1.8	擴張	前月為緊縮	1	50.0	53.3	50.0	38.9	64.3	35.7	28.6
服務收費價格	53.2	56.5	-3.3	上升	趨緩	30	75.0	50.0	51.7	45.3	55.9	57.1	44.4
存貨觀感	54.7	55.1	-0.4	過高	趨緩	7	50.0	51.6	51.7	46.5	52.9	54.8	70.4
未來六個月展望	37.4	33.6	+3.8	緊縮	趨緩	8	75.0	29.0	41.7	32.6	47.1	42.9	35.2

資料來源：中華經濟研究院

五、未來半年個別產業景氣預測 (以2022年10月為預測基準月)



未來半年景氣看好 未來半年景氣持平 未來半年景氣看壞



ON SITE Nov. 29 Wed ... Dec. 2 Sat 2023 10:00 a.m. 5:00 p.m.
Tokyo Big Sight [East] 1-8 Halls [West] 3-4 Halls

ONLINE Nov. 22 Wed ... Dec. 15 Fri 2023



© UDAGAWA YASUHIRO 1998



資安西遊記— 製造業資安的取經之旅

文 工研院產科國際所 林威佐

明朝吳承恩所寫的西遊記，講述唐三藏帶著孫悟空、豬八戒與沙悟淨三個徒弟，前往西方國度天竺國取經的故事，沿路上所經過的王國/地域若有發生不尋常的事件，背後多有妖怪所致，一般解決方式通常是靠著三位徒弟的武功，但若遇到較為厲害的妖怪，往往需請人協助(如太上老君)，而且遇到聰明一點的妖怪，僅靠武功還不見得奏效，多半還要智取才能圓滿解決。

整個資安布署的人員組織，像極了整部西遊記的人物角色，精神領袖的師傅有如資安長及資安專責主管負責制定資安政策、武功高強的大師兄有如資安專責人員負責資安防護的規劃，採購資安設備與工具/服務、而多一事不如少一事的二師兄如同一般員工需符合資安措施，給予資安教育訓練、安分守己的小師弟如同IT資訊人員協助各項資安防護工作，而不尋常的事件如同資安事件，背後的妖怪如同駭客，需請人協助如同找資安協力廠商協助。

製造業該如何進行資安布署，本文以「面對它」、「接受它」與「處理它」進行描述，希望可以提供製造業廠商做為初步的參考。

面對它-正視製造業的資安威脅

依據統計台灣製造業最常發生的前三大資安威脅，分別是勒索軟體、惡意程式攻擊，以及網路釣魚攻擊。

勒索軟體是台灣製造業最常面對的資安威脅，通常是由具有組織性的駭客集團發起，先建立看似合法的網站，並將具有破壞性的勒索軟體偽裝成合法軟體，避開防毒軟體掃描應用程式後加以隔離，一旦經人員點擊網頁被安裝勒索軟體後，將對其電腦的文件系統進行加密，駭客在要求支付贖金後才解密

文件。甚者，在被勒索人員放任不管的話，其電腦上的勒索軟體會在企業網路內橫向移動到其他使用者的終端和伺服器系統，並對那些系統進行加密，進一步擴大勒索範圍。

其次是惡意程式攻擊，此類資安威脅的攻擊方式通常是利用贈送免費的USB，或是在某個特定對象企業中隨機發放多個受感染的USB。這種作法可以使得毫無戒心的員工在插入USB驅動器後啟動惡意程式，該惡意程式會立即修改使用者文件，或是刪除使用者電腦上的媒體文件。

第三大的資安威脅為網路釣魚攻擊，駭客最常利用受感染的電子郵件附件，竊取一般員工個人資料進行詐騙，另外還有更進階的魚叉式網路釣魚(Spear Phishing)，為針對目標企業中「特權人員」進行網路釣魚，鎖定高度敏感性資料，如智慧財產權及商業機密等，其攻擊的技巧包含假冒他人名義、使用迷人的誘餌、避開安全機制(如電子郵件過濾及防毒)等，只要目標族群中，有一個用戶打開附件時，受感染的郵件就會立即開始為目標電腦建立後門，以供未來進行更深入的攻擊使用。

接受它-掌握資安管理標準與政策

當部分營運風險來自資訊安全時，依據

資訊安全管理系統(Information Security Management System, ISMS)的定義，資訊安全所要確保的就是企業營運資訊的機密性(Confidentiality)、完整性(Integrity)與可用性(Availability)，三者說明如下：

(1)機密性：指資訊不得被未經授權之個人、實體或程序所取得或揭露，也就是需確保企業經營資訊能在對的人、對的時間、對的地點與對的裝置設備上被使用與存取。

(2)完整性：指對資訊的精確與完整安全的保證，換句話說為企業經營資訊在儲存、傳輸的過程中，在未經授權下不得被篡改。

(3)可用性：指授權實體在需要時可存取與使用資訊，簡單來說就是企業經營的相關資訊或系統需處於隨時可工作狀態，不能無故中斷。

國際上最成功的資訊安全標準首推ISO 27001，ISO 27001的名稱為「資訊科技 - 安全技術 - 資訊安全管理系統 - 要求(Information technology - Security techniques - Information security management systems - Requirements)為資訊安全管理系統(ISMS)的國際標準，此標準是由國際標準化組織(ISO)與國際電工委員會(IEC)聯合發布，因此也會被寫成ISO/IEC 27001，目前最新為2013年版本，內容列出有關資訊安全管理系統(ISMS)架構、實施、維護以及持續改善上的要求，目的是幫助組織可以使其保管的資訊資產更加安全。

而ISO 27002搭配ISO 27001提供最佳的實踐方式，ISO 27002名稱為「資訊科技 - 安全技術 - 資訊安全管理作業法規(Information technology - Security techniques - Code of practice for information security controls)」，包含具體的指引參考，目前最新為2022年版本，與先前版本(2013年)相比，新版的控制措

施數量從114項減少到93項，分布在章節A.5組織控制(Organization Controls)有37項、A.6人員控制(People Controls)有8項、A.7實體控制(Physical Controls)有14項與A.8技術控制(Technological Controls)有34項。

如表一所示，整體來說ISO 27XXX家族皆為資訊安全管理系統(ISMS)的國際標準，其中以ISO 27001作為資訊安全管理系統(ISMS)的共通標準，也針對次產業特性與相關應用發展出各自專用的標準，如ISO 27017為雲端服務資訊安全管理。

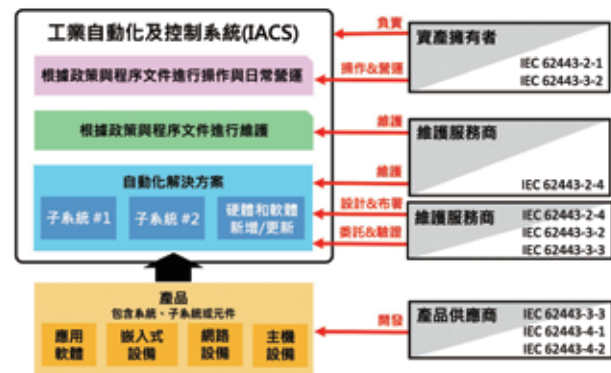
表一、資訊安全管理國際標準家族

資訊安全	
ISO 27001	資訊安全管理系統
ISO 27002	資訊安全管理操作準則
ISO 27011	電信組織的資訊安全管理
ISO 27017	雲端服務資訊安全管理
ISO 27034	應用程式安全開發管理
ISO 27799	健康與醫療產業資訊安全管理
ISO 20000	服務管理系統
ISO 20614	協作和保存資料檔案之數據交換協議管理
IEC 62443	工業自動化及控制系統資安標準

資料來源：工研院產科國際所整理

工業4.0、人工智慧AI、物聯網IoT、5G行動通訊等新興技術發展趨勢，帶動製造業數位升級與數位轉型的需求，相關的資通訊系統架構也朝向IT(Information Technology，資訊技術)與OT(Operational Technology，營運技術)的融合，如何在數位升級與數位轉型的過程中確保資訊安全將是每個企業主必須面對的課題，包含資通訊安全，網通安全(Cybersecurity)都需面面俱到，企業面對資訊安全，首先可參考ISO 27001所定義的資訊安全管理系統框架，但此標準框架是根據IT環境所制定的，並不全然適用於工業控制系統(Industrial Control System, ICS)的操作和程序控制的OT環境，尤其缺少OT環境下不同角色的觀點、實作以及應用。

因此，國際電工委員(IEC)以OT環境為主軸



資料來源：工研院產科國際所整理

圖1. IACS四大類角色功能與對應標準

發布的IEC 62443，IEC 62443名稱為「工業通信網路 - 網路和系統的IT安全性(Industrial communication networks - IT security for networks and systems)」成為目前國際上廣泛採納用於工業自動化及控制系統(Industrial Automation and Control System, IACS)的國際資安標準，此標準可達多邊認可效用，目前各國、各行業在制定OT環境下的資訊安全相關標準都會參考IEC 62443的內容。

IEC 62443主要有四個部分，第一部分為一般(General)作為標準的概論與介紹，定義工業自動化及控制系統(IACS)安全性的術語、概念及模型；第二部分為政策與程序(Policy & Procedure)說明工業自動化及控制系統(IACS)安全相關政策與程序之規劃，藉此確保系統、設備運作的安全；第三部分為系統(System)說明工業自動化及控制系統(IACS)的安全技術、風險評鑑、安全要求與等級；第四部份為元件(Component)定義與規範如何開發符合工業自動化及控制系統(IACS)相關安全產品要求及規格。

IEC 62443也將參與整個工業自動化及控制系統(IACS)的對象分為四大類角色，分別為資產擁有者(Asset Owner)、維護服務商(Service Provider)、系統整合商(System Integrator)與產品供應商(Product Supplier)，此四大類角色的功能與IEC



資料來源：工研院產科國際所整理

圖2. 上市上櫃公司資通安全管控指引三大構面資安規定

62443驗證標準的對應如圖1所示，並在第二部分政策與程序中，針對資產擁有者，也就是工廠的管理者，或是委外的維護服務商，說明應該如何透過管理政策和流程規劃以確保生產運作的安全性；在第三部分系統中，則是以系統整合商的角度，說明透過需求討論、規劃設計、連線部署後的自動化運作工廠，從技術面如何確保這些整合後的自動化方案免於資訊安全攻擊的威脅，探討內容包含執行安全評估等方式；在第四部份元件，則探討產品供應商的安全，說明如何確保導入自動化的設備機具之安全性，也就是定義與規範如何開發一個安全的產品。

而我國資訊安全相關政策，由政府近年積極推動「資安即國安」，為了因應駭客攻擊與資安事件影響政府機關與關鍵基礎設施運作，於2019年1月1日施行資通安全管理法，規範公務機關、關鍵基礎設施提供者、公營事業及政府捐助之財團法人，需強化資安防護能量與資安事件應變通報。

針對私部門部分，則透過臺灣證券交易所2021年12月23日所公布的「上市上櫃公司資通安全管控指引」，要求上市上櫃公司應配置適當資安人力資源及設備，進行資通安全制度之規劃、監控及執行資通安全管理作業。接著金管會根據2021年12月28日修正的「公開發行公司建立內部控制制度處理準

則」第9-1條，將上市上櫃公司依據收入規模分成三級，以循序漸進方式推動辦理私部門資安管控。

對製造業來說，或許部分廠商在臺灣證券交易所規範下，不需要強化企業資安防護能力，但在產業數位升級與數位轉型下，身處駭客猖獗的現在，營運過程中的資安風險與資安事件只會與日俱增，建議製造業廠商可依其產業特性、規模大小及資安風險適度採行，而採行的資安方案，則可以「上市上櫃公司資通安全管控指引」三大構面資安規定(政策&管理面、技術面、認知訓練與社交工程)作為資安部署的參考。

處理它-鏈結政府相關資源

製造業廠商若需要資訊安全相關的資訊，優先推薦可以到政府ACW網站找尋 (<https://www.acw.org.tw/>)，ACW全名為Art of Cyber War，該網站結合目前政府資訊安全推動資源，有任何找資安、做資安、學資安的需求都可以到此網頁瀏覽。

此外，政府也在台南沙崙設立了台灣首座集展示、演訓、實證功能合一的資安實戰基地，並命名為沙崙資安服務基地(ACW SOUTH)，該基地座落在台南沙崙智慧綠能科學城內，鄰近高鐵台南站，步行約10分鐘可到。

基地一樓設置有「沙崙資安應用多元展區 ACW SOUTH Exhibition Center」提供智慧製造、關鍵基礎設施(石化/化工、天然氣、變電所)、智慧綠能與新興主題等四大主題模擬產線與資安防護展示，難能可貴的是該展區也提供實際可執行的攻擊劇本，模擬資安攻擊情境，除了可供資安廠商進行產品驗測外，也歡迎領域廠商申請實測，確保選用的資安解決方案與企業自身的可適性。

另外，沙崙資安服務基地(ACW SOUTH)也



資料來源：ACW SOUTH計畫照片

圖3. 沙崙資安服務基地(ACW SOUTH)多元展區與產品驗測

舉辦多元的資安活動(如資安新秀大賽)，以及與資安相關的議題講座、主題式研討會、課程、交流會、焦點活動等，為企業進行資安人員育成與實務經驗奠基，強化產業資安人才的培育。同時也提供產業資安諮詢顧問服務(資安相談室)，串聯台灣資安專家於在地提供資安諮詢服務，另視廠商資安需求媒合資通訊業者、系統整合業者、資安業者，以提升廠商自身數位與資安防護能量，為製造業導入資安防護，提升競爭力，以因應物聯網時代國際供應鏈之挑戰。

製造業廠商如有資訊安全的需求，不妨親自走一趟沙崙資安服務基地(ACW SOUTH)，相關資訊如下：

數位產業署沙崙資安服務基地

電話：06-3032260

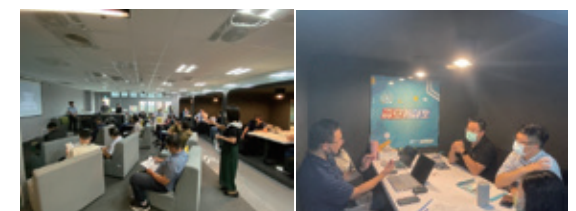
地址：臺南市歸仁區歸仁十三路一段6號

預約參訪：06-3032260 #145 吳小姐

(annawu@iii.org.tw)

產品驗測：06-3032260 #535張小姐

(changyunyun@iii.org.tw)



資料來源：ACW SOUTH計畫照片

圖4. 沙崙資安服務基地(ACW SOUTH)資安交流會與產業資安顧問諮詢服務

打造資通安全的台灣



文 國家實驗研究院科技政策研究與資訊中心 周媛韻 佐理研究員、王宣智 副研究員

科技文明的發展目的是為了降低人類生活所面對的不確定性與風險，但弔詭的是，為了解決問題所研發的新科技，常常又因為科技衍生出新的問題與風險。科技與風險雙生是人類文明發展史的一大特徵，也是文明發展的重要機制 (林崇熙, 2008)，其中資訊通科技與資安技術，就是科技與風險雙生的經典代表。

資通訊科技帶來了更高運算能力與系統整合的管控方法，讓製造業生產效率提升。即時性的資訊交換，讓金融與服務業有著更有效的營運效率。但是，資通訊科技帶來的資訊安全危機，也深深影響著世界上的人們，如資訊洩漏的造成的詐騙問題、勒索病毒造成的供應鏈和基礎建設危機、資訊偽造衍生的公衛危機、阻斷式攻擊的癱瘓事件和系統漏洞造成的商業影響等，其中美國司法部受到了Solarwinds Orion供應鏈攻擊的影響，其3%的員工信箱被入侵以竊取敏感數據，導致多達18,000名客戶遭受入侵。以下根據資安攻擊類別來進行2021年國外資安重大事件的整理（表1）：

近期國內因地緣政治因素，台灣政府機關、關鍵基礎設施(如油、水、電、交通、通訊及金融等)、各產業的指標企業都遭受到了中國國家級組織的駭客鎖定攻擊。2022年8月，美國國會眾議院議長裴洛西(Nancy Pelosi)訪台前，台灣總統府及外交部等部分政府機關網站受到了境外的「分散式阻斷服務攻擊」(Distributed Denial of Service, DDoS)攻擊(Digitimes, 2022)。根據「110年國家資通安全通報情勢報告」所接獲之政府機關資安事件通報顯示，2021年全國政府機關通報了696件資安事件，較2020年525件成長了約25%。其中通報類型為非法入侵的事件為最大宗，占了63.32%(110 年國家資通安全情勢報告, 2022)。

iThome電腦報周刊2022年調查指出，未來1年企業最可能發生的10大資安風險第一名是勒索軟體資安事件(46.6%)，其次為駭客攻擊(40.6%)，社交工程手段(38%)，為了避免面臨資安造成的企業損失和優化資安投資效益，建議企業應優先投入勒索軟體及駭客威脅的資安防護資源(iThome, 2022c)。從台灣上市櫃公司面臨的資安事來看(如表2所示)，勒索軟體及病毒攻擊事件為大宗且攻擊產業類型廣，國內半導體、電腦及周邊設備、電子零組件產業外，駭客還將魔爪伸入汽車工業、鋼鐵、建材營造、貿易百貨、生物科技等產業(iThome, 2022b)。另外，社交工程衍生造成的資安問題仍待改善，仍常常有企業因社交工程導致遭受企業內部系統受損或資料遺失等問題。

2021年台灣多家證券及期貨公司發生了下單系統被駭客入侵，導致客戶的帳號被盜用(iThome, 2022a)。雖然與其他產業相比，金融業資安表現尚佳(KPMG安侯建業聯合會計師事務所, 2022)，但還是有可能因為地緣政治等外在環境因素導致資安風險受到威脅。隨著全球金融系統與人類生活緊密相連，為了強化金融資安事件管理，金管會在2021年11月30日正式發布新版「公開發行公司年報應行記載事項準則」，針對所有上市、上櫃、興櫃及公開發行公司，要求其年報必須揭露資通安全事件的損失、影響及因應，藉由資訊公開、公司治理、監理協助角度著

手，來提升各產業對資安的重視(iThome, 2022d)。

台灣強化資訊安全的作法

資安即國安，隨著日益嚴峻的資安問題，再加上台灣各產業正面臨數位化及數位轉型，台灣試圖從國家的角度擬定了資安防護策略。台灣行政院於2001年成立「行政院國家資通安全會報」(簡稱資安會報)，並成立「技術服務中心」，以協助台灣政府機關強化資通安全防護的工作，具體的工作項包括了事前的安全防護、事中的預警和應變、事後的復原與鑑識。除了組織面外，同年台灣也開始推動「國家資通訊安全發展方案」，逐步完善台灣資安基礎建設工作。迄2022年止，台灣已經推動了六期國家資通訊發展方案，包含了機制的建立以及科技發展，其中第一、第二期屬於機制計畫，第三期到第六期為發展方案。目前為台灣第六期國家資通安全發展方案階段，該期方案的重點在基礎環境、聯防體系、產業發展和人才培育等四個面向資案的改善(圖1)。

此外，政府科技預算針對國內的資安進行切實的投資，投入的政策中還包含了技術研發、技術應用及人才培訓。其中，「資安產業發展行動計畫」主要在培育資安人才、聚焦台灣產業具利基市場的技術研發、建構產品試煉場域及國際拓銷。金融業的資安防護

表 1：2021 年國際重大資安事件

資安攻擊類別	事件描述
資訊洩漏	美國司法部受到了Solarwinds Orion供應鏈攻擊的影響，導致多達18,000名Solarwinds的客戶遭受入侵。Spotify遭受攻擊，導致100,000用戶帳戶的驗證資訊洩漏。
勒索病毒	勒索軟體攻擊並關閉了美國最大的精煉產品Colonial Pipeline的日常工作。 美國的肉類加工巨頭JBS遭受了勒索軟體的攻擊，迫使其暫時關閉在美國的所有牛肉工廠，並暫停在澳洲的牛肉及羊肉的屠宰工廠。 勒索病毒對託管服務供應商(MSPs)及其客戶進行了供應鏈攻擊，1,000家公司受影響。
阻斷式攻擊	Mirai殭屍網路以每秒請求次數高達1720萬次的請求次數，透過分散式阻斷服務攻擊(DDoS)的方式，試圖癱瘓金融產業的日常運作。
資訊偽造	偽造Covid-19的疫苗接種證書擴展到28個國家如奧地利、阿拉伯聯合大公國、巴西、英國及新加坡等的黑市。
系統漏洞	Microsoft Exchange Server發生了「零時差」安全漏洞，影響包含美國30,000家機構及英國7,000家伺服器。 Apache Logging模組Log4j漏洞，影響了Twitter、Amazon、Microsoft等科技巨頭的服務。

參考資料：Cyber Security Report 2022，Check Point Research

表 2：2021 國內重大資安事件

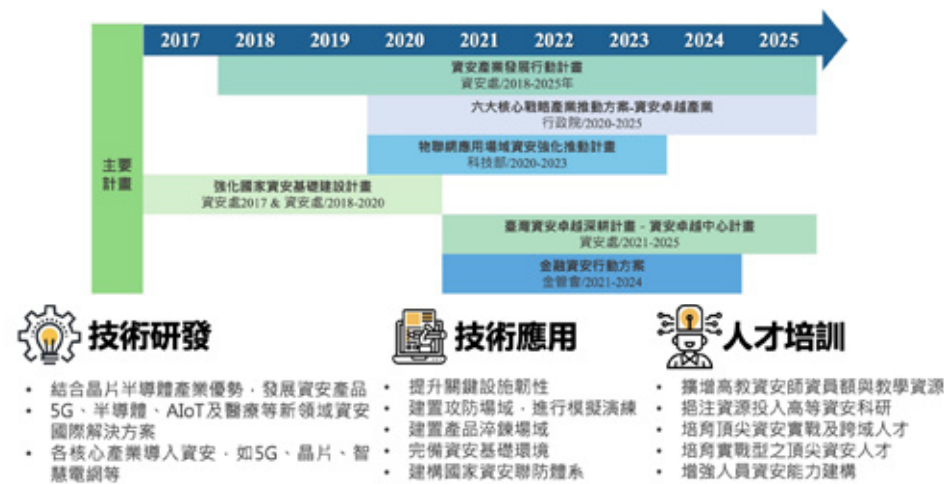
資安攻擊類別	日期	受資安威脅企業名單
勒索病毒	2021年3月	宏碁電腦
	2021年4月	Asteelflash Group及廣達電腦
	2021年5月	記憶體大廠威剛科技
	2021年8月	技嘉科技、關中旗下的外國子公司(Grand Home Holdings INC.)
	2021年10月	鋼鐵大廠中鴻鋼鐵、建材營造公司日勝生及其子公司
駭客攻擊	2021年10月	宏碁電腦印度售後服務系統
	2021年11月	日勝生公司旗下的興櫃公司京站實業、生技醫療業雙美生物科技公司
	2021年12月	東元電機與東元集團旗下東捷資訊部分
社交工程手段	2021年6月	電子零組件翔名科技
	2021年10月	車燈製造公司帝寶工業
	2021年11月	封測廠矽格公司

參考資料：iThome 國內上市櫃公司資安事件，2022

2001-2004	2005-2008	2009-2012	2013-2016	2017-2020	2021-2024
第一期發展方案	第二期發展方案	第三期發展方案	第四期發展方案	第五期發展方案	第六期發展方案
建構資安防護體系，完成政府機關分級機制	健全資安防護能力，成立國家資安監控中心	強化資安整體應變能力，精進通報應變機制	加強資安防護管理聯防監控機制與資安情報分享	推動資通安全管理法，完備國家資安聯防體系	建構主動防禦基礎網路，打造堅韌安全之智慧國家
願景：確保我國擁有安全、可信賴的資訊通訊環境	願景：持續強化我國整體資安防護基礎	願景：安全信賴的智慧臺灣，安心優質的數位生活	願景：建構安全資安環境，邁向優質網路社會	願景：將資安提升至國安防護層級	願景：打造堅韌安全之智慧國家

參考資料：數位發展部資通安全署資安政策與法規

圖1. 「國家資通訊安全發展方案」推動進程



參考資料：六大核心戰略產業推動方案，2020、資安產業發展行動計畫

圖2. 台灣資安主要計畫推動及屬性

則由2020年金管會推出的「金融資安行動方案」為主，透過四年分階段推動來強化主管機關資安監理、深化金融機構資安治理、精實金融機構資安作業韌性、發揮資安聯防功能，保障台灣金融運作的安全。其它的計畫項目則強調透過政策設立資安場域驗證專區，加強產官學研之資安技術的合作研發，如「物聯網應用場域資安強化推動計畫」之「發展先進製程資安攻防演練實測場域」項目，即以資安應用導向來為資安軟硬體技術及資安應用導向技術開發；或是強調國際交流合作並將技術移轉創新育成的「臺灣資安卓越深耕-資安卓越中心計畫」（圖2）。

行政院在2021年3月通過「數位發展部組織法」草案，並於同年年底獲得立法院三讀通過後，正式在8月27日正式掛牌成立「數位發展部」，透過新的組織結構來整合電信、通訊、資安、網路與傳播5大領域，規劃整體的數位發展政策，並統籌基礎建設、環境整備及資源運用業務，以達確保國家資通安全、促進數位經濟發展及提升國家數位轉型。為打造全民數位韌性，數位發展部下設了6司2署及1行政法人，其中的6司包含數位策略司，職掌為推動國家數位發展政策，統籌協調規劃施政計畫及資源；韌性建設司，職掌

為強化我國通傳網路之強韌性，維持數位應用暢通；資源管理司，職掌為前瞻分配管理數位通傳資源，確保資源使用符合公共利益；數位政府司，職掌為深化數位應用，提升政府施政效能；民族網絡司，職掌為參與國際數位民主網絡，增進我國對國際社會之貢獻；以及多元創新司，職掌為發展資料運用，打造資料創新應用生態。還設立了2署包含數位產業署，其職掌為辦理促進數位經濟相關產業發展與數位科技應用事項之政策規劃及執行及，以及資通安全署，其職掌為辦理國家資通安全政策規劃、計畫核議及督導考核，執行國家資通安全防護、演練及稽核業務及通傳基礎設施防護(如圖3所示)。

此外，數位發展部項下設定一個監督行政法人「國家資通安全研究院」，將納入現有的「行政院國家資通安全會報技術服務中心」以及正在籌備的「資安卓越中心(Cyber Security Center of Excellence (CCoE))」，以國家層級的觀點，挹注資安前瞻研究、培育頂尖資安實戰人才、創新育成資訊企業、建構實驗場域與促成國際合作。藉此增進台灣長期資安前瞻基礎研究的能量，並解決資安人力不足的問題，以長期培訓產業所需資安人才。數位發展部項下也主管了3個財團法



參考資料：數位發展部業務職掌

圖3. 數位發展部職掌

人，包含「資訊工業策進會」、「電信技術中心」及「臺灣網路資訊中心」。透過成立「數位發展部」，來扮演「國家數位發展領導者」的角色，專責整合「電信、資訊、資安、網路與傳播」五大領域，連結公民與技術，以加速促進國家數位轉型，推動國家數位政策的創新及變革(行政院院會議案, 2022)。

結論

根據經濟部中小企業處資料顯示，台灣中小企業比率最高，占總體企業的98.92%(經濟部中小企業處, 2022)，大部分企業的資安

意識與對資安管理機制的投入較少。除了金融業及科技業以外，大部分企業仍然缺乏資安意識。透過我國資安政策的概況盤點，我國正積極推動資安，並將其列為我國重點政策，同時擬訂技術研發、技術應用及人才培訓相關計畫的推動，還透過組改來設立專責整合「電信、資訊、資安、網路與傳播」五大領域業務的數位發展部。

我國於全球ICT產業供應鏈及工控電腦產品為出口優勢國，因此資訊相關人才培育的素質相較高，再加上5G、物聯網、AI及產業數位化創新等資安防護的需求日益提升，對台灣來說都是具有非常大的優勢。但礙於國內資安產業的規模較小以及產值較低可能面臨國際大廠強大的競爭威脅，且因政經情勢特殊，較常面臨國家級組織的駭客攻擊。因此建議聚集台灣各界的能量，藉由新部會的力量推動公私合作機制，來強化關鍵基礎設施及供應鏈的資安防護。另外，在新型態的資安威脅不斷變化的情況之下，資安國內法規比較難全面的考慮周全，全民的資安意識需要再提升才能防止資安攻擊。

參考資料：

- [1] 110 年國家資通安全情勢報告。(2022)。110 年國家資通安全情勢報告。
- [2] 經濟部中小企業處。(2022)。2022 年中小企業白皮書。https://book.moeasmea.gov.tw/book/doc_detail.jsp?pub_SerialNo=2022A01686&click=2022A01686
- [3] 林崇熙。(2008)。科技就是風險。科技大觀園。<https://scitechvista.nat.gov.tw/Article/C000003/detail?ID=19fe3170-36fa-4938-8b7f-5358e1a6ef58>
- [4] 行政院院會議案。(2022)。行政院全球資訊網。<https://www.ey.gov.tw/Page/448DE008087A1971/e03388cc-566c-4946-861b-2a1132c3c2cf>
- [5] Digitimes。(2022)。網路攻擊為地緣政治新變數 應納入營運風險考量。DIGITIMES 智慧應用。https://www.digitimes.com.tw/iot/article.asp?cat=&id=0000641588_J1G4W16B9PXZR2734VKAI
- [6] iThome。(2022a)。【資安日報】2022 年 2 月 22 日，臺灣

- 金融業遭中國駭客軟體供應鏈攻擊、安卓木馬 Xenomorph 鎖定 56 間歐洲銀行的用戶而來。iThome。<https://www.ithome.com.tw/news/149490>
- [7] iThome。(2022b)。2021 年國內上市櫃公司至少 14 件資安事件重大訊息，平均每月一起。iThome。<https://www.ithome.com.tw/news/149271>
- [8] iThome。(2022c)。【iThome 2022 資安大調查（下）資安風險】用資安風險圖分辨風險，資安布局先聚焦勒索軟體和駭客威脅（分析版）。iThome。<https://www.ithome.com.tw/article/153106>
- [9] iThome。(2022d)。【臺灣資安大會直擊】上市櫃企業年報資安揭露現況大公開，115 家中有 113 揭露資安管理架構，有 14 家如實說明重大資安事件。iThome。<https://www.ithome.com.tw/news/153488>
- [10] KPMG 安侯建業聯合會計師事務所。(2022)。2022 臺灣企業資安風險大調查。<https://assets.kpmg/content/dam/kpmg/tw/pdf/2022/09/2022-taiwan-cyber-risk-report.pdf>

智慧製造的IoT安全防護

文 緯謙科技股份有限公司 葉卯陽 副總經理

工業 4.0 時代來臨，加上中美貿易戰持續發燒，帶動台灣製造業更積極地朝向數位化、自動化、智慧化的方向轉型發展。製造業不僅面對同業的競爭，還需要考量氣候變遷、ESG、碳交易、循環經濟等議題帶來的挑戰。對應這些挑戰，數位轉型是製造業的最佳策略，智慧製造則為製造業創造對應挑戰的優勢。

智慧製造，從機械化、自動化、數位化發展到现在的智慧化，需要軟硬結合，所需導入之技術也不盡相同，所涵蓋範圍包含產品智慧化、設備智慧化、生產方式智慧化、管理智慧化及服務智慧化等生產製造各階段。

有人比喻「網路時代，資料就是石油」。數位轉型與智慧製造都是奠基在大量的數據，可以說「智慧製造時代，資料就是石油」。既然「資料就是石油」，那麼取得並確保資料安全，就成為數位轉型與智慧製造的成功關鍵。

相較於IT資安，製造業較常忽略IoT/ICS(Industrial control systems)的資安議題。IT資安重視的是資料保護，包含資料中心(電腦機房)與網路安全、端點與使用者安全、雲端服務安全等。資安領導廠商甚至提供資料庫安全解決方案。而OT資安重視的是作業流程的保障，保護IoT設備/裝置與相關網路安全，以及設備內建的安全防護。

傳統的OT設備很少和企業其他系統介接，也不會連結到Internet與Cloud。但是，為了實現智慧製造，OT設備就需要與IT網路連結，並與其他系統介接。在連結與介接之前，通常需要確認以下幾個部分是否已經有防護的解決方案：

1. OT設備到OT系統之間的網路安全；
2. OT系統連結IT網路所經過的交換器、路由器、閘道器等設備；
3. 如果連接到Cloud，須採用加密的通訊、VPN，或私有網路；
4. OT裝置間須採取加密的安全通訊協定(如Modbus, MQTT)；

除了上述幾項，還需要訂定操作人員的標準作業原則，以確保資料安全，如封鎖未使用的服務、管理USB裝置與傳輸埠的使用，以及建立許可使用的應用軟體清單。

一般而言，OT/IoT裝置/設備普遍有下列的安全風險，因此容易遭受針對裝置本身攻擊(例如，遠端操控、系統中斷、殭屍網路、挖礦攻擊等)，以及網路入侵與後門(例如，橫向感染至其他內部網路)的資安漏洞：

- 1) 使用初始密碼或使用公用密碼；
- 2) 裝置/設備無內建安全設計；
- 3) 作業系統老舊；(例如，Windows XP/7)
- 4) 升級不易，或廠商已經不提供升級。

另外，IoT/ICS環境複雜度遠高於一般IT網路，更需要資安管理者留心注意：

1. 多重裝置與多供應商；
2. 複雜的通訊協定與使用行為；
3. 隱藏/無法識別的安全風險；

根據Check Point 2022年中資安調查與趨勢分析報告資料顯示，各產業被攻擊增幅集中在40%~60%之間，製造業受攻擊數亦快速增，增幅達到42%。在同一份報告中亦指出，資安威脅趨勢為釣魚攻擊/勒索軟體、供應鏈攻擊與IoT威脅、新興應用帶來的攻擊型態。

要如何實施IoT聯網資安方案，以下是前述資安大廠的幾點建議：

1. 強化IoT設備的可視性：發現與識別IoT裝置。
2. 掌握IoT設備的使用狀況與實際運行數據：蒐集網路IoT流量，以及設備的詳細資訊，如設備類型、供應商、軟體版本、網路連結類型等。識別並分析風險，如弱密碼、韌體過時，以及已知的漏洞。

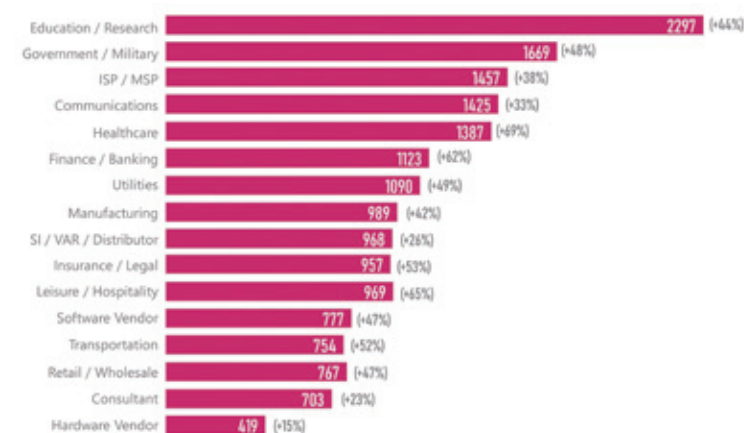


Figure 12: Average weekly attacks per organization by Industry H1 2022 compared to 2021.

(Ref. cyber-attack-trends-report-mid-year-2022, Check Point)

3. 確實執行IoT安全政策：標準作業流程、權限管理、密碼管控、操作紀錄。
4. 偵測異常行為：採用有效的資安軟體，偵測異常行為後採取對應的防護措施。

針對IoT設備更新不易的問題，已經有廠商開發出「虛擬補丁」的解決方案，來防護已知安全漏洞，目前已經可以保護超過50家廠商的設備，提供10,000+ 預設特徵碼與自訂安全特徵，並且可以即時在雲端更新，以提供更高效的保護效益。針對設備的安全防護，國內資安大廠還推出USB Dongle大小的防毒工具，在不需聯網的情況下，毋須安裝軟體，就可以偵測並移除惡意軟體。

OT設備聯網已然成為趨勢，製造業勢必提升OT的安全防護，並且與IT的安全防護整合成一個全方位的網路安全防護網。特別是製造業的OT/IoT設備面臨前述的複雜環境與升級問題，在規劃導入智慧製造的同時，更需要全面的通盤考量，挑選合適的IoT安全防護解決方案與佈署對策，才能應對智慧製造轉型過程中的挑戰，順勢扎穩永續經營基石。

智慧工廠資安 導入實戰經驗談



文 泓格科技股份有限公司 趙英傑 研發處長

隨著資訊通訊技術 (Information and Communication Technology, ICT) 以及物聯網 (IoT) 技術愈趨成熟，各製造業者期望透過智慧自動化的生產方式提高生產效率，因此 ICS 由過往的封閉環境逐漸轉為與公司內部網路甚至網際網路連結。從資訊安全的面向來看，傳統 ICS 所依賴的封閉性正逐漸的消失，以致面臨各種潛在的入侵威脅。

加上近年來許多工廠興起工業 4.0 的建置，已導入原有工控 (IACS、DCS、SCADA) 等元件構成的 OT (Operation Technology) 環境，興起智慧製造及關鍵基礎設施的智慧連網，也造就各工廠往智慧製造的趨勢前進。但 2018 年某半導體製造公司全台各廠因 WannaCry 病毒弱點未修補，造成生產線大當機超過數十小時，損失高達數十億台幣，震撼國際製造業及資安產業，也燃起製造業長期漠視的資安意識，管理階層及利害關係人紛紛關切資安對工控物聯網議題。然而工控物聯網的資產擁有者雖然都知道資安的重要性，但卻不知如何進行對工控物聯網的風險分析及如何發展一個可持續改善資安防護水準的資安計畫，更談不上與利害關係人如何進行風險溝通，另一方面 IT 的資服業者、工控元件的供應商，亦無法提出全面完整的工控物聯網安全解決方案。

然而工業控制系統 (Industrial Control System, ICS)，由不同的工業設備、控制器以及軟體組成，負責即時接收來自工業機器的數據，監控系統狀態並管理自動控制的機制。其涵蓋的系統或裝置包括數據採集與監控系統 (Supervisory Control And Data Acquisition, SCADA)、分散式控制系統 (Distributed Control System, DCS)、可程式邏輯控制器 (Programmable Logic Controller, PLC) 等。ICS 已廣泛應用於天然氣、電網、水利、交通、通訊、工業製造等關鍵基礎設施中。但各工業基礎設施之生產控制網路 (Operation Technology, OT) 完全未導入資安解決方案，最基本之要求為不影響改變現有設備與網路架構為原則，不允許在各設備主機進行侵入式安裝 agents 之資安解決方案，因此，迫切需要非侵入式之資安偵防解決方案。

智慧工廠的安全性考量需對 IT 與 OT 的分別進行資安強化的建置，可針對既有資安弱點來強化安全性，同時可以機器學習的基礎來進行工業物聯網有關工業協定異常偵測的資安偵測技術與方案，可在既有智慧工廠聯網的基礎下，導入產線及其他系統的資安風險管控可

視化技術，打造智慧工廠設備資料安全傳輸環境以提升工廠設備的穩定性，藉由工業物聯網安全異常偵測的開發也提高產線穩定性與提升品質。

綜合因應未來智慧工廠資訊安全挑戰與對策整理如下：

需求	相關對策
缺乏工業 4.0 基礎的工業物聯網有效方案，佈建成本高	提升不同工控聯網的技術以提供不同方案的工業物聯網解決方案，例如：非侵入式聯網方案
缺少在既有設備聯網的安全強化性產品，成本高及功能不符合	現有工控網路異常偵測產品僅針對特定協議作協議分析，缺乏自動化功能。
IT 與 OT 的監控產品皆為獨立分開系統，缺乏有效的 IT 與 OT 整合性系統	提供 Total solution 及整合性介面，讓 IT 與 OT 系統能夠整合，提高營運效率與降低成本
缺乏有能力整合 IT 與 OT 的系統廠商，協助工廠升級。	提升 IT 與 OT 人員的能力，並能夠整協同合作，尤其 OT 人員需懂得不同工控網路協議。
缺乏兼顧安全的智慧工廠示範場域	以國際安全規範的制度，(如 IEC-62443 安全規範) 應用於工廠

智慧工廠資安導入實戰

泓格科技成立將近 30 年來一直注重開發各種自動化領域的解決方案，各項產品廣泛的應用在國內外工控與自動化領域中；國內半導體、LCD 面板、石化等龍頭產業應用在廠務監控與自動化系統，而近年也發展工業物聯網安全偵測相關技術，並以自身智慧工廠場域的資安建置提供給讀者，藉此提供可實現的具體安全性智慧工廠參考指南。

由於泓格公司之生產場域具備機聯網智慧製造基礎，場域中已導入先進自動化生產設備，場域中同時也有傳統工業控制系統技術存在，此為大多數國內製造場域常見現象，提供以下三個步驟來實現智慧工廠的資安佈署。

- 首先透過第三方資安團隊協助識別現有產

線工業控制系統及資安防護設備之潛在弱點與威脅、導入 IEC 62443 資安標準對產線系統分析不足之資安控制項，並協助提出資安改善事項也建立泓格公司「專責資安團隊制度及架構」。

- 基於上述檢視結果，由泓格科技針對產線工控與環控設備安全，發展「工控網路威脅智慧偵測系統」及「工控網路安全威脅模擬系統」，以建立 / 強化工控網路於端點、網路架構、邊界與資料傳輸鏈路之資安防衛。

- 建置資訊安全可視化技術整合，進行「智慧工廠整合安全平台開發」、「資安通報與情資分享」與「智慧製造資安示範場域佈建」，藉此強化產線資安防護能力。

執行步驟示意圖如下，以下分為 A,B,C 三項說明：

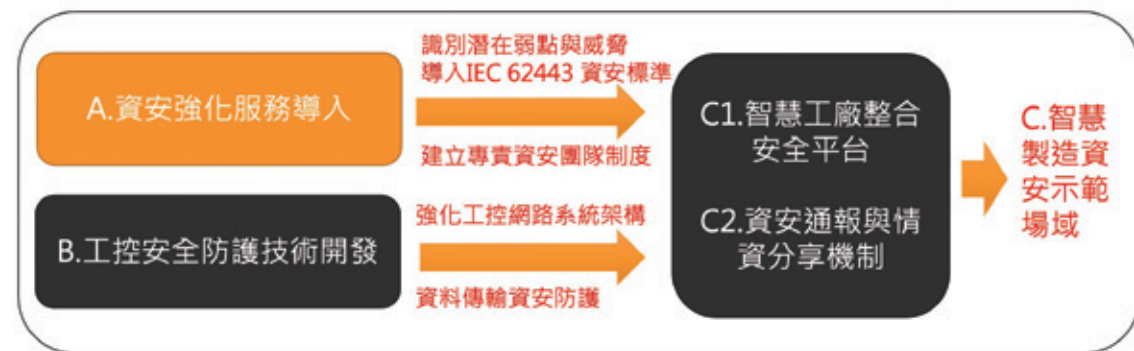


圖1. 智慧工廠資安導入流程

整體智慧工廠資安架構圖如下：

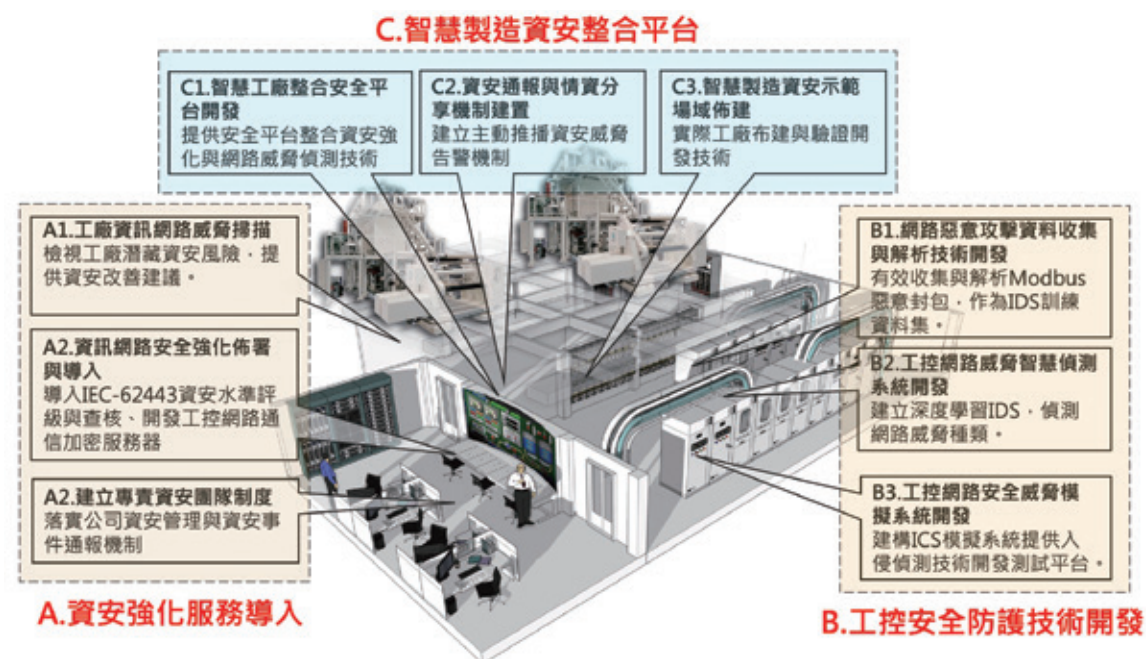


圖2. 智慧工廠智慧安全架構情境

A. 資安強化服務導入

包含項目如下：

1. 工廠資訊網路威脅掃描

• 工廠資訊網路威脅掃描：針對工廠 IT 環境執行網路、系統及終端三種資安風險檢測，

並提供資安改善建議。

• 產線資訊網路威脅掃描：提供工控場域可視化、產線系統與網路安全及生產設備資安強化項目，針對網域中的資產、網路及整體架構，進行檢測與分析。

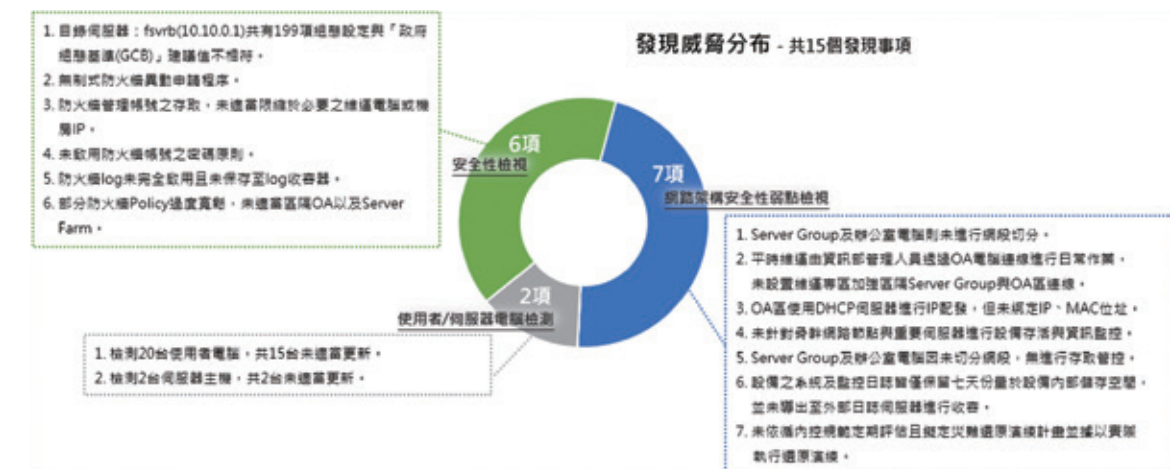


圖3. 資訊網路威脅掃描結果

2. 資訊網路安全強化部署與導入

• IEC 62443-3-3 產線系統資安水準評級與控制項部署（七大工控系統安全要求與 51 個資安基本控制項）

• 場域資安水準查核（符合性驗證）：透過

中華資安國際與泓格科技共同派員進行內部 IEC 62443-3-3 查核。

• 工控網路通信加密服務器：將上層 Modbus 協定轉換成具高度安全性之 OPC UA 協定。



圖4. 風險評估報告

3. 建立專責資安團隊制度

• 建立專責資安團隊制度與相關文件產製。
• 資安事件通報應變制度演練。

B. 工控安全防護技術開發分項

本項設計在 ICS 部署蜜罐以誘捕駭客攻擊封包，並部署 IDS 以對正常或異常封包做分

類判斷與發出警示訊息。包含：

- 1. 網路惡意攻擊資料收集與解析技術
 - 建置 Modbus 實體蜜罐，有效引誘駭客攻擊。
 - 自動收集惡意攻擊封包的程序，將其存入惡意攻擊資料庫。
 - 解析惡意封包，取得 10 種特徵屬性。
- 2. 工控網路威脅智慧偵測系統開發
 - 建立深度學習集成式 LSTM 分類器模型，以區分正常封包與異常的攻擊封包。
 - (訓練階段) 採用 Bagging 方法，具多個分類器可提高分類精度與降低模型的不穩定性。
 - (測試階段) 分類器採多數決方式輸出預測結果 (7 種分類 (含正常)，正確率 90% 以上)。

3. 工控網路安全威脅模擬系統

- 模擬工廠裝配程序與 Modbus TCP 網路通訊，做為測試工控網路威脅智慧偵測系統功能。

C. 智慧製造資安整合平台

1. 智慧工廠整合安全平台

- 建立可視化介面，整合上述 A、B 分項功能，提供產線人員進行資安維護作業。
- 當 IDS 偵測出入侵威脅時，安全平台會即時提出告警並顯示資安威脅事件型態，主動推播警報訊息；並提供歷史警報功能。

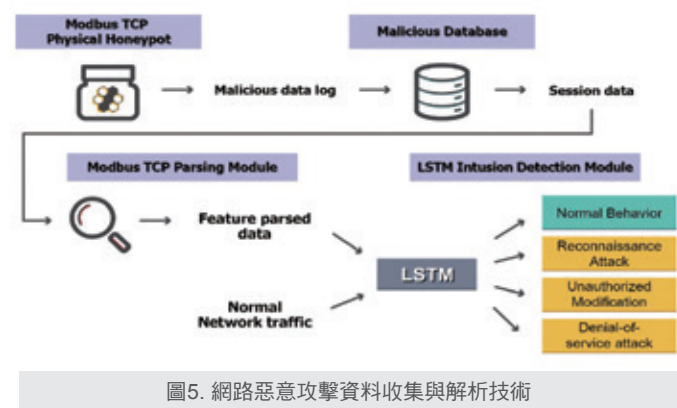


圖5. 網路惡意攻擊資料收集與解析技術

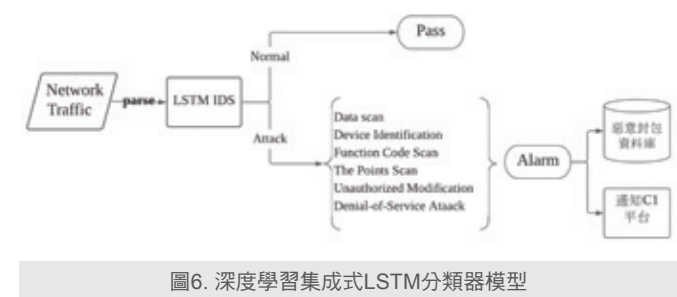


圖6. 深度學習集成式LSTM分類器模型

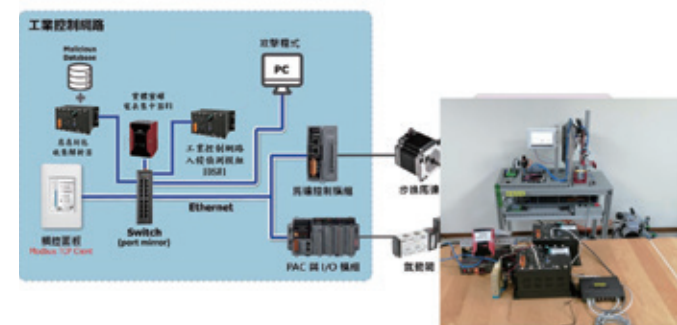


圖7. 工控網路安全威脅模擬系統

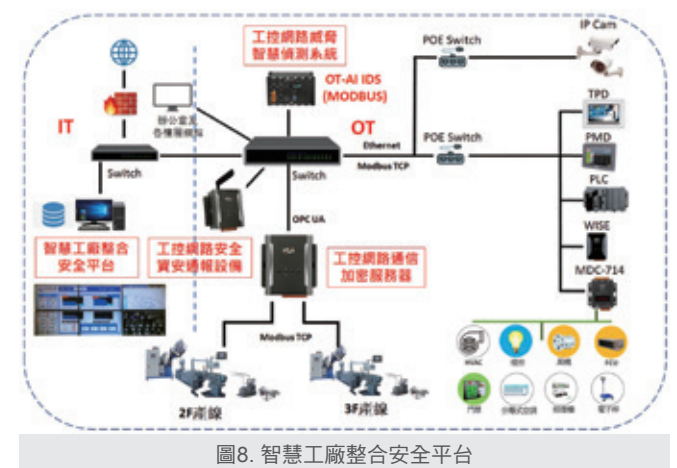


圖8. 智慧工廠整合安全平台

2. 資安通報與情資分享機制建置

- 資安事件通報至 TWCERT/CC 網頁進行人工資料登錄。
- 工控網路安全資安通報設備：協同智慧工

廠整合安全平台提供主動告警：

- (1) 手機簡訊告警
- (2) Email 告警
- (3) 即時通訊軟體主動推播警報。

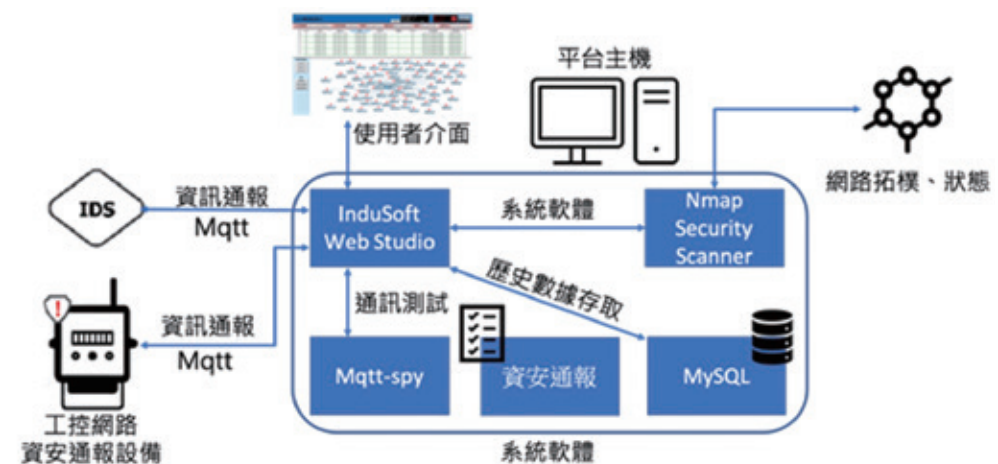


圖9. 資安通報與情資分享機制



圖10. 工控網路安全資安通報結果

經由上述資安項目實施前後，所產生效益如下表：

建置項目	導入前	導入後
資安強化服務導入	本公司既有 MIS 部門做資安管控	導入標準 IEC 62443 資訊安全制度 建立資安專責團隊
	網路區段無區隔	網路區段分割
	產線資料無加密	產線及工廠環控系統之傳輸資料加密
工控安全防護技術開發	工控網路無異常封包偵測方案	開發與導入具 AI 分析方法之工業網路偵測系統
	產線聯網設備無擴充及安全資料傳輸	導入具彈性工業網路安全偵測系統，可更新安全偵測方法
智慧製造資安整合服務平台開發	無整合型 IT 與 OT 資訊安全可視化介面與警示系統	建立智慧工廠整合型監控系統與資訊安全整合系統 提供部署資安強化成果展示平台

結論

智慧工廠除一般 IT 資安應用已有相應成熟產品可用外，也須對工業控制系統的資安防護做更深層考慮，其攸關產線運作外，更牽連到健康、安全以及環境三個層面的影響。過去工業系統維護專注於設備之功能安全 (Functional safety)，然而，事實上資訊安全的含蓋範圍更廣，且與設備功能安全緊密相關，意味著工業控制系統受到資安危害，其範圍不僅是單一設備或 SCADA 系統，而是可能造成人身安全的傷亡，因此，為協助強化國內工業控制系統之資安架構及避免此類憾事發生，本團隊積極規劃參與此案，具體服務內容如第三章實施方法。

泓格公司了解邊界防護於智慧製造場域之重要性，期望透過此智慧工廠資安的部署，可以協助讀者導入 IEC 62443 標準資安制度，

建立專責資安團隊，針對產線也可參考工控網路威脅智慧偵測的導入來強化產線網路防護；並以可視化 IT 與 OT 資訊安全整合介面與示警系統，部署於實際產線作為技術驗證與提供資安強化之展示場域，藉以最大化提升產線資安水準。透過此案強化生產場域資安水準，以國際信賴安全製造供應鏈為目標，建置智慧工廠資安場域，藉此可強化智慧工廠自我產線資安防護能力。未來隨著智慧製造、物聯網的趨勢發展，將會有越來越多聯網的生產設備暴露在網路威脅當中，國際標準組織 ISO 今年已經發佈物聯網設備資訊安全檢測規範 ISO 27400，已經為未來的設備的資安標準指出方向，泓格科技將秉持提供客戶高品質服務的精神也積極研發所需要的軟硬體技術。

Smart Industry, Smart Life!

ROBOT WORLD 2023

R O B O T W O R L D .

OCT 11(Wed) ~ 14(Sat), 2023, KINTEX, Hall 1~3



淺談智慧製造的資安防患與因應

文 TXOne Networks 鍾銘輝 市場研究團隊

一、智慧製造面臨的資安風險

當今智慧工廠的製程逐漸走向高度數位化，其透過機連網使產線和周邊環境的資料被收集以作為營運管理優化的基礎，並使得工廠管理者對內部和周圍可能發生的任何變化能更自主、更靈活地回應。傳統上營運系統防禦最常見的是依賴實體隔離，但基於實體隔離的安全假設可能導致防禦部署的誤判，事實上許多工控環境並未完全隔離，仍有機會被遠端入侵，甚至使得工控資產變成內部其他系統的攻擊起點，主要原因有三：

(1) 原始設備缺乏安全考量：傳統的工控資產由於原始設計目的在實現最佳的可用性和實體安全性，而非抵禦網路攻擊。加上資產生命週期長而導致系統老舊，這些系統通常缺乏最新的系統安全更新。例如：產線設備為了保持機器的性能穩定，而持續使用已停止安全更新的作業系統(Windows 7)，使得資產面臨的攻擊風險也日益增加。

(2) 擴大駭客攻擊表面：較新的工控資產為了能夠方便管理，於是整合Internet和IT網路，以促進遠端控制和操作，從而擴大了網路攻擊面。例如：在COVID-19期間增加遠端

控制的採用，同時也增加識別、驗證和保護帳戶的風險[1]。

(3) 針對工控的威脅和弱點不斷增加：駭客可運用一系列工具攻擊常用的工業通訊協定，如：FINS、Modbus和OPC UA破解或控制多種ICS/SCADA設備。從Stuxnet、LogicLocker、DoppelPaymer，一直到近期被公開的Industroyer2和PIPEDREAM [2] 足以顯示攻擊武器變得更為細緻。加上工控系統是製造業和關鍵基礎設施創造價值和營收的核心，如果它們出現故障產線就會被迫停止，使得工控系統更容易成為攻擊目標。

二、智慧製造常見的攻擊情境

惡意行為者可分為兩種，其一是出於經濟利益的網路犯罪團體(例如：資料勒索、勒索軟體);其二是以實現政治利益的國家型APT組織(例如：竊取國家機密、破壞社會關鍵基礎設施)。聰明的駭客總會因應時局挑選高經濟價值攻擊目標，並進行偵查、開發技術或工具，取得關鍵系統的初始存取權限，最後執行攻擊達成預期效果。有鑑於此，企業必須理解網路犯罪組織針對工廠的攻擊情境法，以識別潛在威脅：

(一) 情境一：存取控制權限洩漏

透過利用社交工程，內部人員或供應商疏失，導致駭客獲得內網立足點，駭客有機會利用特權升級，並橫向移動而不被發現，直到駭客找到關鍵的工控系統。例如：DoppelPaymer會透過魚叉式網路釣魚進行網路滲透，以誘騙攻擊目標執行偽裝成合法文件的惡意程式。此程式負責將其他具有更高級功能的惡意軟體（例如：Emotet）下載到受害者的系統中，執行進一步執行各種活動，例如：竊取憑證、內部橫移，以及執行不同的指令[3]。

(二) 情境二：利用軟體漏洞

通常利用“軟體漏洞”來破壞、禁用或破壞供應鏈系統、流程或操作。駭客現在可以透過Shodan、Censys等弱點搜尋工具，公開尋找存在弱點的PLC或RTU。當PLC或RTU中的具有遠端存取功能時，攻擊者可以發送停止指令來擾亂PLC的正常運行，或是對目標設備植入惡意程式，以發起各種攻擊，例如：LogicLocker [4]。

(三) 情境三：軟體供應鏈攻擊

當駭客滲透到設備供應商的網路，並在供應商的產品交付給客戶之前，使用惡意程式破壞感染設備就會屬於軟體供應鏈攻擊。通常受感染的軟體會破壞客戶的資料或系統。這種攻擊的特點是駭客在軟體編譯之前就滲透到供應商的軟體開發過程中。供應商的產品成為帶有惡意程式的軟體，這使得惡意軟體更難被發現。例如：國家資助的駭客組織修改了SolarWinds 的 Orion 網路管理軟體程式，在自動軟體安全更新中植入「Sunburst」的後門程式，從而使駭客取得目標企業網路的完整存取權限，此事件影響全球18,000名客戶。

三、建立OT零信任防護的四個方法：

採用OT零信任架構促使網路防禦永遠不預設可信度，而且會不斷在進行信任評估，並透過自動化方法實現OT零信任，以確保生產力為最高優先順位。建議工廠管理者可運用四個方法來實踐OT零信任資安架構：

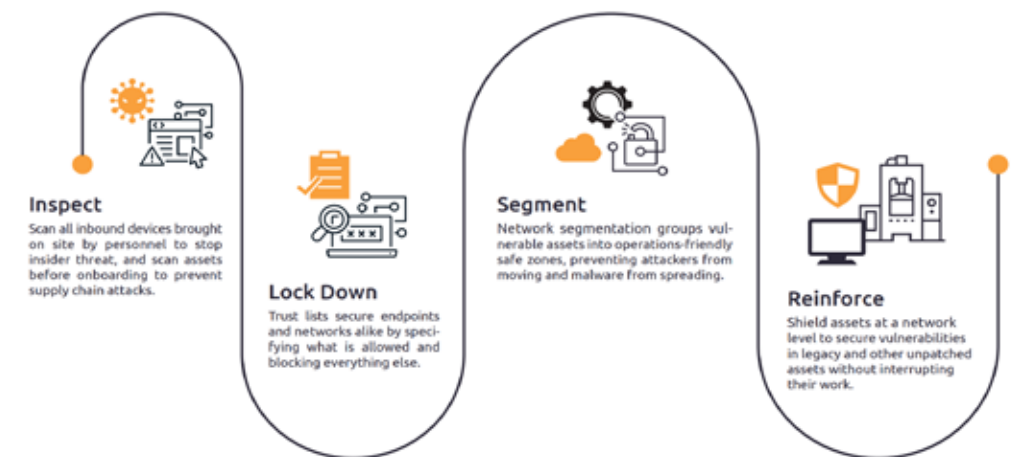


圖1. OT零信任的四個方法

(一)Inspect :

OT零信任的第一個關鍵是「永不信任，持續驗證」，因此對資產執行安全檢查是重要的第一步，這意味著對進入工作現場的每台設備必須實施惡意程式和安全狀態掃描。不論是從內部員工或可信任供應商帶來的資產都可能將威脅帶入OT環境。惡意程式可能隱藏在準備部署的資產中（供應鏈攻擊），以及人員帶入生產線的設備中（內部威脅）。建議組織可以設置一個檢查流程，該檢查流程能夠快速執行和記錄所有進入設施的資產中是否挾帶惡意程式或存在高風險弱點。

1.從設備入廠即執行威脅管理：由於惡意程式無時無刻都在演進，掃描工具也須回應新威脅而不斷地更新，並確保設備的掃描報告是有效的，故掃描報告必須在內容中詳實記錄，包含：

- 掃描軟體名稱：確保掃描工具為值得信賴品牌
- 掃描引擎版本：確保掃描引擎和病毒資料庫是最新版本
- 受測設備版本：確認受測設備的基本資訊
- 掃描引擎設定：將掃描引擎設定為掃描所有檔案類型和系統儲存空間
- 掃描範圍：確保掃描引擎會檢查機台設備內的每個運算裝置與其儲存空間
- 執行時間和日期：記錄掃描開始與完成的時間，並確保掃描時有使用最新的病毒碼
- 掃描結果：清楚記錄掃描狀態和通知，包含：未偵測到、已清除，或已隔離惡意程式等

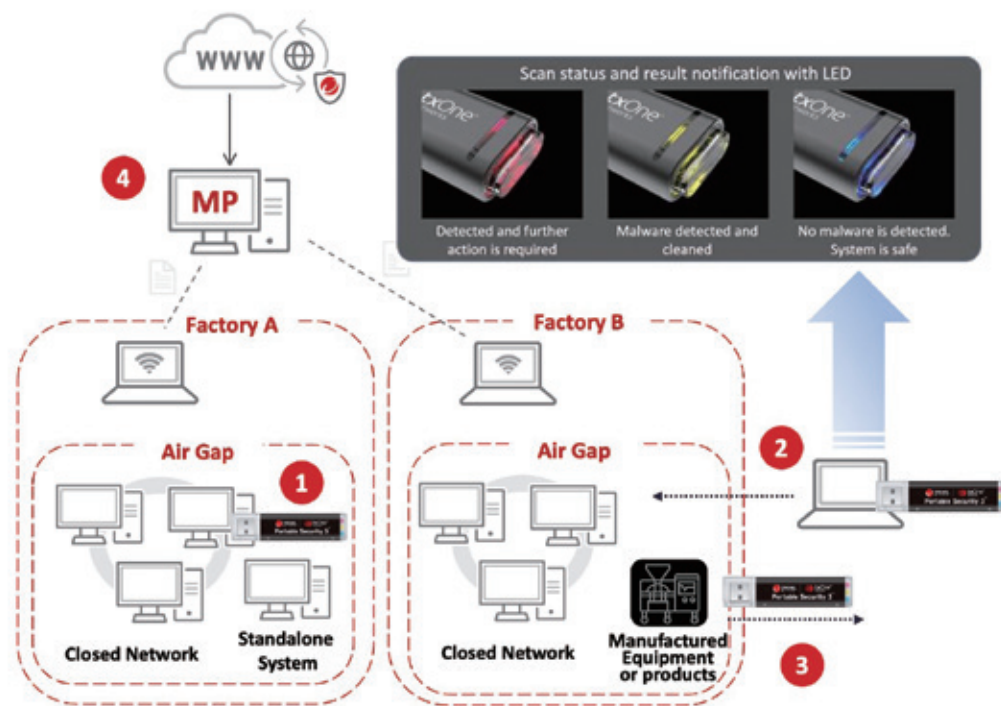


圖2. 使用可攜式掃毒工具檢查供應鏈設備

2.系統安全狀態檢查：現代的作業系統功能和服務並非專為工廠營運所設計，許多功能可能已經超出基本營運所需，為了做到自動化檢查設備的軟體弱點和組態配置，美國NIST推出的安全協定標準，以便於供需雙方可以依據自動化安全系統組態清單進行評估，自動地驗證清單上設置是否屬於「安全狀態」。如果資產擁有者無法自行定義安全掃描內容，也可以仰賴公開的資訊，如：NIST所維護的National Checklist Program (NCP)裡面有美國政府公開可用的安全檢查表（或基準）資料庫可供產業使用[5]。因此組織必須仔細檢查運算設備是否配置為「安全狀態」，並避免引入高風險漏洞。例如：檢查作業系統的版本、啟用的服務和Port、Windows Update List，以及安裝的應用程式清單等，讓組織了解運算設備系統配置是否安全。

(二) Lockdown :

資產強固是消除攻擊手段的關鍵階段，這包括網路服務強固，以及修補系統漏洞和關閉非必要服務，例如：應用程式、使用者權限、使用帳戶、網路服務、網路埠和其他不需要的系統功能。透過強固資產方法能夠

延長資產使用壽命，保護已經老舊的資產，讓技術人員可最大程度地減少攻擊者存取執行關鍵任務電腦，並阻止惡意程式運行的機會。

1.核心資產部署工控防毒軟體：在產線設備上部署防毒軟體最大的挑戰在於不影響生產前提下發現異常活動，並保護關鍵資產。組織可以運用能夠使用有效的方法（例如：OT/ICS軟體數位簽章、checksums和憑證資料）以驗證軟體是否來自可信來源。

2. 實施最小權限控制：產線設備必須要能夠智慧化識別關鍵任務流程，從而將生產相關的應用程式給予其工作所需的優先順序，並執行營運行為異常偵測，例如：透過學習、偵測和授權日常操作行為，並在最小權限控制下監控易受攻擊的合法流程，可確保必要任務的快速操作和資源可用性。

3.禁用多餘、未授權的服務和軟體：組織可以使用應用程式信任列表來鎖定資產上的應用程式、組態配置、資料和USB埠。這有助於阻止未經授權的應用程式執行，並且只有受信任的使用者和應用程式才能更改組態配置或資料。

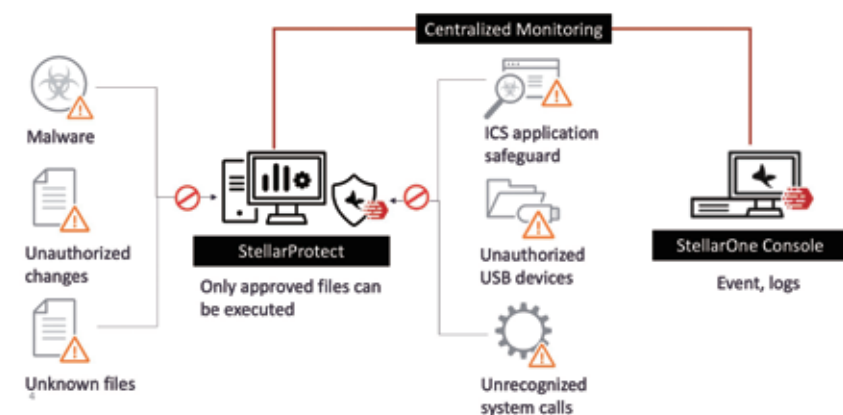


圖3. 使用端點防護解決方案強固系統

(三) Segment :

工廠的管理者必須準備好抵禦駭客渴望利用網路散播的各種威脅。網路隔離的重點在於可以根據資產屬性定義需要或不需要通訊，將組織的OT網路分割為更容易防禦的區域。例如：基於可信任的工控通訊協定來定義可執行的指令，或者基於特定IP的策略來確定哪些資產可以相互通訊。這讓工廠網路得以強化網路存取控制，運用更好的封包分析，並使駭客在工廠網路中收集資訊或移動變得更加困難。工廠管理者可以透過下世代IPS 和防火牆設備以下列方法達成動態網路隔離：

- 僅允許合法必要網路服務通過
- 僅允許合法、安全或具使用者授權之檔案分享通過
- 防止未授權之外部網路存取行為
- 防止未授權裝置連接工廠網路
- 合宜之內網微分割、隔離產線，以及將產線相關的服務主機移至安全網段
- 支援深度網路封包檢測技術，搭配最新工控威脅情資，以便於阻止威脅入侵
- 支援資產風險評估，包含：詳細的弱點情資、攻擊向量報表

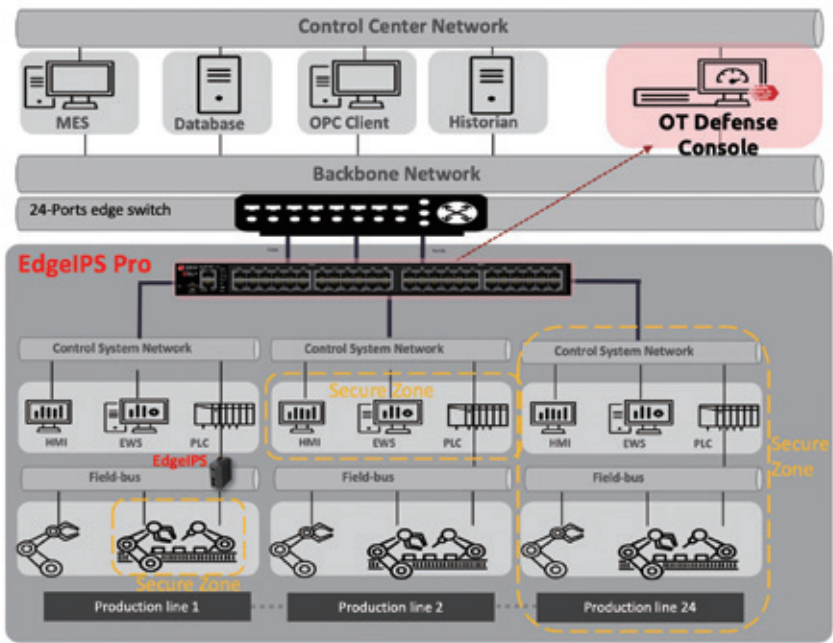


圖4. OT 原生IPS和防火牆實現高效率內部威脅偵測

(四) Reinforce :

產線現場的維護是惡意程式進入實體隔離環境的途徑之一，現場技術工程師常會從事替換生產設備內的運算裝置、儲存裝置或更

新軟體，這些活動都必須確保在無惡意程式的前提下才能夠安裝。

- 1.維護作業的威脅管理：設備在執行每次軟體或配置發生更改時，都需要進行另一次

掃描。但在工廠的產線環境下，有嚴苛的環境限制，例如：如果是無法安裝軟體於機台上，最佳方法是手持快速掃描設備啟動惡意掃描;如果設備可安裝工控防毒軟體，則可以在符合生產政策下啟動惡意程式掃描。最重要的是監測易受攻擊的合法流程，以防止任何未授權的軟體和資訊變更，並自動化驗證應用和檔案更新為乾淨無害，同時將日誌集中到中央管理平台中以供分析和存檔。

2.弱點管理與資產屏蔽：更新資產取決於很多因素，安全更新可用嗎？如果可用，是否相容？OT環境是否允許對資產進行修補？資產狀態和安全更新狀態是維護過程中不斷考慮的因素。針對未能更新，或尚未更新的資產，此時可透過OT入侵防禦系統的虛擬補丁技術抵禦已知漏洞利用;或者運用Application鎖定功能來阻擋不安全的更新。使用這種方法，無須強制端點進行系統更新，意即不須重新啟動系統，亦不須讓產線停機，能為技術人員爭取更多時間來降低風險，直到原始設備供應商已經發布和測試安全更新;或者無限期地保護其他無法修補的老舊資產。

四、結論

有志邁向智慧製造的組織必須重新審視企業的IT和OT保護架構，TXOne Networks建議採用OT 零信任架構：永不信任，持續驗證。從新設備進入工廠的那一刻起，即對資產進行資安檢查，並協助工廠管理者滿足OT/ICS的複雜網路防禦需求，進一步部署更自動化、更全面的OT零信任資安解決方案。我們的解決方案致力於提供智慧製造場域建立供應鏈安全、現代與老舊的端點保護，以及複雜多變的動態網路防禦，確保廠務管理者簡化資安合規性、打造高韌性網路和端點，同時最小化對機台營運的影響。



參考資料

[1] NSA, CISA, "Control System Defense: Know the Opponent", CISA, September, 2022.
[2] Nathan Brubaker, Keith Lunden, Ken Proska, Muhammad Umair, Daniel Kapellmann Zafra, Corey Hildebrandt, Rob Caldwell, "INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems", Mandiant, April, 2022
[3] Trend Micro, "An Overview of the DoppelPaymer Ransomware", Trend Micro, January 21, 2021.
[4] Beyah, R.; Formby, D.; Durbha, S. "Out of Control: Ransomware for Industrial Control Systems". Fortiphyd Logic., 2017, Accessed Sep 15, 2022.
[5] Melanie Cook, Stephen Quinn, David Waltermire, Dragos Prisaca, "Security Content Automation Protocol (SCAP) Version 1.3 Validation Program Test Requirements", NIST, April 2018.

華碩雲端雲原生、數位韌性 引領企業建構新世代經營 DNA

文 華碩雲端股份有限公司 數位轉型事業處暨技術服務處 潘育群總經理

疫情帶動IT流程自動化和資安議題

在COVID-19疫情期間，防疫政策導致企業必需分地、分流工作，在過去自動化能力不足的公司，更面臨了停工、缺料的風險，嚴重一點甚至會導致公司倒閉。IT產業在這樣的變局之下，顯得更形重要，無論是提供遠距上班機制、同儕共同協作機制、產線自動化機制、遠端監控與除錯等等，若僅靠公司內部有限的IT人力資源，通常無法即時滿足企業營運需求，這時候仰賴可靠與穩定的雲端服務，就是一個最佳選擇。在過去幾年，企

業其實已經加速上雲的進度，同時仰賴雲端服務協助監控效能與維護架構，而目前在積極發展中的是將應用服務「微服務化」以及「容器化」，更進一步就是進行IoT 與 AI 分析(如圖1)。

在本文中想要重新定義IT架構的二個重要面向，第一個面向是IT流程自動化，要將流程自動化其實是一個很大的議題；以製造業為例，這幾年因為工廠人員管理成本增加，因為疫情導致整廠停工的新聞時有所聞，所以「智慧無人工廠」成為IT投資的方向。我們可

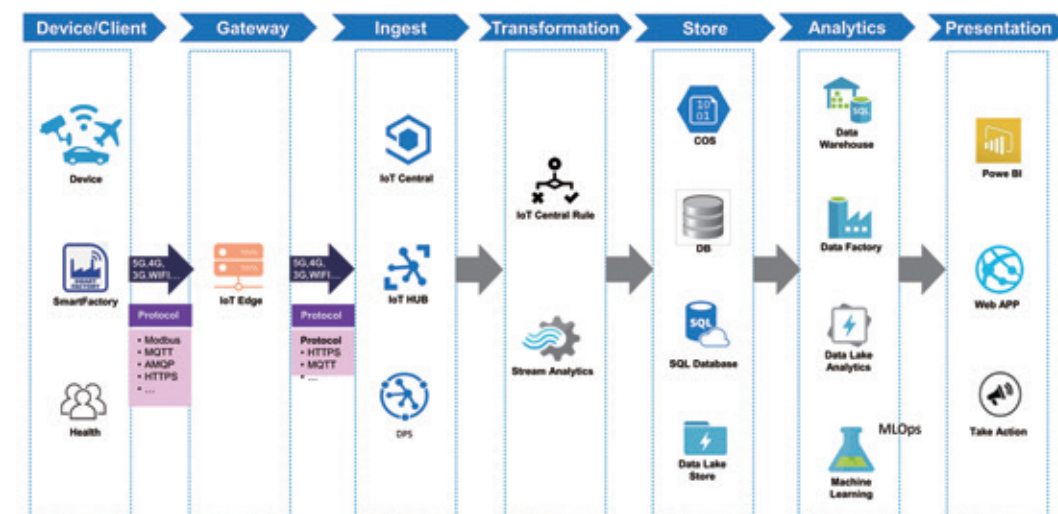


圖2. End to End AIOT流程

資安的定義依據不同角色有不同觀點



Ref. <http://www.tablogic.com/solutions/unified-security/>

圖3. 不同角色對資安的觀點不同，但都應具備資安DNA

IT 的前世今生

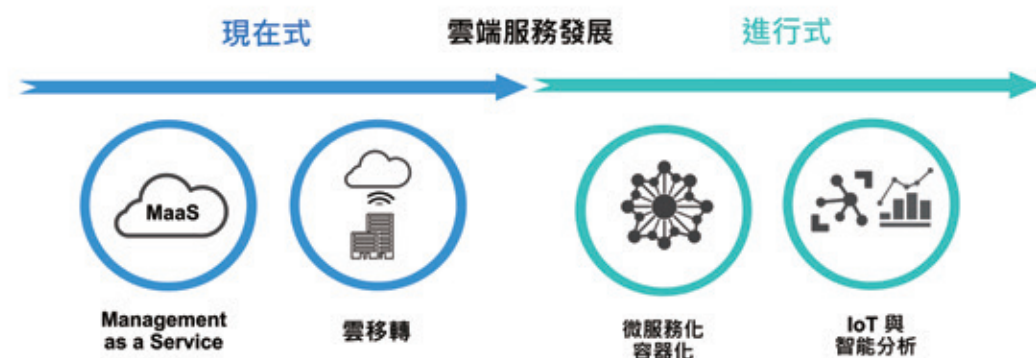


圖1. 雲端服務發展的現在式和進行式

以想像其中工廠內需要有各種精密的感知設備、高解析度攝影機、多軸機械手臂等，但是要能正確地做出回應，前提是已經收集好大量的數據經過AI模組的訓練學習，多次參數迭代調校，才能具備足夠的能力取代人力作業，所以智慧無人工廠為目前IT智慧最大的應用場域。運用精準控制、電腦視覺、AI邊緣運算結合的一站式服務，AI與IoT的結合才能極大化產能與最佳化效益(如圖2)。第二個面向是資訊安全，當企業要進行數位化，或更進一步的數位轉型，一定要先考慮資訊安全。

在數位轉型的過程中，可能會因為一個勒索軟體，讓過去的努力付之一炬。資安的範疇很大，也會因不同角色而有不同的觀念，舉例來說，網管人員、網站開發工程師、軟體開發工程師、與ISMS 稽核要注意的面向均不相同；然而在資安的議題，每一個IT的項目都應該要具備資安的DNA，現在稱為security by design (如圖3)，也就是在設計各種IT/OT架構時就將資安的機制考慮進去，而不是等應用程式上線之後，才在外面加了很多高牆式的資安防護，導致成本難以控制。

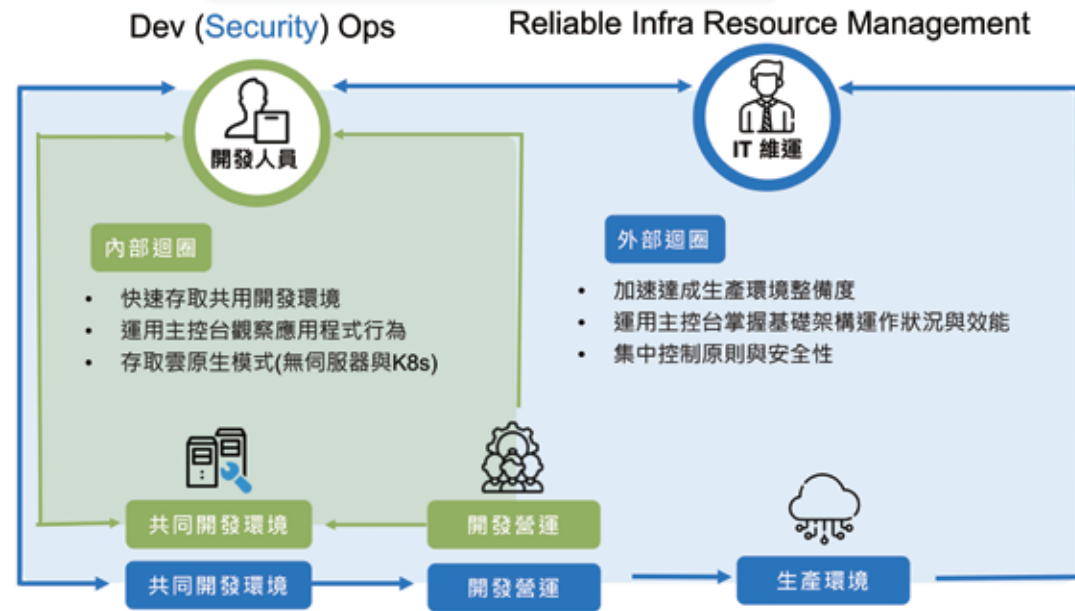


圖4. 開發人員利用容器化的資源管理快速部署營運

透過雲原生與AIoT將服務自動化

雲原生技術(Cloud Native)，從開發工程師應用程式開發到佈署環境的自動化，鼓勵程式架構設計為微服務模式，將運算資源的需求容器化(Containerization)，傳統式的三層式的IT架構會面臨效能上擴充的問題，譬如儲存效能不足時，會導致服務效能低落，唯一作法只能不斷採購更昂貴的硬體設備，另外當應用程式需要即時更新時，也會面臨服務中斷的問題。

以自動化角度不要仰賴太多的人工來做，主要是靠寫程式來達成。以現在如果要使用AI 模組例如語音、文字語意、圖形辨識等不需要從零開始寫，可以藉由地面或者雲端業者提供的服務來達成，只需要透過 API 呼叫其應用即可。在下圖中我們可以看到現在開發人員如何使用IT維運人員所提供容器化的資源管理調度進行開發，並且可以快速佈署營運。(如圖4)

華碩雲端在架構面以容器為基礎搭配Kubernetes的解決方案，負責管理與監控平台的軟硬體資源，包含管理節點、運算節點、儲存系統與網路，具有水平擴展與HA的功能，並讓容器具備GPU運算或多執行個體GPU (Multi-Instance GPU, MIG)的能力，並從2020年開始通過CNCF的認證並且持續升級至Kubernetes v1.23 版本。

在數據面，大多數的機器學習應用，能分類成影像視覺、自然語言處理、語音相關任務與結構化數據等4大類機器學習任務，而這4大類機器學習任務在產、學、研已有相當多成熟的演算法(神經網絡架構)，在社群也有數以萬計的預訓練模型(Pre-Trained Model)，無論是AI專家、資料科學家(Data Scientist)、AI 工程師或機器學習的初學者，不一定凡事都要從頭來打造一切，而是可以運用這些預訓練模型及演算法(神經網絡架構)做遷移式學習(Transfer Learning)，在最短的時間內得到數據基礎結果(Baseline)。

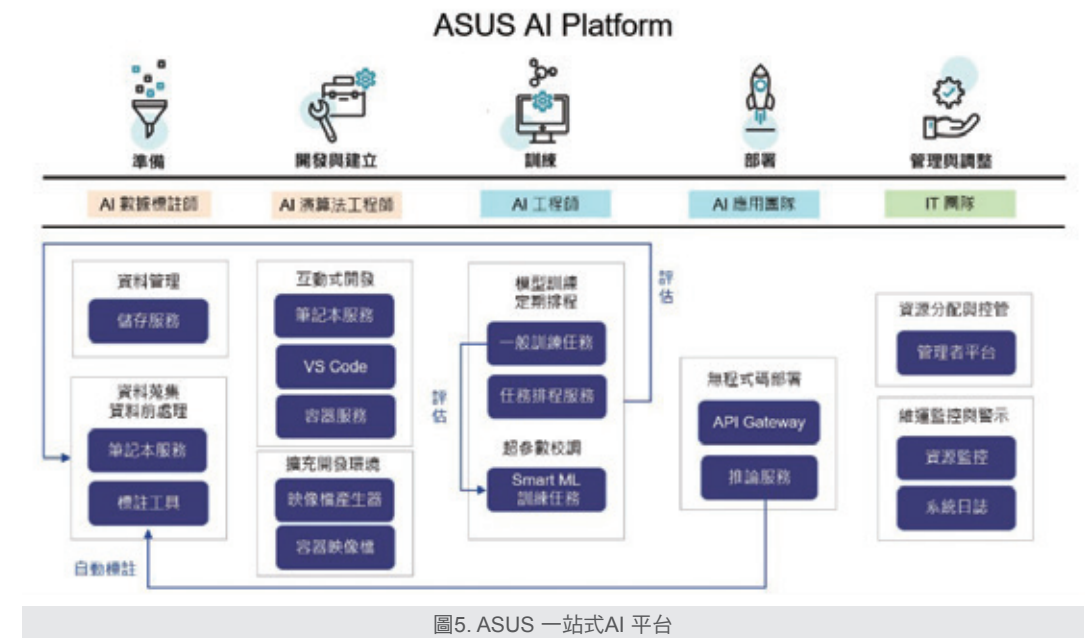


圖5. ASUS 一站式AI 平台

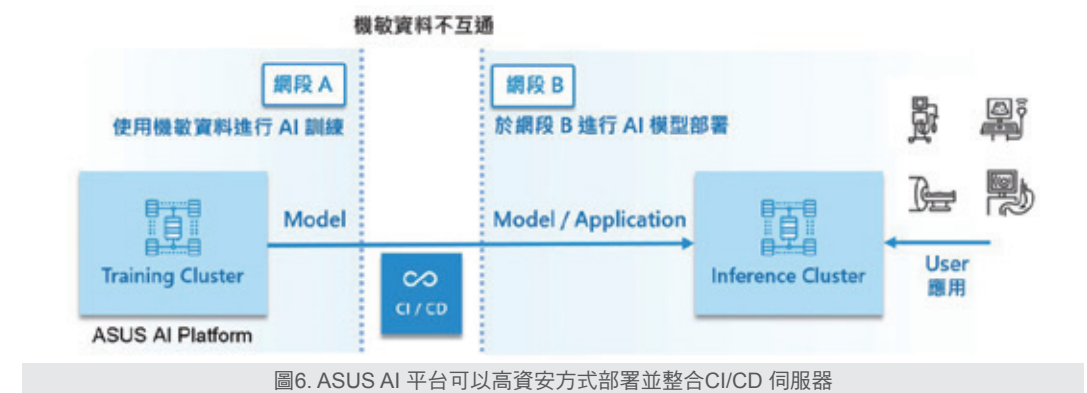


圖6. ASUS AI 平台可以高資安方式部署並整合CI/CD 伺服器

從初版模型(Baseline)一路演進到成熟模型，AI團隊勢必在MLOps的過程中(如圖5)所示，對機器學習流程與演算法做不同程度的修改與調整，也可能對訓練環境做各式各樣的變更，而這成熟的製程(Best Practice)若要套用到不同的數據，或是想交給專案內不同的團隊運用，本平台提供的儲存範本服務，能讓用戶仿照情境式範本建立專屬的客製化範本，讓最佳化的範例能輕易的在專案團隊內擴散。

客製化範本的製作，範圍涵蓋平台的訓練任務、推論服務及容器服務，搭配平台的容器映像檔服務、映像檔產生器服務及儲存服

務，不僅能在訓練任務及推論服務提供客製化範本，in-house開發或專案團隊所需的服務(例如DB等)，也能建立成容器的客製化範本。

除了具備在同一個叢集中模型部署的功能外，亦可根據客戶多個叢集環境需求，提供跨叢集模型部署，滿足基於安全性考慮所需要的運行環境隔離。

平台可以透過Web Service整合CI/CD 伺服器，如Jenkins 伺服器，當平台有合適的模型需要部署到其他叢集環境，使用者除了將模型匯出下載外，還可以透過CI/CD 伺服器的整合，直接將模型匯入其他叢集環境。(如圖6)

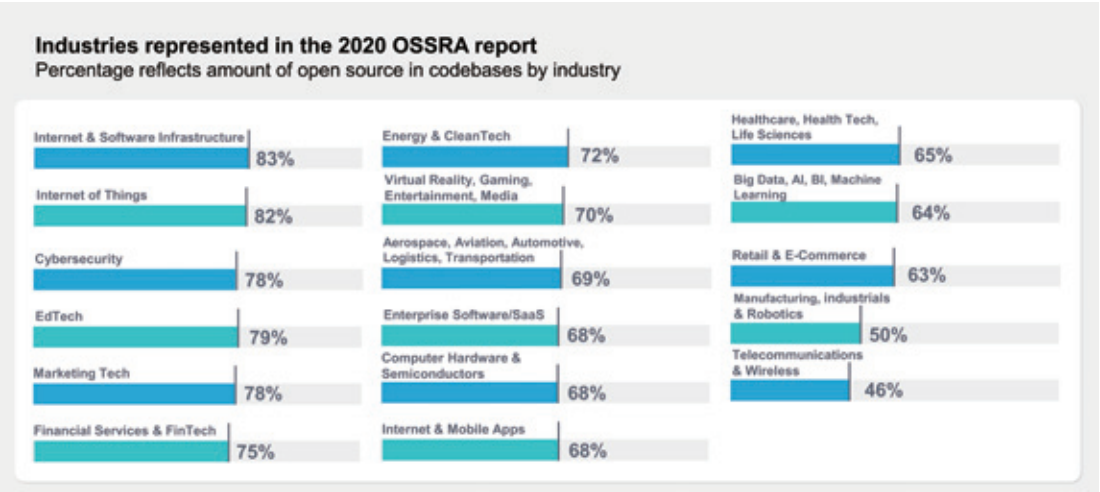


圖7. 2020 OSSRA報告

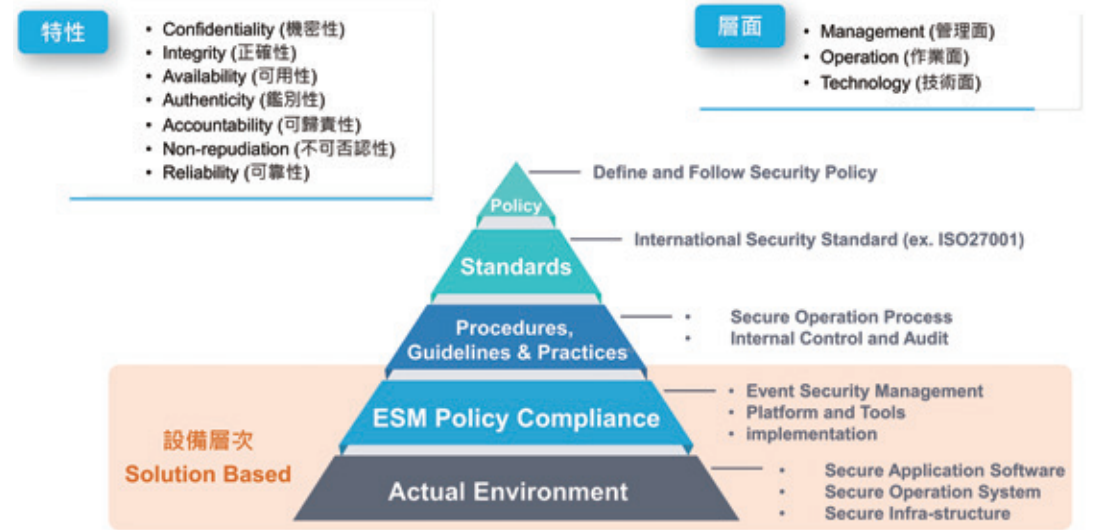


圖8. 資安金字塔



圖9. 企業資安的層次及各類解決方案



圖10. 台智雲及華碩雲端聯合推出多層次防護解決方案

資訊安全

現在資安領域主要在推零信任與供應鏈資安，其實都是Security by Design的概念，為什麼要推供應鏈安全，主要是目前軟體服務開發中大量使用開源軟體，在2020年OSSRA的報告中，使用開源軟體前三名的產品分別是Internet & Software Infrastructure、Internet of Things與 Cybersecurity (如圖7)，所以管理與追蹤開源軟體模的溯源供應鏈是一個非常重要的議題，而且即使目前測試沒問題，也不代表隨著時間的演進，不會有新的資安弱點被利用，進而遭受零時差攻擊。由於資安防護無法保證100%的安全，所以安全軟體開發SSDLC(Secure Software Development Life Cycle)，從需求、設計、開發、測試與佈署維運，每一個階段都有相對應的資安程序需要被執行。也因此近來政府非常強調所謂的數位韌性，當系統被入侵破壞了之後，必須快速恢復服務，從中學習並強化自身體質。

在資安金字塔中(如圖8)，政策(Policy)、標準(Standard)與程序(Procedure)所執行的深

度取決於產業與法規的需求，在實體設備層次中ESM(Event Security Management)與基礎建設的環境(Actual Environment)則要處理實體、網路、作業系統、應用程式與資料(如圖9)。其中核心的應用程式與資料是我們最重要的部份，其韌性也建立在當遭受攻擊時是否能夠快速還原應用程式與資料，重建作業系統恢復服務運作。而要能達到此一目標，最基本而簡單的方式就是備份，這也是數位韌性的最後一道防線。

台智雲及華碩雲端聯合夥伴提供多層次防護的六大解決方案(如圖10)，建構企業永續經營 DNA，提供從端點備份、核心系統備份到虛擬機、容器環境備份以及檔案管理與基礎儲存服務，以國家級高安全性的基礎建設，協助企業打造縱深防禦的資安戰略。

這六大層次解決方案涵括了資料儲存層級、檔案層級以及營運系統層級的備份服務，適用於各類規模的企業。

雲端物件儲存服務: 企業級海量資料儲存空

間，整合嚴謹的安全性機制，支援 S3 協定，可存取各種資料類型，並運用 API 完成儲存任務。傳輸經加密，可搭配 TWCC 各式運算服務，存放關鍵任務如企業資料湖、網站、行動應用程式、備份和還原、封存、企業應用程式等，最適合海量資料安全儲存需求的企業。

檔案協作典藏儲存：高可靠度與擴展性的雲端管理與檔案共享儲存空間，支援多樣系統與傳輸協定，便於進行 AI/ML pipeline、資料分析等工作，以專案方式開發，使用資料達到超高效率。可設定自動資料轉移與生命週期管理，如將冷資料遷移到冷儲存媒體，大幅降低儲存成本。

企業資料安全治理：為私有雲檔案儲存系統，以現代化高可用架構整合企業關鍵資料。單一平台，獨立管理機制，強化資料存取權限控管與安全交換，免除高昂 IT 維運與硬體建置及長期汰換成本，兼顧資料自主性、獨立性，保障資料隱私與企業機密。最適合成長型企業檔案管理與分享。

企業端點資料備份：企業成員端點備份保護服務，可自動備份成員桌機、筆電等資料，透過多路徑、多時間備份保護成員關鍵個人資料。內建勒索防護，阻斷可疑威脅；傳輸儲存多重加密機制，強化安全，遇資安事件，可一鍵快速復原至指定時間版本，任務不中斷，最適合中小微企業成員電腦資料保護。

企業營運系統備份：Safisfy-BKvt 為 Veritas 企業級備份與復原系統，命名結合 Safe 及 Satisfy，以期提供用戶安全滿意的主機系統備份服務。透過 Safisfy-BKvt，數分鐘內即可復原虛擬機器、伺服器、資料庫、檔

案和精細的應用程式物件，大幅節省時間，並達到成本最佳化，最適合成長型企業訂製型虛擬機備份需求。

容器平台備份服務：企業容器備份與還原機制，採開源的 Velero 方式，以異機還原方法將應用程式移轉至雲端或其他環境。備份特定時間點（容器和關聯的磁碟區狀態）的 Kubernetes 集群狀態和磁碟區快照，輔助企業降低維運成本，強化服務韌性，最適合企業 IT 打造開發者多容器備份環境。

建構新世代經營 DNA

國際數據公司 (IDC) 認為數位韌性將是因應新常態的關鍵生存法則，根據其定義，數位韌性指的是「組織利用數位化能力迅速適應業務中斷，不僅能恢復業務營運，還能從變化中找到新機會。」據 IDC 統計，約 80% 企業的數位韌性準備程度處於中高風險，而其中高達 89% 曾遭遇網路攻擊，致使營運中斷，導致重大損失，實突顯企業實施數位韌性方針的急迫性與重要性。

而根據 2022 iThome CIO 大調查顯示，為了因應新常態，有 67.4% 的製造業 CIO 正在強化全公司的遠端工作能力，54.7% 則正在加速內部流程數位化和自動化，以配合各種營運調整及產線需求，可見遠端工作能力和流程數位化已是企業數位韌性的基本能力。這份調查同時也顯示，為了更彈性的跟進市場快速變化，有超過 40% 製造業 CIO 要強化 IT 敏捷性、模組化和彈性能力，24.6% 的一般製造業已經開始將自身的 AP 容器化，而當中採取提高 IT 上雲比重的企業占比，也有超過 30%。這些現象，在顯示這個產業正進一步內化新的經營 DNA，邁向 IT 現代化！

22nd

Electronics Manufacturing Korea

SMT/PCB &
NEPCON KOREAS-Factory &
Robotics ExpoPhotonics
SeoulHighly-functional
Film ExpoPE & Electronic
Materials Show

2023. 4. 12(WED) ▶ 14(FRI), coex

All technology and products
from A to Z in one placecoex
Korea's No.1
exhibition center, COEXKorea's leading electronics manufacturing
industry networking platformUFI approved
international event

www.automotiveworld.kr

5th

Automotive World Korea

AUTOMOTIVE
WORLD KOREA

Automotive Electronics Technology Expo



EV, HEV & FCV Technology Expo



Automotive Lightweight Technology Expo

智慧製造資安痛點與因應策略

文 中華資安國際股份有限公司 劉叡 鑑識暨健診部經理

智慧製造資安防護的痛點及困境

近期國內外工控場域重大資安事件頻繁發生，駭客攻擊對象除關鍵基礎設施外，知名製造業者更是被頻繁攻擊，因製造業無法接受產線停擺而造成的巨額損失，往往願意妥協付出贖金，已是國際犯罪組織覬覦的目標產業，之前人們鮮少探討工業控制系統（Industrial

Control System, ICS）的資安議題，彷彿 OT（Operational Technology）世界不會遭遇加密勒索與資料外洩等風險；但地緣政治衝突加劇，工控資安事件的發生頻率明顯攀升，從關鍵基礎設施到世界級高科技製造業都無法倖免，不禁讓人納悶，為何工控資安威脅會從無到有，而且有恃無恐地在臺灣落地？



中華資安國際股份有限公司版權所有 © 2022 by CHT Security Co., Ltd.

圖 1. 歷年ICS受駭與攻擊案例

關鍵原因是工廠智慧化吸引駭客。工廠欲提升生產效率、增進營運競爭力，積極導入智慧聯網技術，引用大量資通訊技術來建造虛實整合系統（Cyber-Physical System）、數位分身（Digital Twin）與智慧機上盒（Smart

Machine Box, SMB）等智慧製造系統，如此一來，原本封閉的機臺設備開始連網，使 OT 與 IT 網路產生連線，導致 OT 承襲了過往 IT 場域各種資安風險，也接連釀成產線中斷、資料外洩、智財權外流等商譽財務損失。



中華資安國際股份有限公司版權所有 © 2022 by CHT Security Co., Ltd.

圖 2. 數位轉型伴隨的機會與資安風險

2020 年以來，臺灣不少高科技製造業與關鍵基礎設施，遭駭客攻破，進行加密勒索攻擊，中華資安國際也協助部份受駭的高科技製造業與關鍵基礎設施進行資安鑑識及 OT 資安健診，除了分析駭客入侵管道，也檢視網路架構安全，提供強化改善建議，避免再次遭駭。IT/OT 系統互聯化與新興通訊技術導致工控場域資安威脅面日益擴增，本公司觀察到，駭客

攻擊目標已不再侷限於 IT 環境，但國內多數 OT 環境尚未採取任何資安防護措施，從諸多場域發現的共通現象是 OT 與 IT 沒有適當的隔離控制措施，惡意程式可從 IT 設備橫向入侵 OT 網路對產線重要資產造成危害，依實際鑑識與資安健診經驗，可歸納出 OT 環境存在四大資安痛點，分別是「可視性」、「漏洞修補」、「邊界防禦」與「落實度」。



中華資安國際股份有限公司版權所有 © 2022 by CHT Security Co., Ltd.

圖 3. ICS資安痛點

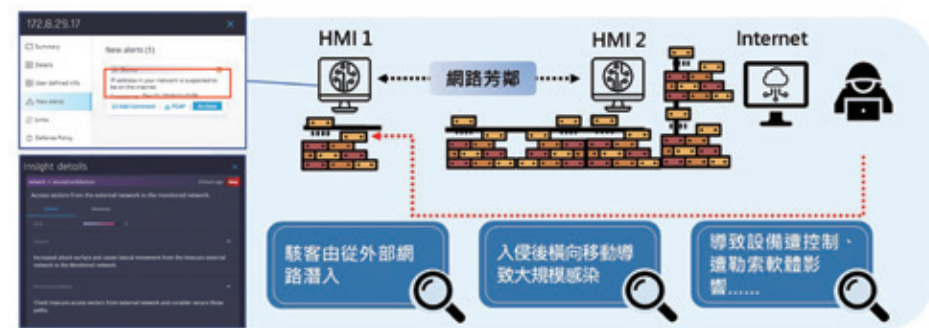
「可視性」是指管理者對 OT 場域中的資產掌握度甚低，無法全面盤點資產清單、網路拓模及資產間的傳輸鏈路關係，存在幽靈資產也不自知。「漏洞修補」是指 OT 環境中的資產常因要求可用性的緣故，無法即時安裝更新以修補漏洞，也沒有任何補償措施，讓過

時的 IT 漏洞攻擊仍可以對 OT 造成嚴重的傷害。「邊界防禦」是指 OT 環境的隔離性與控制措施不足，如存在跨 IT/OT 的 RDP (Remote Desktop Protocol) 遠端桌面連線或是未授權的 Internet 連線行為，以中華資安國際的檢測經驗，有五成的 OT 網路可連接 Internet，高於

國際專業研究報告所揭露的比例數字；至於為何如此，原因不外乎是使用者為求方便，改變若干設定，遂使得 OT 設備出現幽靈連線行為，且無對應的管控措施，造成 OT 網路曝險。「落實度」則是指多數的 OT 場域發生資安事故後，

才發現日常生產與維運作並未按照內部資安規範執行，如應隔離而未隔離、未關閉非必要服務 Port、未更改工控設備預設密碼等諸如此類的「不小心」疏失，當四大痛點被串聯起來時，通常就是重大資安事故與鉅額損失。

- 工控場域普遍存在實體隔離失效問題，將直接或間接面臨Internet攻擊威脅
- 風險事件如：Windows存在弱點、使用SMBv1不安全的通訊協定、對外Internet連線行為、存在幽靈資產等



中華資安國際股份有限公司版權所有 © 2022 by CHT Security Co., Ltd.

圖 4. 資安威脅已在臺灣關鍵基礎設施與製造業落地

中華資安國際以自身執行過的多家能源、交通關鍵基礎設施以及高科技智慧製造業的工控資安健診結果，發現超過五成 OT 場域存在資安缺口。雖然理解 OT 場域的業主將工廠持續運作視為最高原則，資安防護不能影響生產，但是針對企業賴以維生的 OT 場域進行資訊安全檢測、營運風險評估，確實是目前關鍵基礎設施與智慧工廠的當務之急。

近期智慧製造場域與物聯網裝置駭客攻擊案例分享

近期臺灣不少知名製造業者與關鍵基礎設施遭駭客攻破，本公司也協助部份受駭的高科技製造業與關鍵基礎設施進行資安鑑識及 OT 資安健診，除分析駭客入侵管道之外，也提供客戶後續資安防護強化方案，包括建立安

全的網路架構、部署 OT IDS、建立 24/7 OT SOC 監控機制、定期執行資安檢測與導入 IEC62443 制度，降低工控場域資安風險，同時提升企業競爭力，如圖 5 所示。

本公司近年已陸續處理多件物聯網裝置遭入侵案例，主要針對 DVR（數位影像錄影主

機）、網路攝影機、無線路由器與門禁系統等裝置。駭客的攻擊手法，大多為攻擊網頁管理介面、用戶端軟體、網路服務與軟 / 韌體更新機制之漏洞，這些漏洞包含緩衝區溢位、命令注入（Command Injection）、弱密碼、權限控管不當與無更新驗證機制，導致物聯網裝置易被駭客植入後門程式。

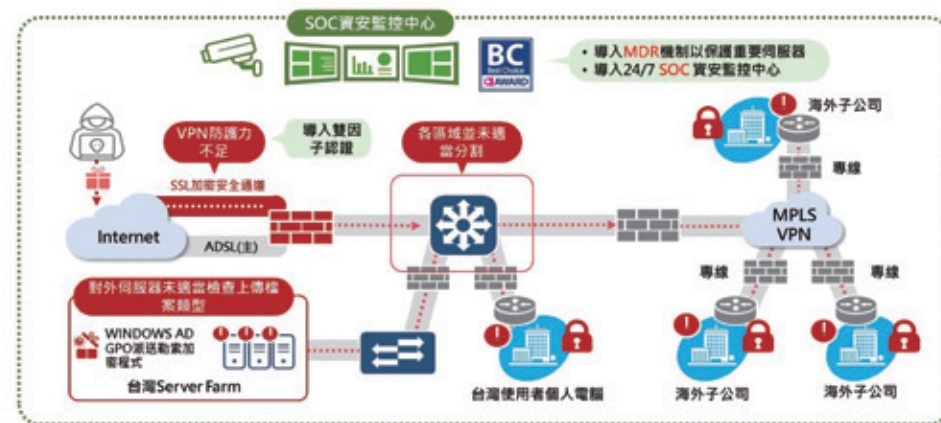


中華資安國際股份有限公司版權所有 © 2022 by CHT Security Co., Ltd.

圖 6. DVR Command Injection

「正所謂『富貴險中求』，當智慧製造廠域提升效率和競爭力的同時，也因為連網承擔了比以往更大的風險」，依本公司資安事件調查結果統計數據顯示，工控場域的主要的

資安破口包括外部曝險介面、實體隔離失效、VPN 帳密外洩與供應鏈攻擊，因此工控場域需超前部署監控與防護措施以因應可能的威脅。



中華資安國際股份有限公司版權所有 © 2022 by CHT Security Co., Ltd.

圖 5. 近期智慧製造場域資安威脅

2021 勒索攻擊事件Top2產業



中華資安國際股份有限公司版權所有 © 2022 by CHT Security Co., Ltd.

圖 7. 近期智慧製造場域資安威脅

智慧製造資安威脅因應對策

總括而論，智慧製造場域的資安缺口成因，主要源自於不安全的連網，以及未修補的設備弱點，加上供應鏈安全問題與資安制度落實程度之多項因素交疊，才會造成攻擊者能夠輕易

入侵，儘管情勢險峻，智慧製造業者可以選擇與專業的資安夥伴合作，執行 OT 資安健診識別潛在風險以建立安全網路架構，並導入 OT SOC 監控機制，搭配 IEC62443 制度導入，為一些無法修補的老舊系統建立防禦措施，將能夠大幅提高駭客攻擊門檻。

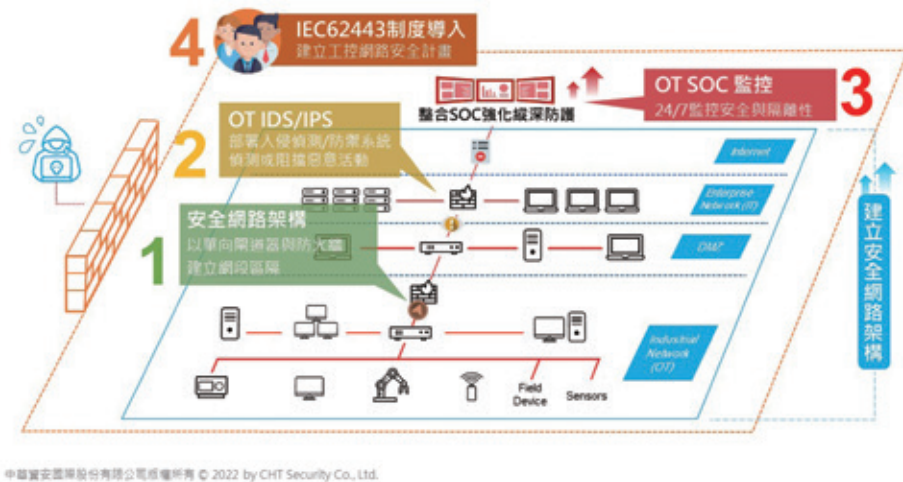


圖 8. 智慧製造場域資安防護四防線

要了解 OT 場域的潛在風險，最有效的方法就是 OT 資安健診，因此，中華資安國際特別利用「非侵入式的網路封包分析」技術，透過交換器連接埠的鏡像，間接側錄 OT 場域的訊務行為，藉此洞悉整個產線與工業控制系統的

設備資產、網路拓撲，以及其使用的網路協定，藉此建立 OT 場域的資產可視性、建立正常行為基準線（Baseline），藉此掌握 OT 環境的系統、網路的資安漏洞，在評估過程中，100% 不影響任何 OT 設備的運作。

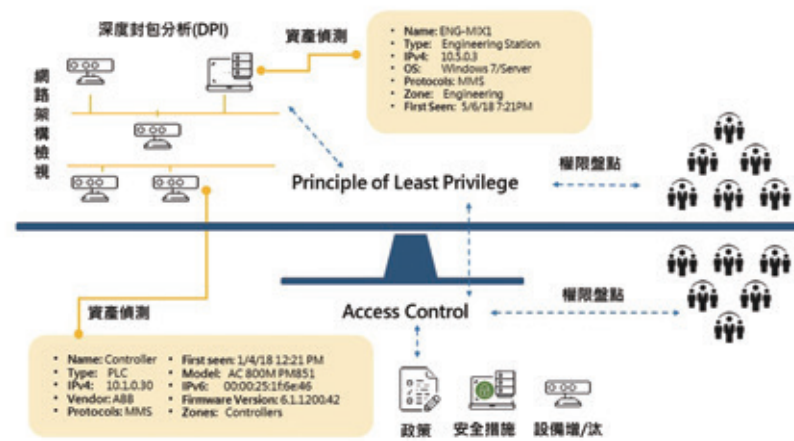


圖 9. 鑑別-深入了解一個看不見的世界

為了管理風險，中華資安國際在執行 OT 資安健診服務協助用戶檢測惡意活動與建立安全行為基準線的同時，也會提供風險評估服務，並執行風險緩解措施。中華資安國際綜觀 OT 資產配置、網路架構及資料流傳輸鏈路，

深入分析曝險介面與駭客可能的攻擊路徑，建立 STRIDE 威脅模型，藉以定義風險級別、掌握曝險程度的高低，再據此設計最適當的資安防護、偵測與控制機制。

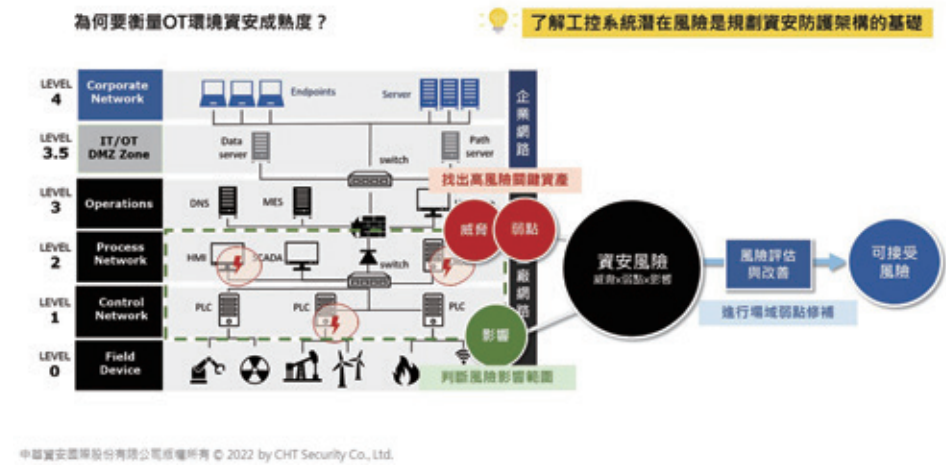


圖 10. 評估-謹慎處理可能的威脅

執行非侵入式檢測的目的是協助智慧製造場域與關鍵基礎設施建立正常行為的基準線，OT SOC 則是持續地監控 OT 場域通訊活動有無偏離基準線的狀態。若 OT 設備的訊務行為未逾越基線，都視為正常、無需加以干涉，但

相反的，萬一哪天有設備的行為出現偏差，開始做出像是封包重送、流量攻擊與控制命令植入攻擊等異常行徑，不論背後原因為何，偵測機制都會立即發出警訊，以利管理者趕緊應變處置，避免事態擴大。

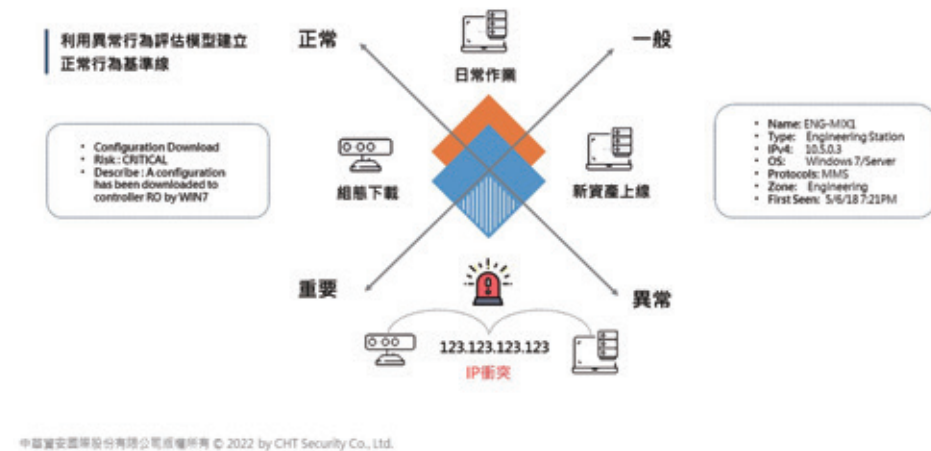


圖 11. 感知-建立內外部的威脅警報器

現階段智慧製造場域與關鍵基礎設施的 OT SOC 監控，就是塑造一個類似『觀察員』的角色。「觀察員」將駐守工廠，在資訊交換節點上持續側錄訊務，接著中華資安國際與 OT 領域專家密切合作，將收集到的訊務進行分析，區隔哪些指令屬於正常或是屬於不正常，針對經判斷為異常的部份，則依據該場域既定

的 SOP 審慎處理，做到既能控制威脅、又絕不影響產線運行，透過部署 OT IDS(Intrusion Detection System) 或 IPS(Intrusion Prevention System) 來建立場域內外部威脅感知能力，包含隔離性與惡意行為監控，若選擇 IPS 還可以透過 Virtual Patch，建立網路防護與阻擋能力，如圖 12 所示。

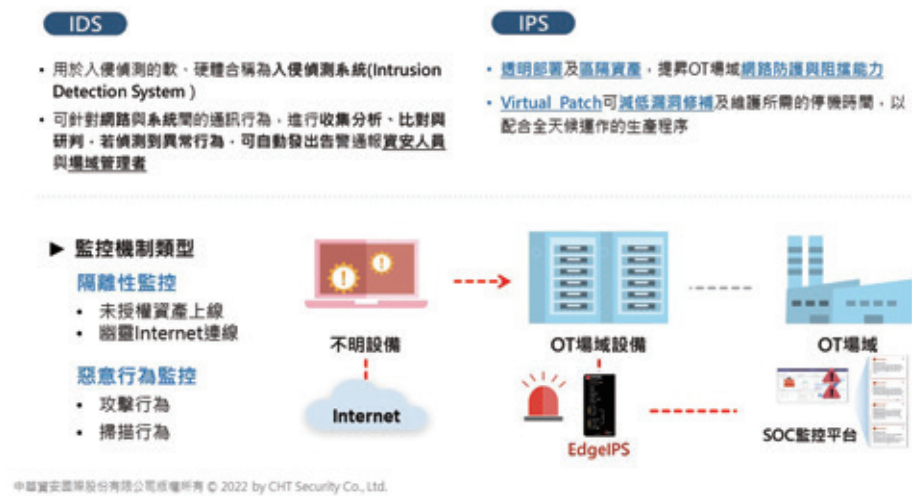


圖 12. OT IDS/IPS

針對 OT IDS / IPS 產生的告警，會由本團隊專家進行分析，例如：有關程控完整性告警，資產是在預期時間內增加的嗎？來源主機執行設定檔下載是否正常？有關安全性事件

的告警，是誤操作還是暴力密碼破解攻擊？事件相關主機進行惡意程式快篩，我們會把這樣的專家知識與經驗，轉化成 OT SOC 監控關聯規則，這樣的好處是可分析的 Log 來源較



圖 13. OT SOC監控-ITxOT



中華資安國際股份有限公司版權所有 © 2022 by CHT Security Co., Ltd.

圖 14. IEC 62443 CBLT 認可檢測實驗室

多樣，例如：EDR(Endpoint Detection and Response)、IPS、Netflow，監控關聯規則範例，例如：跨 IT/OT 網路，在非上班時間 IT 主機 RDP 遠端桌面連線工程師工作站，就會視為高風險事件發出告警通報，以即時應對資安威脅，如圖 13 所示。

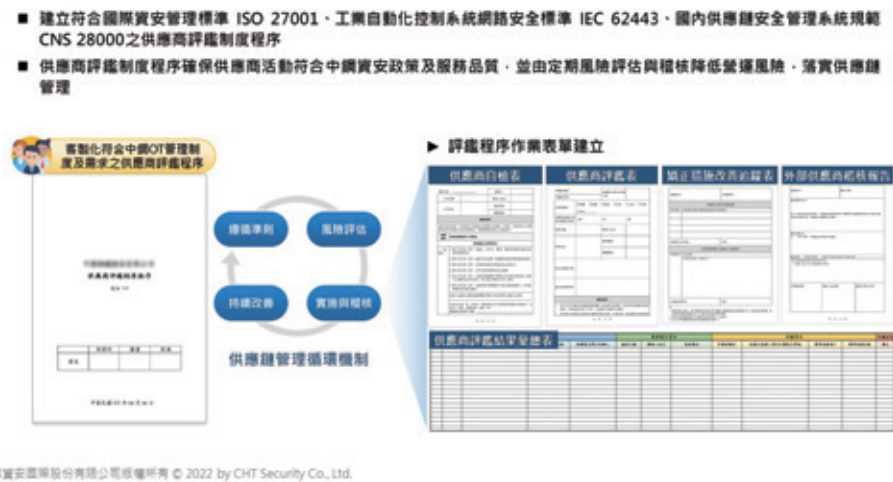
本公司「數位鑑識暨資安檢測中心」已通過 CBTL 實驗室認證，取得 IEC 62443 CBTL 實驗室認證，如圖 14 所示，代表中華資安國際具備提供工業控制系統安全標準的檢測能力與合規諮詢專業，可提供國際認可的 IEC

62443 工控資安檢測報告，協助客戶從智慧製造的場域資安防護，到如何生產製造安全的產品，都能符合國際規範。

2022 年中華資安國際就協助超過 5 家客戶導入 IEC-62443 制度，九月前已有 2 個場域順利取得 IEC 62443 2-4 認證，預計明年將會有更多場域陸續通過，同時也協助多家關鍵基礎設施與知名製造業者強化工控場域資安防護及提升資安事件應變能力，包含協助 OT 場域建立供應商評鑑制度程序，以落實供應鏈資安管理，如圖 15 所示。



圖 15. 建立管理制度-提升企業及產品資安強韌性



結語

本公司已於工控資安領域耕耘多年，基於為多家能源、交通等關鍵基礎設施與智慧製造業者提供工控場域 SOC 監控、資安鑑識與顧問輔導等各式資安專業服務之實際經驗，非常理解 OT 場域擁有者皆將產線持續運作視為最高原則，現實中的資安防護機制部署必須考量場域存在的限制與防護優先順序，本團隊能夠提供的便是確實告知場域擁有者資安風險的嚴重性與可能性及提供資安防護建議與規劃，並在雙方溝通討論後，共同找出資安部署與限

制條件之間的最佳平衡點。

考量 IT 和 OT 場域架構有顯著差異，中華資安國際在協助智慧製造工廠或關鍵基礎設施部署防護架構的過程中，會充份援引 IEC-62443、NIST SP800-82、NIST SP800-64、NIST SP800-115 與 ISO 27001 等國際標準，做為 OT 場域的資安管理框架，在維持 ICS 可用性的最高指導原則下，解決 OT 場域的資安痛點，又可以幫助企業追求工廠智慧化的策略目標。

智慧科技 導入指引

預約索取

製造業者、資服業者、對數位轉型有興趣之相關人士

教你掌握企業罩門，
找出破壞韌性的原因
案例分享如何藉由可視化技術
強化供應鏈韌性



財團法人資訊工業策進會
地方創生服務處

+886-49-6003775 # 5034

lilianlin@iii.org.tw

<https://www.its.org.tw/index.php#>

一本結合智慧科技與風險管理，針對中小企業製造業打造，投入數位轉型的參考指南

RESERVATION
RETRIEVAL

從無到有 打造智慧製造之資安防線 以某上櫃特用化學中小企業為例

文 聚和國際股份有限公司 總經理室暨資訊中心 王邦峻 協理

新常態下資安挑戰

近年來，特用化學產業積極推動工業4.0，建構智慧工廠(Smart Factory)，而個案企業亦不例外，大量採用IOT技術，整合IT與OT的系統環境，消除系統間之資訊孤島，並致力將產線智能化，朝生產作業與製程參數最佳化，使能快速回應客戶需求變化。

然而，隨著智慧化生產管理與設備即時監控之需求，逐漸將之前完全實體隔離的生產系統連上了網路，但卻也增加被攻擊的風險。另外，以往舊有系統的保護機制也可能在連網之後，無法防禦層出不窮的新型態攻擊。因此，企業勢必與時俱進的部署適當之資安機制，來加以應對。而下圖1，便整理在新常態之智慧製造下，個案企業在資訊安全防护上的主要挑戰：

(一) VPN漏洞，供應鏈讓駭客有機可乘：

這幾年，國際間發生多起虛擬私人網路(Virtual Private Network, VPN)相關的供應鏈攻擊事件(Supply Chain Attack)，駭客組織利用竊取VPN帳密，進行登入與攻擊，或入侵供應鏈廠商企圖獲得商業機密。另外，因疫情而衍生的混合辦公型態，也使家庭網

路成為企業安全的潛在破口，駭客利用家庭網路漏洞，對企業網路發動攻擊，企圖找到VPN網路中具有關鍵的數據，進一步攻擊以竊取企業資料。因此，零信任模式(Zero Trust)在近年成為企業安全策略關鍵點之一，如何落實安全存取可視性，以及提升訪問資料的管理權限，是防禦布局的重點。

(二) 縱深(垃圾郵件、端點防毒)與橫向(APT)防禦工事不足：

隨著進階持續性滲透攻擊(Advanced Persistent Threat, APT)的日益猖獗，端點

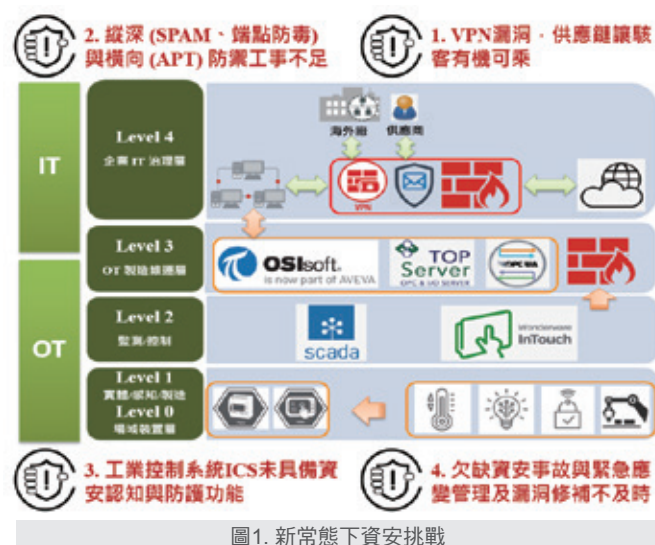


圖1. 新常態下資安挑戰

安全的嚴謹性也隨之到達前所未有的程度。由長時間持續性之連串攻擊行為所構成的APT威脅，不論透過郵件或網站來做為入侵的管道，駭客打從一開始鎖定的目標不是桌機、筆電、伺服器，就是手機或平板等端點裝置，並且為了增加入侵端點的成功機率，APT駭客會量身訂做專屬的惡意攻擊程式，傳統基於特徵碼的防禦技術在毫無樣本與特徵碼的狀況下，根本無法有效偵測出任何安全威脅。對此，全球領先資訊科技研究及顧問機構 Gartner呼籲企業應該趁早導入端點偵測與回應解決方案(Endpoint Detection and Response, EDR)，進而全面提升防範、偵測並回應各類精細目標式攻擊的能力。

(三) 工業控制系統(ICS)未具備資安認知與防護功能：

許多工業生產設備原本操作於獨立的系統或隔離的網路環境中，所以在初期設計欠缺考量資安防護功能，如身份驗證和加密。這表示一旦內部網路遭受入侵，常缺乏有效阻擋的機制，攻擊者可以輕易地進入關鍵的製造系統裡，包括監視和操縱生產程序的控制器。另外，企業在引進製造設備與資訊系統時，如果沒有靠上、下游廠商間資安的稽核與把關、可能威脅情資的分享，並確認出系統的潛在漏洞，就容易出現不斷中毒、掃毒，重灌系統等頭痛醫頭，腳痛醫腳的被動防禦工作。

(四) 欠缺資安事故與緊急應變管理及漏洞修補不及時：

針對火災等公安事故，許多企業都會定期進行相關演練，但對於資安事故，多數企業並沒有一套應變措施，往往直到事故發生之後，才把所有系統廠商找來緊急處理，在

兵荒馬亂之際，可能就不小心破壞駭客入侵的跡證，或是無意之間透露公司受害，進而影響後續的事件調查與因應。而企業在面對資安威脅，還是得儘速建立有關的緊急應變機制，才能在真正發生資安事故時能夠按部就班處置。

如何有效找尋相關資源的協助

駭客攻擊手法多變，手段也不斷在進化，企業無不費盡心力希望能做到滴水不漏，但如下圖2所示，我們永遠無法預測“明天”與“無常”誰會先到？除了透過持續提升資安的防護層級外，更重要的是萬一不幸遭遇駭客滲透攻擊後，我們是要選擇“支付贖金解危”，還是建立完善的“備份機制”，能以最短的時間，還原最完整的資料，讓企業能迅速恢復正常運作，相信，後者才是企業有必要打造的真正最後一道防線。



圖2. 備份_資訊安全的最后一道防線

但是，要持續提升資安的防護與建構完善的備份機制，企業需有充分資源才能做有效因應，如下圖3，一般大型企業在建構智慧工廠與資安規劃時，內部具備專門的資安人員或專業的跨部門團隊，有能力自主規劃，或是有足夠資金找外部顧問諮詢，完善導入相關機制。然而，檢視個案企業在內之大多數中小企業卻面臨類似的困境，一方面，沒有專門的資安人員從事規劃與執行監控，人力不足是資安的最大弱點，亦凸顯企業普遍對資安重視度的不足。另一方面，提升資安防

護是需長期且足夠的預算投入，這對一般中小企業來說是筆沉重的負擔。而每間企業都會認為資安很重要，但實際做到的資源投資卻不一定有及格，常落入「講起來重要，做起來次要，忙起來不要」的情境。所幸，政府持續推出相關補助計畫，秉持扶植產業永續發展，與協助企業成長的精神，對於積極投入資安防護的企業，適時給予經費或節稅上補助的一臂之力，並匯集產官學等專家意見給予指導，讓企業得以快速突破瓶頸，維持企業的競爭力。

智慧工廠規劃	
大企業有資源投入	中小企業面臨問題
由內部跨部門團隊合作，自主規劃	通常由IT主管規劃，欠缺工廠營運經驗
找專業外部顧問公司規劃	無力負擔顧問費用
找自動化業者規劃	無法評估規劃是否適當

圖3. 中小企業面臨資源上的困境

個案企業便是透過政府補助計畫的申請，除了獲得經費上的援助，更藉由外部顧問的專業協助，於計畫時程內將備份、備援制度臻於完善。初期，先透過導入Pure Storage 高效能之全快閃儲存裝置，大幅改善約2倍的資料存取效率，使虛擬主機上之ERP、AI、BI…等相關服務在效能上獲得改善。接著，以此一台高效儲存設備取代原先舊有5台他牌設備，藉由優異的資料減量技術成功達到6:1的資料減量比，大幅改善容量空間。因此，多出來的儲存容量才得以重新規劃與利用，整合備份軟體把全球海外據點的備份全數架構起來，完成異地備援。最後，利用Pure Storage 內建快照與無法將其加密的安全副本，以確保備份資料的有效性與可用性，搭配強化高效復原功能，建構優異的資料保護能力。

資安策略與改善架構

針對上述所面臨之四大資安議題，個案企業探討應如何有效做好資安防護，而訂定出公司在資訊安全上的策略願景：「強化自身完善」和「供應鏈聯防」兩部分。因為，即使本身做了完善的資安管理，若無法掌握供應鏈廠商對資安的作法，等到所採購的系統或設備入廠，再靠資訊單位進行資安相關防禦動作，情勢就會相對被動與嚴峻，惟有同時強化供應鏈的資安，企業也才能最大程度地避免資安風險。依此原則，展開具體之行動方案加以對應，整理如右圖4所示：

(一) 供應鏈身份識別零信任

隨著數位化應用逐步落實，內建連網功能的裝置數量逐年增長，再加上彈性的遠距工作型態，在如此動態的環境中，更需要有一種同時也具備動態特性的安全性方法，來持續驗證信任，藉此允許使用者從當下使用裝置存取機密資訊。基於此原則，規劃透過雙因子認證機制，結合網域認證、VPN、VDI…等工具，強化登入系統之身分識別、降低網路存取的風險及兼顧使用者便利性，以提升公司內外同仁系統使用安全性。而公司在建置多因素身分認證的同時，也是在建立零信任架構(Zero Trust framework)－「驗證且不斷驗證」(verify, and keep verifying)，經由此主動式防禦的關鍵驗證方法，讓企業能隨時為資訊安全做好準備。

(二) 入侵偵測防禦不中斷

進階持續性滲透攻擊(APT)，簡單來說，其實就是有組織且有針對性的網路間諜活動。攻擊之所以難以防禦，在於APT是針對性、持續性、隱密性並且經過精心策劃後，



圖4. 資安策略與改善架構

對目標對象進行入侵滲透攻擊。攻擊方先鎖定了明確的目標，透過長期觀察分析，了解攻擊目標的資訊系統架構，再針對目標對象的資訊系統，發動客製化的攻擊。面對APT攻擊，傳統如防毒軟體、防火牆、IDS、IPS 等被動式資安防禦機制，均可能被駭客輕易地規避。因此，需整合主動防禦機制，並加強異常分析和狩獵組件來強化縱深防禦策略來因應。

(三) 工控資安防護不疏漏

參考NIST（美國國家標準暨技術研究院，National Institute of Standards and Technology）的資安風險管理架構，對 OT 場域進行一系列防護。針對新購機台入廠前，規範「漏洞掃描、滲透測試」等資安掃毒動作，降低由外部引入惡意程式的可能性。接續，在「生產內網」對實體生產設備做好微隔離，以便當災害發生時，能將損害控制在有效的區域範圍內，並能對來源有效識別。而上述風險管理措施都需要在結合供應鏈中的上、中、下游生產設備原廠通力合作，加強對供應鏈資安的稽核與資訊交流的透明度，一起共同解決面臨的資安問題。

(四) 資安團隊建立與威脅監控分析

為了降低在面對資安威脅時之危害與風

險，建立事件應變及處理的流程與標準，是刻不容緩的事。個案企業規劃在制度面上，成立跨部門、最高權限的資安權責單位，並建立資安事件分級，依照事件嚴重程度訂定相關的緊急應變機制，期許當事故發生當下能按步就班處置，在最短時間內，確定事件影響範圍，找出問題發生原因並盡快復原，與預估損失。另外，亦制定通報事件的規則，以及對內外利害關係人的通報機制。

供應鏈之資安聯防

個案企業透過強化自身的資安管理，再串接至供應鏈聯防機制，以獲得國際客戶稽核之信賴，繼續站穩國際供應鏈，並持續推動產業數位轉型與升級，以提升出口產值與國際市佔率。在緊密相連的供應鏈體系，過去企業獨善其身的資安防護已不足夠，為了強韌供應鏈資安，客戶已逐步慎選其上游供應商，甚至在採購流程裡，強制納入供應商的資安評鑑，以確保不會有重要資料洩漏，或被駭客有目的與組織性的供應鏈攻擊。此外，企業也得考慮投資建立數位鑑識能力，向客戶說明、提出具體的例證，去釐清一旦出現資安攻擊時，自身已經做了哪些努力、盡到哪些責任。

智慧製造廠商可能面對的 資安威脅與防禦方式 (應用層篇)

文 Sky Yu, Senior Security Solutions Architect - APAC Lead, Edgio



一、工業革命趨勢提升資安控管重要性

工業生產帶來的大量生產和便利性，驅動著人類社會持續進步，工業革命自1750年的蒸汽機發明後，機械動力突破了傳統的動力限制，進展到現在透過電氣化設備，以及資訊系統來控管整合產線與上下游物料供貨，能夠更有效率地反映市場需求與降低成本的浪費。

IT技術的引進為工業帶來了新世代的運營模式，但在帶來便利與效率的同時，IT本身面臨的資訊安全挑戰也隨之而來。當IT技術參與甚至接管了維運、監控、生產、庫存等環節，IT與OT的邊界不再壁壘分明，加上內外連網需求越來越大，原本在IT系統上的資安議題也隨之而來，工廠製造業因為資料外洩導致訂單流失，或是被駭客攻擊勒索導致停工的案例屢見不鮮，唯有制定正確的架構，明確定義IT/OT邊界與最低權限管控資料數據流，並定期進行備援演練，確保在服務遭受影響時，可以在有效時間內排除問題或啟動備援，讓產能不受影響。

二、工業4.0導入可能帶來的資安威脅

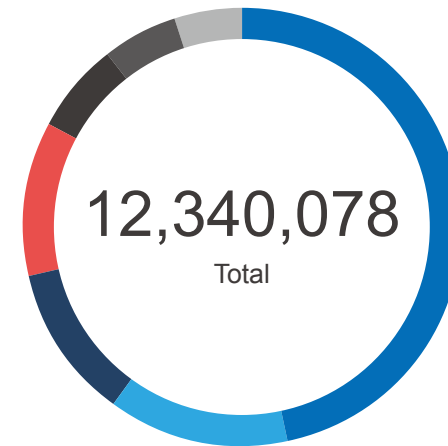
工業環境引進的IT設備與聯網系統越多，相對的也就暴露了越多的弱點，為有心人士

提供了更多可供利用的入侵途徑，舉凡可透過網際網路存取的外部環境，到只有內部網路能存取的環境，以及監視與門禁控管等實體安全，都涵蓋在資訊安全領域的範疇之中。不同領域有各自專長的資安服務供應商，也因此截至目前為止，還沒有一個資訊安全完整解決方案出現，必須在各自不同的製造生產場域，尋找搭配最適合自己的安全解決方案，並整合彼此的優勢截長補短，方能達到最佳的安全防護。

三、工業化產品轉為客製化需求

隨著產業升級，工業生產的產品漸漸不再藉由大量生產降低成本，創造利差空間當作營利方式，很多廠商開始以貼近消費者的客製化需求，藉由獨一無二的單品少量生產，但利潤極大化來創造獲利空間，例如專業運動智能手錶、個人攜帶式用具例如智能麥克風、球鞋、球拍等等，藉由提供小眾但具有個人化專業的需求，搜集使用者數據（聲線、運動習慣與強度等）並分析行為紀錄後，提供使用者對應的專業反饋。

或是搭載內容服務的設備，例如車用音響主機、遊戲主機等等，在硬體設備生產之後，還需要藉由提供軟體韌體更新，持續提供終端使用者優質的服務體驗。



Based on customer data, illustration purposes only.

圖2.網站服務流量分析

四、常見的駭客攻擊事件與資安防禦方案

這類的服務仰賴著內容傳遞網路（CDN，Content Delivery Network）來快速接收全球客戶的請求，並且可以快速部署更新程式到全球客戶的終端設備，但這些服務也有其資訊安全的疑慮：

1.對伺服器進行DDoS攻擊造成服務中斷：

依賴即時線上服務創造營收的客戶，需要特別注意這類攻擊，根據過去的經驗來看，不論攻擊者有沒有能力產出DDoS流量，他們都會亂槍打鳥對這類客戶進行勒索威脅，部分尚未完善DDoS防禦的客戶，在收到勒索信件的當下就選擇交付贖金，也造成攻擊者食髓知味持續進行勒索。

2.對網站進行應用層攻擊造成內網被突破，或是機敏資料外洩：

疫情影響造成遠端作業需求變大，原本只提供實體辦公室存取的外部服務，現在也必須提供來自網際網路的登入需求，攻擊者透

Typical Bot Traffic

- 49% Human Traffic
- 14% Search Engine
- 12% Web Scraping
- 12% Brute Force & Credential Stuffing
- 7% Fake Account Creation
- 6% Transactional Testers
- 5% Fake Search Engine

過暴力式攻擊或利用服務漏洞登入內部系統案例屢見不鮮，身份驗證與相關安全防護變得更加重要，如去年底的log4j零時差漏洞，一個更新來不及部署或是零時差漏洞修補太慢，都有可能直接造成內網被外人闖入，帶走機密資料。

3.沒意義的網路爬蟲流量造成不必要的頻寬成本支出：

網路爬蟲業者持續發送請求取得網站資訊，再綜整相關訊息直接販售或是搭配廣告，提供給他們的使用者資訊藉此獲利。這些請求這些請求佔了所有請求的一半以上，且可能無實際效益，如果能在條件下設定有效過濾不必要的這類請求，除了網站的效能可以提昇，也可以有效節省每個月固定的網路頻寬成本。

五、Edgio CDN全面安全解決方案說明與特色介紹

Edgio身為全球前三大的CDN服務提供廠商，提供了全球邊緣運算的對應安全解決方案，我們無法預期下一個是什麼攻擊在什麼

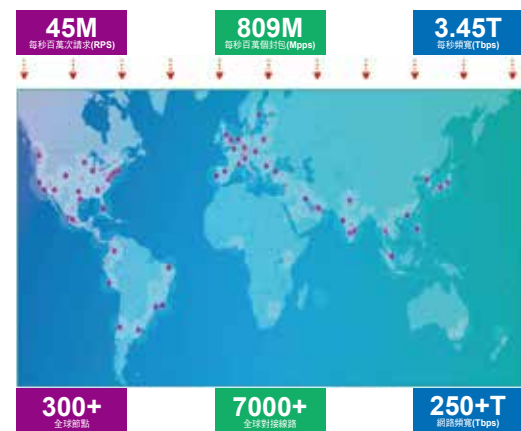


圖2.Edgio全球資源部署完整，全球超過300個以上超級節點與大於250Tbs的頻寬署

時候發生，但藉由全面的資安防禦偵測服務，可達到威脅快速偵測與響應，有效地在資安威脅發生當下快速獲取相關數據，並進行對應的阻擋防禦措施，在實際危害尚未發生之前，就將其消弭於無形之中：

1. Anycast架構加上全球超過300個以上的超級節點，和大於250Tbs的頻寬，全時有效開啟並對第三第四層的DDoS攻擊完全免疫，在今（2022）年中Edgio的架構，有效協助一位台灣高科技製造廠商，阻擋來自歐洲的大量封包請求DDoS攻擊，透過Edgio節點邊緣伺

server_timestamp	rate
2022-06-14 20:59:01	1.85 million
2022-06-14 20:59:02	64.76 million
2022-06-14 20:59:03	126.95 million
2022-06-14 20:59:04	147.65 million
2022-06-14 20:59:05	165.33 million
2022-06-14 20:59:06	166.51 million
2022-06-14 20:59:07	170.08 million
2022-06-14 20:59:08	172.01 million



即使邊緣節點承受大量DDoS攻擊，客戶服務卻完全不受影響

圖3.Edgio防禦DDoS實例

伺服器發出效能告警，但藉由高可用的網路架構，有效的將此流量分流並且過濾，完全沒有對客戶的服務造成任何影響與延遲。在第七層Edgio提供了速率請求限制規則，可以根據不同網站流量，制定對應的請求流量限制，來有效阻擋應用層的DDoS相關攻擊，包括持續性低慢速DDoS流量攻擊等皆可有效防禦。

2.全方面的網站應用防火牆

（Web Application Firewall，WAF）規則，共有三大主要規則分述如下：

- (1) 存取限制規則：可根據地理國家、IP 或 User-Agent等所有請求相關檔頭進行偵測過濾，並支援ISO 3166-2可對地區性城市進行IP過濾，本次烏俄戰爭中部分有爭議的地區如克利米亞半島，目前既不屬於烏克蘭也不屬於俄羅斯，就可以藉此規則進行偵測過濾；
- (2)、託管式規則：Edgio的安全威脅情報部門根據過去的攻擊資訊，對常見的網路攻擊預定義了將近1000條的安全規則部署，可有效阻擋OWASP前十

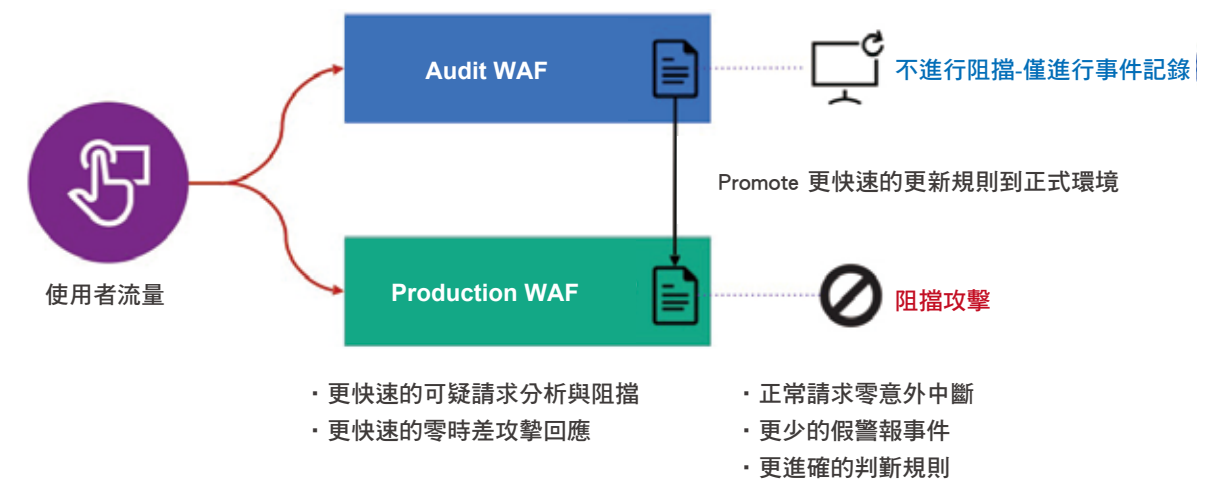


圖4.Dual WAF的架構與優勢

大的攻擊之外，也針對了常見的網路套件部署了零時差偵測的規則，在今（2022）年發生的spring4shell零時差攻擊，即使原廠尚未提供修補程式，但因此攻擊需利用java等服務，已在我們預先定義好的規則之中，本波零時差攻擊並未對Edgio下所有託管的客戶造成任何影響。

- (3) 客製化規則：每個客戶的環境皆不相同，總會有預定義安全規則無法偵測到的特定需求，Edgio提供了客製化規則讓客戶可以自行撰寫規則，可以偵測任何可能有潛在危害的請求。去（2021）年的log4j零時差攻擊漏洞在攻擊程式碼釋出的24小時內，Edgio的安全威脅情報部門就對該攻擊進行客製化規則定義，藉此確保所有的客戶不受此攻擊影響。

以上規則同時支持Edgio獨家的Dual WAF模式，可在攔截阻擋惡意請求時，同步進行事件記錄，可以更快速有效地找出看起來正常，但實際上有有害的請求。

3.第四代網路爬蟲機器人解決方案：整合人工智慧與機械學習分析爬蟲機器人請求，不僅能偵測特徵和行為，可透過長期收集的數據進階分析請求意圖，不但可以找出長期潛藏的低頻請求，也可以抓出假帳號這類沒意義且浪費公司頻寬成本的請求。

目前Edgio提供了全球各大製造商與智能設備 / 服務供應商CDN網路安全的解決方案，提供快速且安全的CDN網路服務，也透過客戶的網路數據分析，持續強化CDN服務效能與安全防護，希望藉由Edgio全方面的安全防護，能夠持續協助客戶阻擋可能的網路威脅，在後疫情時代下達成穩健資安防禦兼具提升內外網絡效能。

有關Edgio的更多信息，請掃描下方QR CODE訪問我們的網站



有效防禦勒索軟體 構建企業資安新思維



文 杜浦數位安全

最新資安威脅與面貌

台灣因地理位置與國際局勢之特殊性，政府機關與高科技製造業長期遭遇大量進階持續性威脅（Advanced Persistent Threat, APT），通常是有心人士精心策劃，出於商業或政治動機，針對特定的目標（如特定組織或國家），進行之長期攻擊過程，此類型攻擊特點之一是在長時間內保持自身行動的高隱蔽性，使受害者難以察覺，此類的攻擊者多為背後有政府力量挹注的國家級網軍。

又因近年來加密貨幣興起，其身分隱蔽性的特點，難以調查金流去向，讓更多有心人士投身加密勒索攻擊行列，要求受害者以加密貨幣支付贖金，或以加密貨幣作為同夥的交易方式。根據 TeamT5 長期所掌握的情資顯示，加密勒索攻擊是一個龐大且分工細膩的生態系統，分別有攻擊者負責提供登入憑證（Credential）、漏洞攻擊程式（Exploit）、加密惡意程式（Ransomware）、收受贖金的加密錢包位址（Cryptocurrency），甚至包含專門負責攻擊活動的惡意駭客。

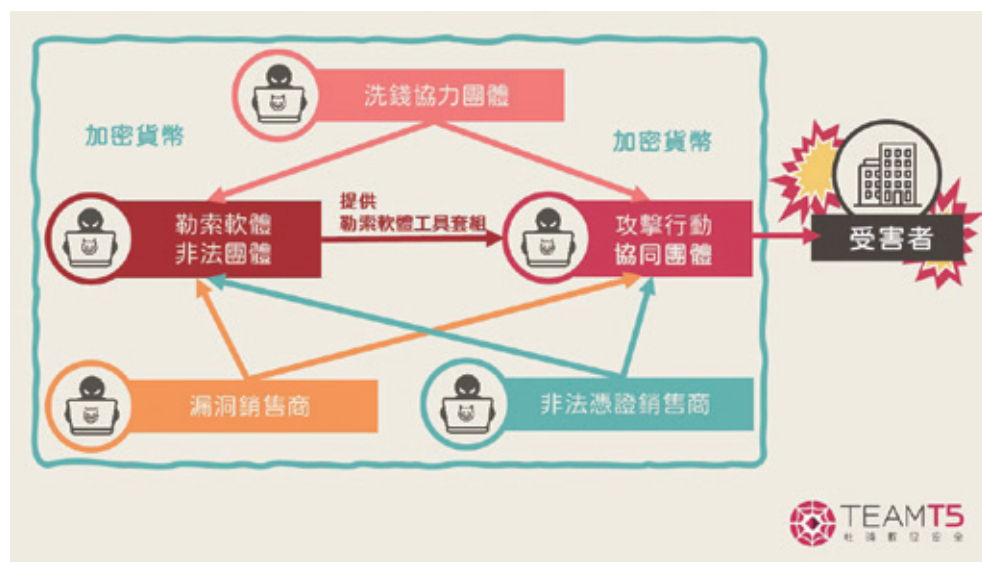


圖1. 加密勒索攻擊的生態系統



圖2. 加密勒索攻擊步驟

從實際攻擊事件看企業的資安防禦

根據 TeamT5 的威脅情資與資安事件調查結果，將加密勒索攻擊手法彙整為五個步驟階段，各階段詳見圖2。

駭客在一開始會找尋攻擊目標，從中取得可做為初步入侵的突破口，例如近年因遠距辦公，而常遭到攻擊者利用的 SSL VPN 設備漏洞，抑或是 Exchange 郵件伺服器的 ProxyShell 和 ProxyLogon 漏洞。

當駭客成功入侵到受害環境中，取得初步控制權之後，接下來會在環境持續進行入侵攻擊，目的是取得更高的權限或是取得更多受害主機的控制權，方可進行下一階段的大規模加密勒索攻擊，而此階段的攻擊行動稱為水平橫向移動（Lateral Movement）。

當取得環境中多數電腦的控制權後，駭客下一階段會竊取關鍵機敏資料，如產品設計圖、用戶個人資料、訂單資訊等機敏資料，後續就會發動大規模加密攻擊，常用的管道包含利用Active Directory 群組原則物件

（Group Policy）或是資產管理系統，大量派送部署加密惡意程式。

當加密完成後，駭客會在受害電腦留下顯眼的勒索訊息，要求受害者不得報警、不得通知資安廠商，甚至不得重新安裝系統。更有甚者，2022年最猖狂的加密勒索族群 LockBit 3.0 會公開招募受害單位的員工，若有人提供受害環境中的登入憑證，將可以獲得部分勒索贖金的分潤。

最後，駭客會將先前所竊取的機敏資料，逐步在地下論壇、暗網（Dark Web）部落格中揭露，藉此逼迫受害者因心生畏懼，害怕遭到供應鏈或主管機關的裁罰或求償，因此繳付贖金，企圖取得可將被加密資料還原的解密金鑰。而駭客就是抓準了受害者的心態，不斷地施壓，重複向受害單位多次勒索。

企業防禦加密勒索威脅的策略與方向

企業用戶在面對加密勒索攻擊時，需要因應不同階段採取不同的資安防禦策略，



圖3. 加密勒索防禦策略

TeamT5 建議可分別從威脅認知（Threat Awareness）、遭到攻擊前（Before Attack）、受攻擊期間（During Attack）及攻擊後（After Attack）四個階段分別規劃。

在威脅認知階段，首要目的是了解可能的攻擊者為何，從攻擊者的來源、手法來擬訂後續的防禦策略，防禦策略分述如下。

- ◆從其他加密勒索攻擊案例，取得受害方的防禦經驗
- ◆定期進行威脅評估（Risk Assessment）
- ◆建立持續營運計畫（Business Continuity Plan, BCP）
- ◆教育訓練與演練模擬（Training & Drill）
- ◆投保資安險（Cyber Insurance）

在加密攻擊發動前階段，主要精神是假設自己的環境會遭到駭客入侵，在即將發生危害前，透過先行導入各式防禦產品，最大程度限制攻擊者入侵得手的機率，其防禦策略分述如下。

- ◆部署加密勒索防禦產品
- ◆導入最新的威脅受害指標（Indicator of Compromise, IOC）
- ◆盡可能修補所有已知的漏洞，避免遭到駭客利用
- ◆長期且定期的備份重要資料

在攻擊者發動加密攻擊的當下，重點在於強化當前威脅的可視性（Visibility）並且立即處置因應（Response），其防禦策略分述如下。

- ◆即時監控並要能關聯到可能的加密勒索族群
- ◆立即阻擋加密攻擊
- ◆快速處理惡意威脅活動，避免威脅持續蔓延擴散

在發生加密攻擊後，需要快速應變，立即啟用復原與威脅抑制作業，並統一對外說明管道，其防禦策略分述如下。



圖4. TeamT5 as a Service 專業工具與服務助企業有效防堵勒索軟體

- ◆隔離受害端點的網路連線，避免擴散感染
- ◆根據BCP計畫，快速重啟服務和恢復資料
- ◆啟動資安事件調查（Incident Response），找到事件根因（Root Cause）
- ◆聯繫公共關係（Public Relation, PR）與法務單位（Legal），統一對外說明管道

TeamT5-as-a-Service 專業工具與服務助企業有效防堵勒索軟體

市場上有許多國內外廠商具有端點偵測與應變系統（Endpoint Detection & Response, EDR），但資安廠商是否具備足夠的威脅情資能量，能夠提供用戶最新的威脅趨勢分析，協助超前部署、防範於未然。另外，資安廠商是否具備在地化服務團隊，能夠協助分析當前的威脅事件，提供相對應的威脅緩解抑制措施，避免環境持續遭受駭客控制，災情不斷擴大。

TeamT5 憑藉長期的自主性威脅情資研究成果，能夠快速辨識各式駭客攻擊手法，利

用所開發出來符合企業用戶需求的 EDR 系統，於用戶的環境中快速偵測與反應，甚至透過專家服務以客製化的方式解決問題。因此 TeamT5 整合情資、產品與專家，提供用戶完整的端點惡意威脅的專家防禦服務，幫助用戶安然渡過每一次的駭侵事件。



跨網路資訊傳輸的零信任作法



文 達友科技股份有限公司 林皇興 副總經理 / CISSP/國際資安師證照

加密勒索攻擊已經變成各行業的資安重大威脅。這樣的事件造成的損失除了同仁辦公作業中斷、資料損失之外，如果造成的是工廠的產線中斷，帶來的損失將更巨大，甚至還可能造成工安的事件，因此不得不列入更積極的防範。

目前還有個攻擊趨勢，加密勒索的駭客集團在企業內網潛伏期間，還會蒐集企業的機敏資料，例如業主的設計圖、企業擁有的個資、研發的資料…等。因此一旦爆發加密勒索事件，企業可能選擇不付贖金，而請資訊人員或委外廠商透過備份來還原系統。此時駭客集團可能會進一步要脅，將其滲透期間所竊得的機敏資料、個資、營業秘密，威脅受害企業如果不願意付贖金的話，則將這些資料加以揭露、或在暗網上進行拍賣，甚至直接去跟該企業的客戶、委託代工的業主聯繫，進行二次勒索。因此，企業如果不幸遇到這類的資安攻擊，壓力一定很大。

存在外部網路資訊交換，就可能是防疫上的破口

當今的企業為了營運所需，一定會跟外部進行資料的交換，包含收送外部的電子郵件、允許同仁瀏覽網路上的網站、傳送接收客戶或供應鏈夥伴所需的檔案…等。然而稍不注意，惡意程式就被帶進來了。

例如使用者可能收到外部寄來的電子郵件，如果該郵件因為駭客收集足夠的情報，客製化的為收件者打造的主旨與內容，這樣的社交工程釣魚信件，其點開信件內容、點擊其中夾帶的網址超連結，或開啟有毒附件文件檔案的機率是很高的。

為何企業都有安裝防毒軟體，還會中毒呢？

為何企業都有安裝防毒軟體，還會中毒呢？原因是目前一般使用的防毒軟體，是仰賴病毒特徵來偵測病毒，因此能夠偵測的必須是已知的病毒，是已經被防毒廠商發現

的，已經收錄病毒特徵的，才能被偵測。如果是全新的病毒，被感染的端點如果沒有發現異樣，就不會去通報，而偷偷的潛伏於電腦中。所以目前許多的加密勒索事件，即是駭客集團一但入侵一家企業的內網，往往不會馬上發作，而是偷偷的潛伏，藉此為跳板進行平行移動，滲透到公司其他端點，甚至重要的主機與系統，最後一槍斃命，癱瘓企業的營運。潛伏的期間，從數十天到數百天都有。企業的資安能量如果無法在駭客集團潛伏期間就能夠識別，則往往已經全面被加密，系統全都被癱瘓了，才發現內部網路原來已經被入侵，且說不定機敏資料已經都外洩光了。

以往的資安都是仰賴偵測 (Detection)，將不好的偵測出並加以阻擋

傳統的資安做法，都是仰賴偵測的方式，依據既有情報將不好的物件或有問題的流量偵測出來。例如防毒就是仰賴病毒特徵，將有問題的檔案進行掃描；例如仰賴封包特徵，透過防火牆或IPS入侵防禦系統，識別異常的網路封包；例如仰賴網址分類資料庫，或威脅情資，識別使用者是否連到惡意的網站、釣魚網站，還是駭客佈署的惡意程式回報連線的中繼站…等。然而這些都只能識別出已知的問題，針對沒有檢出的檔案與流量，就不會阻擋。因此允許的流量與檔案，不代表其是一定乾淨的，只是當下不知道而已。

改變以新的零信任觀念，抵禦未知的威脅

大家可能開始聽到市面上許多資安廠商

開始在談零信任，而大家認知的零信任可能都各自表述，也不確定如何著手才是對的。我們認為或許可以從跨網路交換的資訊角度，來實施零信任的方法。只要您的電腦需要接收來自不同安全等級的網路的資訊、檔案，則一律不予信任，需要進行適當的「隔離」、「檢疫」與「清洗」的程序，才允許這外來的資訊、檔案得以落地到內部網路中被使用。

筆者個人認為，要達成上述零信任的情境與要求，有兩種資安技術是關鍵的。其一是上網隔離瀏覽技術(RBI, Remote Browser Isolation)，其二是針對資訊與文件的CDR清洗技術(Content Disarm & Reconstruction)，下面針對時下的這兩種零信任技術以及應用上的實務進行說明。

零信任的關鍵技術之一，上網隔離瀏覽技術

其中一個關鍵的零信任應用技術，即是「上網隔離瀏覽」技術，原文為Remote Browser Isolation，簡稱RBI。隨著雲端與容器技術的成熟，透過容器化技術，讓瀏覽器核心執行於遠端的隔離容器，讓欲訪問的外部網站執行於隔離容器中，並透過特殊的清洗轉換技術，讓網頁中的內容安全的呈現於使用者的既有瀏覽器上，並確保不會有外部第三方任何可執行的元件有機會於使用者的瀏覽器中被執行，據此確保完全沒有機會讓惡意程式有利用的空間。使用者每訪問一個網站，都啟動新的且獨立的隔離容器，且用完即丟棄。

目前資安業界越來越多的廠商有實現RBI這

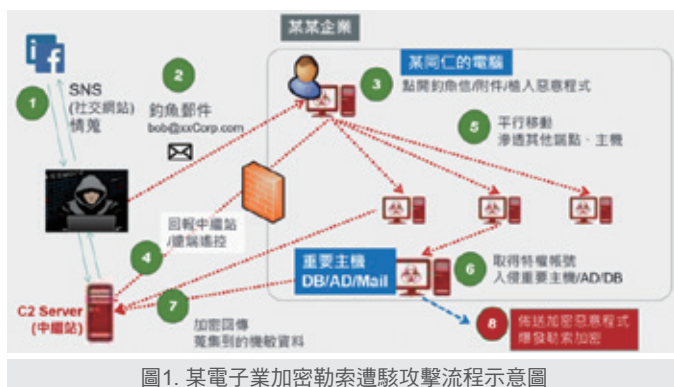




圖2. 上網隔離瀏覽RBI技術示意圖

樣的隔離技術，且都已經產品化。這幾年有導入的都是金融業、政府、科技製造業，以及關鍵基礎設施等單位，對於資安有要求高度重視的。

零信任的關鍵技術之二，文件的CDR清洗技術

文件的跨網路交換時，偶爾會是被駭客利用作為夾帶惡意程式的載具。然而一般防毒軟體對於惡意文件的偵測效果較差，檔案沙箱的檢測方法成本較高且不即時，又容易被駭客規避偵測。因此近幾年衍生出文件清洗CDR技術的發展。CDR清洗技術的英文原名為Content Disarm & Reconstruction，即將

各種文件的內容拆解後，將可能會執行且有機會造成危害的物件依政策剷除，並重組回相同格式可用的文件檔案。這樣的過程又稱為檔案無害化處理。

目前業界提供CDR檔案清洗技術的廠商越來越多。CDR技術須至少能支援企業常用的幾種文件檔案格式，其次是轉換的速度要快，轉換後的檔案可用率要高。最重要的是，CDR技術需要可以彈性的整合既有的環境，並滿足以下幾種常見的應用，例如：

- 電子郵件的內容與附件的清洗與淨化
- 可攜式儲存媒體(USB隨身碟、記憶卡、光碟片的檔案交換)
- 企業官網、便民服務、線上申請、線上報修…等服務的檔案上傳之檔案檢疫與清洗淨化
- 跨網路的檔案傳輸時的檢疫與清洗淨化

跨不同安全等級網路之間的零信任資料安全

在安全的實務上，即使是同一家企業的內部網路，在網路上應該也需要將不同安全等

跨不同安全等級網路之間的檔案交換

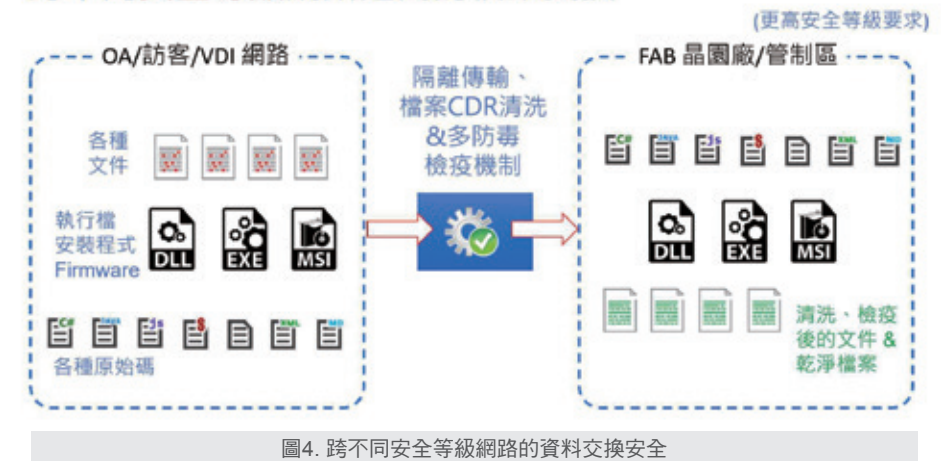


圖4. 跨不同安全等級網路的資料交換安全

級的網路進行區隔。例如，OA同仁辦公區網路、研發部門網路、晶圓廠或生產線網路…等，應該進行網路區隔，並設置網路閘道限縮存取權限，必要時還可以進行實體隔離，並且佈署實體隔離單向傳輸閘道器來進行更安全的資料交換。

當不同的網路有資料需要傳輸時，需要將零信任資料多防毒引擎安全檢疫、清洗納入規劃。由於執行檔型態的檔案，無法透過CDR檔案清洗進行處理，一但執行檔案任何一個位元組被修改，有可能會造成執行檔無法被執行。那如何確保執行檔是安全的呢？因此，如果有執行檔、安裝程式、修補軟體，需要傳送到更高安全要求的網路時，可以藉由多個防毒引擎都掃描過後才能將檔案帶到管制區網路中。依據統計，如果用8家防毒引擎檢測，偵測率可以達到84.58%，用12家防毒引擎檢測，偵測率可以達到90.53%，如果對安全有更高要求，則可以投入更多資源與成本，用更多防毒引擎來檢測，以降低殘餘風險。

針對文件型態的檔案要傳輸到更高安全性

的網路時，為了避免惡意程式被夾帶到管制區網路造成感染，可以透過CDR清洗技術，將文件中可能會被利用來感染的可執行內容進行清洗淨化，確保萬無一失。而針對要外送的檔案也CDR清洗引擎進行處理，以避免機敏資料被夾帶於無關緊要的檔案內容中，造成外洩。

總結，因應資安威脅不斷的在進化，我們的防禦觀念也需要進化調整，傳統僅安裝防火牆網路區隔，以及安裝防毒軟體掃毒的舊思維已經不足以應對這些新興的威脅。隨著物聯網、智慧製造、AIoT 的應用越來越多。要求設備不聯網、不交換資料以避免感染，已經變得不實際，因此本篇文章介紹的零信任相關的資安技術，包含上網隔離瀏覽技術(RBI, Remote Browser Isolation)，以及針對資訊與文件的CDR清洗技術(Content Disarm & Reconstruction)，這兩種零信任關鍵技術將會越來越重要，提供給各位讀者們參考。

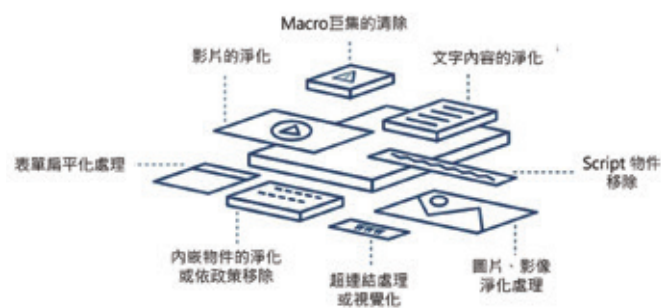


圖3. CDR技術示意圖

上市製造業公司 將安全性機制 標準化案例分享



文 Akamai

近年，國內經濟部工業局所發布的《供應鏈資訊安全管理強化教戰守則》內容統計指出，以200人以上為例的製造業者，其對於資安發展阻力的依序分別為，內部技術能量不足（41.2%）、公司對資安投資報酬率缺乏了解（40.0%）、內部員工欠缺資安意識（33.8%）。統計反映出，當要帶動智慧製造領域的新興資安技術之發展，國內製造業者需要視提升物聯網應用之資安防護能量，為重中之重。然而，當經濟轉型的速度加快，範圍擴大，傳統製造如何躍進為智慧製造場域內，製造業者該如何，除了營運的穩定之際也同時加速資安防禦部署的健全？

縱深防禦機制，夠安全嗎？！

身為全球雲端安全與平台服務供應商 Akamai經過二十多年的淬鍊，同時在台灣深耕服務台灣企業，無論是雲平台的建構、資安部署防護等，均是企業資訊IT開發人員的最佳合作夥伴， Akamai除了最深厚的全球內容傳遞網路（ Content Delivery Network CDN ）領導品牌外，資安防護技術更是深根服務，例如雲端身分識別應用程式、防網頁側錄AHP (Audience Hijacking Protector)解決方案、Akamai Bot Manager Premier 和 WAP(Web Application Protector)等。

縱深防禦的機制是透過多層級的安全保護技術，對於製造業而言，只有縱深防禦的安

全機制似乎不足夠，因為營運不中斷是OT與IT的共同共識，因此如何確保網路能持續保持運作順暢安全？Akamai專家團隊則建議，除了縱深防禦的安全機制外，還需要有東西橫軸的安全保護機制思維與工具。

Akamai專注於微分段(Micro-Segmentation)技術推出Akamai Guardicore軟體式網路區隔解決方案，透過監控Server(伺服器)東西向橫軸連通運作，運用微分段的技術加強限縮威脅風險的產生，同時增進企業網路區段的效率與安全，落實零信任的管控機制，也降低企業建置複雜過程與高成本的問題。以下，我們將分享一家已於紐約證交所上市的製造業公司，其服務範圍包含全球各地，同時也是業界的翹楚，其運用科技將網路安全

機制標準化的同時降低支出成本，創造營運的成長。

製造業個案： 導入前的現況與問題

該公司的 IT 資安團隊負責維護公司位於世界各地多處據點，其中大多數為辦公與製造的設施設備共同使用。如同其他許多企業，這家製造業公司最初選擇使用防火牆。然而，因為管理多重的基礎架構規則、個別工作站變更以及快速升級全網路的軟體，因此單一據點很快就變得曠日費時。另外，則是網路活動環境能見度雖然獲得改善，卻只侷限於特定區域，難以全面性集中檢視網路活動，以及不同資產之間的相依性。

個案的防火牆雖然能夠提供基本的區隔防護能力，卻無法解決資安團隊的隱憂-未受管理的點對點通訊。假使不解決此問題，可能導致公司暴露於傳遞資訊過程中遭受駭客的攻擊、勒索軟體入侵及其他威脅，利用端點之間橫向移動，進行惡意程式的植入、滲透，讓企業處於未知的風險當中。

解決方式： Guardicore Centra Security Platform

Akamai網路區隔專案的首席基礎架構設計師表示，為確保個案的網路強固維持於安全狀態，因此協助個案將安全性機制標準化，讓全球各地據點提供一致的保護，從開放式的平整

型網路移轉到符合最佳實務的區隔化架構，同時此解決方案亦可擴大保護範疇與能見度。

這家個案製造業公司，最終經過內部專業嚴密的評選，公司團隊決定採用 Guardicore Centra Security Platform。Akamai導入此專案的第一階段，大約部署 Guardicore Centra 於個案製造業公司的2,000 個工作站。當導入方案上線後，個案公司IT 安全團隊立刻體驗更深入的能見度，全面掌握網路與其通訊狀況，且能深入探索個別電腦的活動，瞭解整體應用程式層級的活動狀態，讓公司高層能做出更有根據的資安決策。舉例來說，有些使用者在公司的筆記型電腦上安裝了家裡印表機的應用程式。個案公司可以透過 Guardicore軟體發現其中許多這些應用程式會持續掃描公司網路，尋找支援的裝置，如判斷為異常狀況，個案製造業公司的IT團隊將可以成功阻止異常違法的掃描動作。

導入效益一： 網路動態掌握更加鉅細靡遺

個案製造業IT團隊，對於網路動態的也能更加鉅細靡遺的掌握，協助公司阻擋外部惡意程式攻擊者。例如平台部署後，Guardicore Hunt 服務即偵測到一個資產存取的檔案符合已知稱為GoldenSpy 的惡意軟體特徵。Hunt 團隊將其偵測到的威脅告知該公司 IT 安全團隊。同時也提供該公司關於感染範圍、潛在風險（符合MITRE 關於 GoldenSpy 的資訊）、鑑識資料（利用

Guardicore Insight)及關於內部調查和緩解作為的分析。最後，該公司使用 Guardicore 的原則控制功能，將感染的系統隔離，阻止惡意軟體橫向移動到其他電腦，避開一場可能會發生的資安事件。

導入效益二： 標準化、節省時間、風險降低

Akamai協助導入過程中，不影響該公司的營運運作，該公司可以持續集中建立與管理規則，包括中央控管的全球工作站規則，也能因使用者需要，彈性靈活設定例外性的規則。因此，安裝Guardicore 代理程式的電腦，除了確保一致性的安全措施，也降低組態錯誤的風險，減少延誤。同時，公司設定規則所需花費的時間也大幅改善。例如，新平台導入之前，變更防火牆的設定可能需花費數日時間，然而使用 Guardicore 新原則範

本作為出發點，即使是最複雜的使用案例，IT 安全團隊也能在一小時內建立控管機制，僅需數秒鐘時間即可套用至所有安裝系統。

結論： Guardicore 延展與開創IT營運的未來

Akamai網路區隔專案團隊表示，最初重心在於將端點網路區隔與存取的安全控管機制標準化，後續已規劃持續運用 Guardicore 處理更多的需求，對於個案製造業公司已經開始規畫將保護範圍擴大，納入伺服器與關鍵應用程式，如公司的 ERP 系統。無論日後規畫內容如何，這家製造業公司的最初專案已視為一大成功，大幅縮減攻擊表面，並降低公司工作站的風險。現在，公司更能防範從端點往端點橫向散播的攻擊，也讓公司IT團隊更放心公司的安全狀態。

關於 Guardicore

Guardicore 為全球資安從業人士提供簡單易用的 Zero Trust 網路區隔技術。我們的任務就是將高傷害的資安事件影響最小化，像是勒索軟體，同時並為您保護網路核心最重要的資產。我們能快速封鎖有害的橫向移動。從實體主機到虛擬機器與容器，Guardicore 都能保護您的所有端點、資料中心和雲端。我們的軟體式平台能幫助您強化安全性，實現公司的數位轉型。



客製化 企業包班

量身打造
培訓計畫
知識性課程
技術性課程



30% off

政府補助最低7折起
提升企業永續競爭力

/ 智動化 / 工具機 / ESG 永續經營 /
/ 綠能減碳 / 精實管理 / 經營管理 /

企業包班聯絡窗口：04-23581866#51 陳小姐 sonomi@tairoa.org.tw
04-23581866#52 王小姐 candice@tairoa.org.tw

 **TAIROA** 社團法人台灣智慧自動化與機器人協會
Taiwan Automation Intelligence and Robotics Association

Are Cybersquatters Going After the Car Manufacturing Sector?

WhoisXML API Inc

Images and data <https://drive.google.com/file/d/1XOWb0LIDWUIEC5mE0dcimwI6NqbiQoyF/view?usp=sharing>

The cyber attack targeting Toyota's top-tier supplier in February led to the loss of about 13,000 cars in production output. Aside from the quantified damage, the supply chain attack highlights how massive and scattered threat vectors can be. Covering all bases requires looking at every possible source of risk, including the Domain Name System (DNS).

In line with this, WhoisXML API researchers explored domains and subdomains bearing the names of leading car manufacturers. These digital properties could be vehicles for attack vectors, such as third-party phishing and business email compromise (BEC) scams. Our analysis uncovered:

- More than 10,000 domains and subdomains containing top car manufacturers' brand names that have been added since 1 February 2022
- Almost all uncovered cyber resources are not publicly attributable to the respective companies whose names appear in them
- Several domains and subdomains have been flagged as malicious

Feel free to download the complete list of properties and relevant data points from our website. We'll discuss our analysis and research below.

10,000+ Car Manufacturing-Related Domains and Subdomains

This research focuses on seven car companies named by Forbes as the top 10 cars and best brands of 2021. These are Toyota,

Mazda, Subaru, Kia, Honda, Lexus, and Tesla. Since Toyota's supply chain attack occurred on 28 February 2022, we limited the properties to only those added since 1 February 2022.

We uncovered 4,972 domains and 5,148 subdomains, totaling 10,120 properties. The chart below shows the distribution of these cyber resources among the companies included in this study.

Possibly Rogue Digital Properties

Distinguishing properties added by the companies themselves is an essential part of this study. If the legitimate company owns the domains and subdomains, they have control over these assets. Otherwise, the digital properties can be considered rogue that can be potentially used in brand abuse, phishing campaigns, and other malicious activities.

While companies can register domains using different registrant details, most large corporations, like the ones in this research, often use the same registrant email address and privacy protection service. As such, the registrant email addresses of the car companies' official domains can help identify potentially rogue properties.

We discovered only 10 domains that are publicly attributable to the top brands, all of which belong to Toyota. It's important to note that Mazda and Honda had redacted or privacy-protected registrant details. Even then, none of the domains and subdomains share the same attributes, such as the combined use of privacy protection companies, namerservers, and registrant countries.

Below are some examples of the potentially rogue cyber resources for each brand. You may download the complete list from our website.

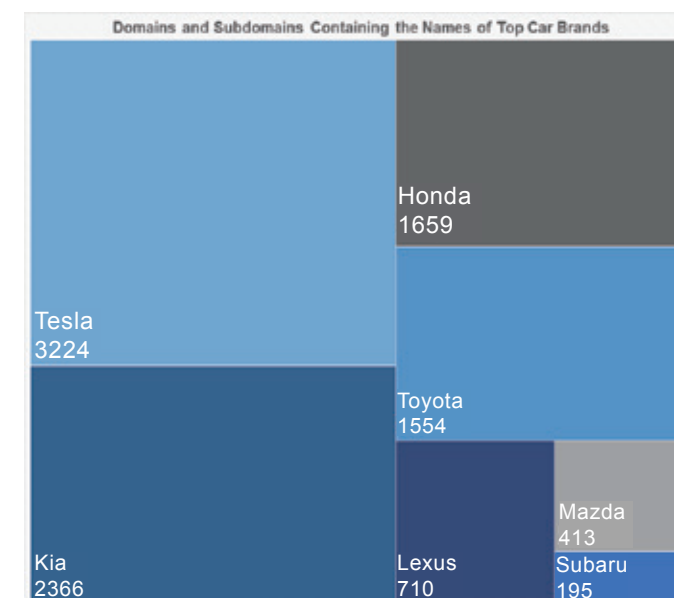
Malicious Domains Alert

There could be legitimate reasons behind

the rogue domains and subdomains. For instance, car dealerships, used car dealers, and brand enthusiasts could find it necessary to register them.

However, that doesn't discount the possibility of threat actors using the domains for malicious campaigns. In fact, we already found dozens of malicious properties despite them being newly added.

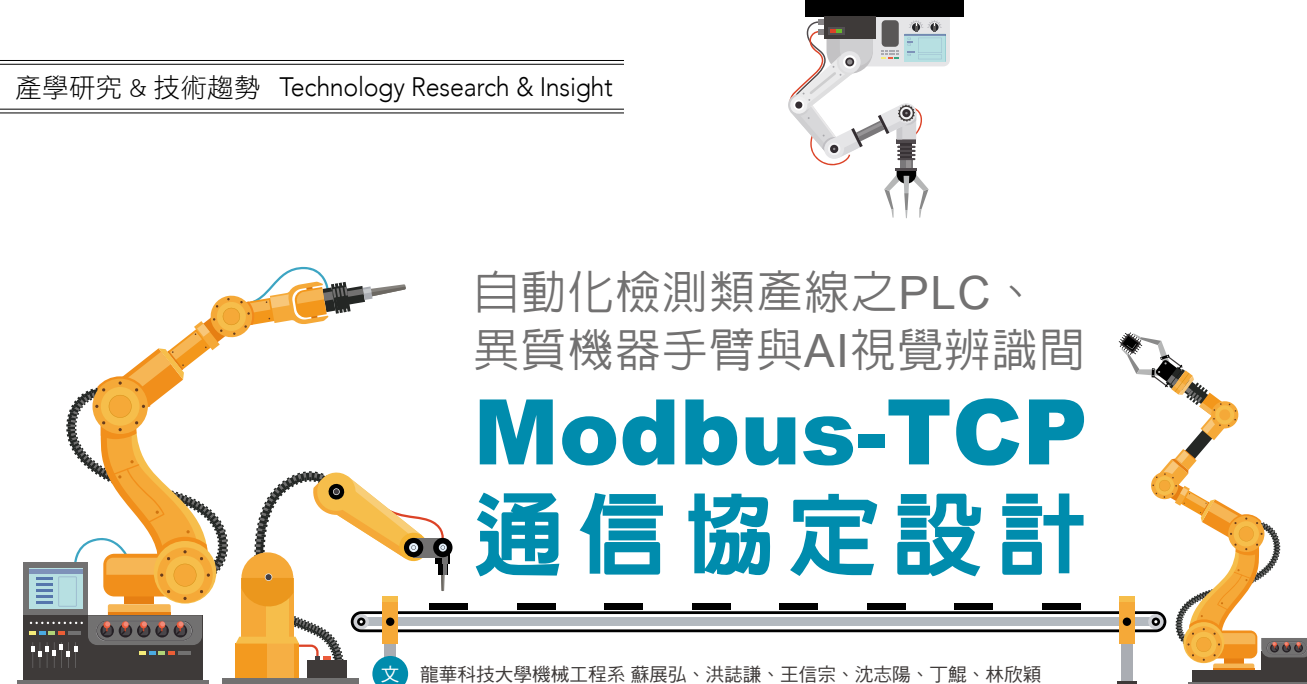
While some of the malicious domains and subdomains have already been taken down, others still hosted live content. Here are some examples of malicious domains encouraging visitors to take part in an Elon Musk project and earn US\$4,000 per month.



Brand Name	Domains	Subdomains
Toyota	- toyota[.]xn--fiqz9s - toyota[.]bar - etoyota[.]ir	- toyota[.]grupolagrajera[.]com - toyota[.]e-mobilio[.]de - toyotadpeer[.]toyotadnet[.]toyota[.]blockededge[.]dev
Mazda	- mazda[.]tk - armazda[.]ir - mazdausa[.]ca	- mazda-cx-50[.]devonline[.]me - mazdacarsmy[.]toyotaalphard[.]com[.]my 2010-mazda3[.]blogspot[.]com
Subaru	- sportsubarucars[.]com - clearshiftsubaru[.]com - tellhaddadsubaru[.]com	- wyattjohnsonsubaru[.]dsi360[.]com - subarurussia[.]users[.]photofile[.]ru - www-carsubaru-com[.]translate[.]goog
Kia	- gkia[.]shop - komkia[.]vg - vlgkia[.]ru	- www[.]cowboykia[.]phpup[.]fzinternal[.]com - kia[.]boravto-vrz[.]mss[.]7apps[.]ru - tutkia[.]plat-xxxx[.]dev[.]plattan[.]fi
Honda	- hondacars-kitachiba-newstepwgn-teaser[.]com - hondausedcrossovers[.]com - hondahonda1739[.]com	- honda[.]simpelink[.]com - honda[.]yasu[.]name - honda[.]demowebku[.]xyz
Lexus	- lexus[.]fo - elexus[.]ph - toyotalexusfinancialservices[.]lu	- autorepairyorbalingaplacentiaanaheimtoyotahondaacuralexusvw[.]spb[.]ru - lexus[.]retek[.]com - lexus[.]oempartsonline[.]com
Tesla	- teslainvestment[.]international - teslatechsolucoeseltricas[.]com - tourismehauteslaurentides[.]com	- ps-st-3344[.]schneider[.]tesla[.]aristos[.]pw - loving-tesla[.]74-208-187-83[.]plesk[.]page - tesla[.]vishwabhartiprjects[.]com

Monitoring the DNS for rogue domains and subdomains can help security teams take timely actions before they are put to use by threat actors. Early detection can help protect third parties, customers, and the general public.

If you're interested in the domains and subdomains related to the car manufacturing sector discussed in this post, you can download the research materials here. You may also contact us for research collaboration.



文 龍華科技大學機械工程系 蘇展弘、洪誌謙、王信宗、沈志陽、丁鯤、林欣穎

本文說明應用PLC整合協作式機器手臂、工業型機械手臂、3D視覺系統以及輸送帶系統，達到生產線產品檢測，達成產線智慧化。採用Modbus-TCP協議作為機器手臂、視覺系統、輸送帶與主控PLC之間數據交換。建構由台灣Vigor PLC、TM協作機器手臂、上銀工業機械手臂、Solomon-Accupick3D視覺系統、輸送帶組成的單一全自動檢測控制系統。達明協作機器手臂將待檢產品送至輸送帶、經過3D視覺檢測，再由上銀工業型機器手臂將及格產品或不及格產品分別撿放在不同的料箱中。此系統在自動辨識與分箱撿放的應用，提高效率、降低人工成本。

“

關鍵字：PLC、機械手臂、Modbus TCP、視覺影像辨識

”

一、前言

面對工業4.0時代的發展，台灣中小型製造業在提升工廠效率、精進製程自動化方面，沒有龐大的資本，一般只能在既有或新購的高異質性機器設備上進行整合，無可避免地PLC扮演著各類設備間交互通信的角色[1]。

在自動化產線中，機器手臂可逐漸取代人力，解決缺工的問題。其中，產品線上檢測可透過AI機器視覺來提升產線的性能以及取代品檢的人力[2]。本文將展示一條小型的自動化檢測系統，可利用機器手臂撿取待檢工件送到輸送帶上、輸送帶上裝有AI視覺檢測功

能，判定工件的合格與否，進而再利用機械手臂進行分箱置放。然而，要將各類不同性質的設備裝置整合成一個完全自動化的系統是一項極具挑戰的工作。此檢測系統可視為工廠生產線上的一個檢測站，用於識別有缺陷的產品。在工業製造中使用全自動系統將提高產品品質和客戶滿意度，並讓公司有更多時間培訓員工以適應快速發展的技術和先進的製造設計。

本文所展示一個小型的產線檢測自動化系統，包括Vigor PLC VS2-24MT[3]、達明協作式機械手臂[4]、上銀工業型機械手臂[5]、Solomon-AccuPick 3D AI視覺檢測系統[6]、

輸送帶等。這些設備間以ModbusTCP協定為數據通訊平台進行設計[7]，整個系統架構如圖1所示。



圖1.自動化檢測產線整合系統圖

自動化系統PLC控制之動作流程圖，如圖2所示，PLC控制達明機械手臂將物件取至輸送帶上，物件經過感測器後停於視覺下方進行檢測，PLC取得檢測結果將控制上銀機械手臂將物件夾取至正確位置擺放。使用Vigor程式編輯軟體LadderMasterS依照此流程圖編輯PLC程式[8]。

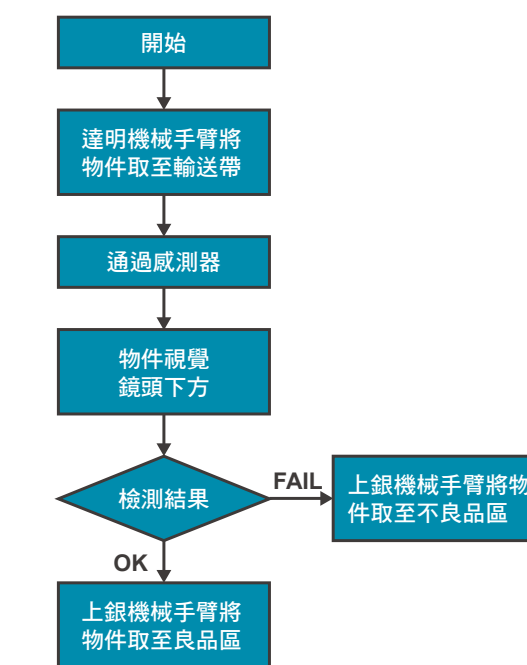


圖2.自動化檢測產線流程圖

二、PLC控制檢測智慧化程序

PLC用於自動化控制，可將已編寫好的程式匯入，並且執行程式來達成使用者所需的自動化控制。本文展示的自動化檢測系統所使用的PLC為台灣製造的Vigor VS2-24MT，如圖3所示，數位輸出、輸入各有12個點位，工作電壓為DC 24V，有兩個擴充位可根據使用需求擴充其他特殊功能模組，編成軟體為Vigor LadderMasterS[8]，通訊協定支援Modbus TCP/RTU、Non-protocol、CPU Link、ASCII。

本文使用的通訊協定為Modbus TCP，Modbus是Modicon公司於1979年為PLC通訊而發展的，現今是工業中裝置之間常用的通訊連接方式，由一個主站與數個副站所組成，主站可進行Modbus命令的發布，由Modbus命令指定的副站進行回覆。

透過通訊協定Modbus TCP與機械手臂、AccuPick 3D進行訊號傳遞，Modbus TCP為被廣泛應用的通訊協定之一，經由網路線來進行傳輸，圖4為本次與機械手臂通訊的Modbus列表，將功能類型、主站(PLC)的位址、副站(機械手臂)的位址以及資料長度設定完畢，即可對該功能進行控制。



圖3.VS2-24MT

No.	Comment	Master addr.	Slave ID	Slave addr.	Length	Modbus	Slave ID
1	H01 Write Single Coil (DO)	R1	1	0	1	DO	1
2	H02 Write Single Coil (DO)	R2	1	1	1	DO	1
3	H03 Write Single Coil (DO)	R3	1	2	1	DO	1
4	H04 Write Single Coil (DO)	R4	1	3	1	DO	1
5	H05 Write Single Coil (DO)	R5	1	4	1	DO	1
6	H06 Read Discrete (DI)	R6	1	5	1	DI	1
7	H07 Write Single Coil (DO)	R7	1	6	1	DO	1

圖4.Modbus列表



圖5.自動化產線檢測系統PLC編程

在編寫程式只使用一個外部輸入X0紅外線感測器與一個輸出Y0控制輸送帶停止，其餘皆以內部繼電器與暫存器透過Modbus TCP做連接完成目標任務。PLC程式如圖5所示，由於需持續Modbus通訊，所以使用M9000常ON接點輸出Modbus功能塊，M0為開始開關，輸出M1與M7使達明機械手臂夾取產品放置輸送帶上，當產品經過紅外線感測器後，計時1.3秒將輸送帶停止於視覺鏡頭下方，並且啟動視覺檢測，並將檢測結果存至D1暫存器中，若值為1，輸出M4正確訊號給上銀機械手臂；若值為2，輸出M5錯誤訊號給上銀機械手臂，同時啟動輸送帶計算2.5秒將產品移至上銀機械手臂夾取處，輸出M3使上銀機械手臂進行夾取並且依照PLC命令將產品移至相對應的料盤中放置，最後輸出重置訊號繼續檢測流程。所用之元件其編號與名稱，如表1所列。

實體動作與訊號傳遞如圖6所示，全自動化檢測系統的動作流程由PLC控制，整合機系手臂、3D視覺、傳輸系統，透過程式輸出訊號完成全部的檢測流程。

表1.PLC編程之元件編號與名稱

Number	Nickname
X0	Infrared sensor
Y0	conveyor
M0	start
M1	TM_DO0_start
M3	HW_SI11_start
M4	HW_SI12_correct
M5	HW_SI13_false
M6	HW_SO14_reset
M7	TM_DO1_place
M11	Launch timer 1
M13	Launch timer 2
T1	Object to vision
T3	Object to HW
C1	Conveyor stops
D0	Vision on
D1	result

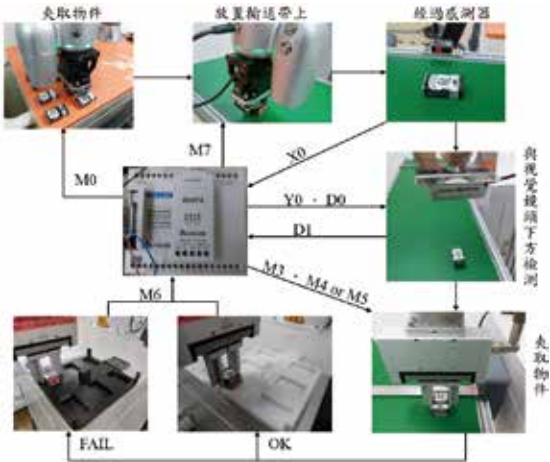


圖6.動作流程與訊號傳遞

三、智慧化類產線系統架構

1. 機器人系統

本文示範產線檢測系統所使用的機械手臂有兩種，分別為達明協作型機械手臂TM5-700與上銀工業型機械手臂RA605-710-GB。達明機械手臂將待檢測的產品移至輸送帶，進行檢測，上銀機械手臂將檢測完的產品合格與否，撿取移動至相對應正確的位置擺放。兩台手臂

皆以Modbus TCP與PLC連接，使PLC可以控制機械手臂動作的開始與結束。

PLC以Modbus TCP與兩台機械手臂連結通訊位址如圖7所示，使PLC的M(內部繼電器)與達明機械手臂的DO(Digital Output)、上銀機械手臂的SI、SO連結控制，PLC內部繼電器控制機械手臂IO功能如表2所示，PLC控制達明機械手臂DO0為夾取待測物件訊號、DO1為放置於輸送帶訊號；PLC控制上銀機械手臂SI11為夾取檢測完成之物件、SI12為良品訊號、SI13為不良品訊號、SO14為動作完成重置訊號。

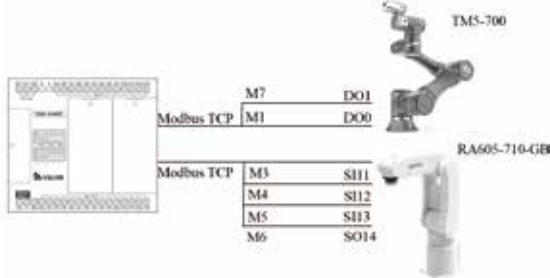


圖7.Vigor PLC與機械手臂Modbus-TCP通訊位址

Modbus-TCP通訊位址

表2.PLC連結機械手臂功能表

PLC 端	機械手臂端	功能說明
M1	DO0	夾取待測物件訊號
M7	DO1	放置輸送帶訊號
M3	SI11	夾取檢測完成之物件
M4	SI12	檢測良品訊號
M5	SI13	檢測不良品訊號
M6	SO14	動作完成重置訊號

2.3D視覺系統

機器視覺系統透過攝像頭對產品樣本進行拍照並且做機器學習，學習後由機器自行檢測產品是否有缺陷，並用於判斷並且選擇出特定的產品。本檢測產線用的視覺系統為所羅門公司的軟體AccuPick 3D[6]，本文所檢

測的產品現階段使用到2D層面就可。視覺系統所搭配的攝像頭為英特爾公司的RealSense Depth CameraD435[9]，如圖8所示。

PLC以Modbus TCP連結AccuPick 3D通訊位址如圖9所示，以PLC的D(暫存器)進行通訊，暫存器位址與功能說明如表3所示，在PLC D0位址進行通訊，當數值為1時，使AccuPick開始檢測物件。在PLC D1位址進行通訊，當檢測物件為良品時輸出1，若檢測物件為不良品則輸出2。



圖8.視覺檢測系統

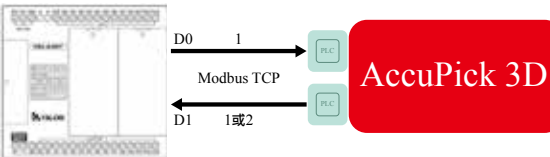


圖9.Vigor PLC與AccuPick3D軟體Modbus-TCP通訊位址

Modbus-TCP位址

表3.PLC連結機械手臂功能表

PLC 暫存器位址	AccuPick 功能塊	數值	功能說明
D0	PLC Input	1	暫存器數值為 1 時開始檢測
D1	PLC Output	1或2	良品輸出 1；不良品輸出 2

由AccuPick 3D進行檢測後將結果透過Modbus TCP傳給PLC，使PLC做後續的控制。AccuPick 3D動作流程圖如圖10所示，在流程圖的前後插入PLC功能塊，使AccuPick 3D的視覺功能與結果皆由PLC進行控制與接收。

第一個PLC功能塊做PLC Input，當PLC將D0位址的暫存器數值改為1時，才會進行後續的檢測動作，確保產品經由輸送帶傳送到位之後再進行檢測。第二個PLC功能塊做PLC Output，視覺檢測完畢後將數據透過Modbus TCP傳送給PLC暫存器D1的位址，PLC會根據回傳數值使手臂做相對應的工作。

產線檢測系統之實驗驗證，所選取的產品樣本如圖11所示，將針對物件上”龍”字做瑕疵檢測，圖中上排三個物件為正確字體，下排由左至右分別為斜體、破損、多行、缺角與被遮蔽之字體。

機器學習在Recognition功能塊進行，如圖12所示，使用Camera功能將產品樣本進行拍照後，於Annotation將所有照片中的樣本

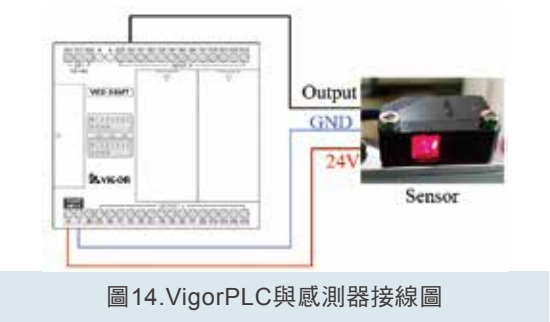
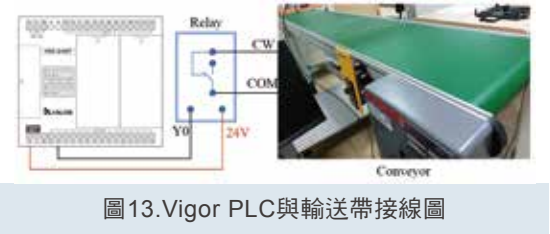


進行標註。檢測系統將樣本分為ok與fail兩個區塊，標註完成後就能進行機器學習，視覺系統會依據機器學習的結果與待測物進行比對，將待測物歸類為ok或fail區塊，並且分別輸出1與2數值給PLC的D1暫存器。

3.傳輸系統

傳輸系統是自動化系統重要的一環，主要是將產品或材料等物件透過傳輸系統在整個工廠各個工作站間運送，傳輸機械有多種樣式，如：AGV無人搬運車、皮帶輸送帶…等，本文使用的傳輸機械是皮帶輸送帶，如圖13所示，此皮帶輸送帶可以控制轉動方向、運轉速度以及輸送帶的啟動與停止，輸送帶有三個接點分別為CW、CCW、COM，只要將COM點與CW相接就可使輸送帶運轉(CCW為反向)，將CW與COM接於繼電器常閉接點，使輸送帶持續運轉，訊號接點與PLC Y0相接，當PLC輸出Y0使繼電器切換，即可使輸送帶停止。

在輸送帶上加裝如圖14之紅外線感測器，此感測器為OMRON回歸反射型E3Z-R61[10]，使物體經過感測器後回傳訊號給PLC將輸送帶停止。紅外線感測器為三線，分別為火線、地線與訊號線，感測器使用24V工作電壓並且將訊號線接至PLC的X0位置。



四、 結論

本文以PLC透過通訊協定Modbus TCP將機器人系統、3D視覺系統、傳輸系統整合成一個全自動化檢測系統，以全自動化系統來檢測產品，藉此提高產品品質與檢測效率，完整的檢測系統如圖15所示。

目前雖使用2D充分可用，未來可朝3D視覺系統推動，相對於2D視覺X、Y方向的測量，3D視覺更多了Z方向的資訊，不再侷限於平面的測量，使檢測的範圍更加廣泛，在市場更



佔有優勢，並且以此形式加入更多得機械、工具機與系統，使得此全自動化系統得應用範圍更多元。

本文也嘗試使用AB PLC來控制，但在與AccuPick 3D通訊時出現問題，AccuPick 3D在Modbus TCP的參數中Register欄位只能設定於暫存器D的位置進行通訊，但因AB PLC的軟體表示方式不同，當通訊成功也找不到暫存器的位置，無法透過Modbus TCP的方式與AccuPick 3D進行通訊，此部分仍繼續進行中，使PLC之應用更多元化。

五、 致謝

本文感謝豐煒科技所提供的PLC控制器與技術指導、台灣智慧自動化與機器人協會(Taiwan Automation Intelligence and Robotics Association)贊助之所羅門AccuPick視覺軟體，以及美國特拉蒙機器人公司(Telamon Robotics)之計畫經費贊助，得以讓本文順利整合完成，特此致謝。

參考文獻

1. Online Technical Training Blog, How smart factories integrate PLCs, automation and robotics, George Brown College. <https://www.gbtechtraining.com/blog/how-smart-factories-integrate-plcs-automation-and-robotics> Accessed on May 24th, 2022.

2. Alghamdi B, Lee D, Schaeffer P, Stuart J, An integrated robotic system:2D-vision based inspection robot with automated PLC conveyor system, Proceedings of the 4thInternational Conference of Control, Dynamic Systems, and Robotics (CDSR’ 17), Toronto, Canada, August 21-23, Paper No. 136, 2017.

3. Vigor VSI-24M User Manual, <https://www.vigorplc.com/en/product-c93722/Main-Unit.html>Accessed on May 2nd, 2022.

4. TM5 Hardware installation manual, HW3.2, Rev. 1.04, TECHMAN ROBOT INC., 2021

5. HIWIN Technical Support Download Center, RA605 Articulated Robot, https://www.hiwin-support.com/Download_center.aspx Accessed on May 26th, 2022

6. Solomon Accupick Operating Manual English, Ver.2.6, Solomon Technology Cooperation, 2019.

7. Meng F, Zhang Y, Yang D, Design of communication among vision system, PLC and industrial robot based on Modbus-TCP protocol, IOP Conference Series: Journal of Physics: Conference Series, 1288, 2019.

8. Vigro Programmable Controller, VS series Programming software “Ladder Master S V0.81” , May 13th , 2022. <https://www.vigorplc.com/en/news-45202/VS-series-Programming-Software-%E2%80%9CLadder-Master-S-V0-81%E2%80%9D-please-download-here-to-update.html> Accessed on May 24th, 2022

9. Intel REALSENCE,Depth camera D435, <https://www.intelrealsense.com/depth-camera-d435/>Accessed on May 2nd, 2022.

10. OMRON Industrial Automation, E3Z-R61,<https://www.ia.omron.com/product/item/711/> Accessed on May 24th, 2022.



移印製程提昇之 相關因素研究

文 萬能科技大學車輛工程系助理教授 周國達教授
翊揚能源科技公司工程師 王士榮

隨著電腦、通訊、以及消費性電子產品的多樣化發展，塑膠材料更被廣泛的應用，而外觀改善所需的加飾技術也不斷的演進。由於移印的承印材料廣泛、印製作業特殊性，有別於一般的印刷方式，移印油墨厚度的轉移更應依據產品特質作適當的調整，使得移印版深度的控制更顯得重要。唯目前國內移印製版作業並未建立標準模式來控制移印版深度的穩定性，製版作業人員多利用主觀經驗作為評斷標準，因此本研究目的希望能透過實驗，針對影響移印附著力及移印製程相關因素與工具設備穩定程度的考量進行探討，以獲得高良率的製程。

關鍵字：移印、附著度

壹、前言

因應世界環保潮流，移印工業走向環保品質的印刷，其產品趨向少量多樣化之高，附加價值。移印是特殊印刷技術，由於其在小面積、凹凸面的產品上面進行印刷具有非常明顯的優勢，彌補了網版印刷的不足。移印技術應用於電子、塑膠、禮品、玩具等範圍，移印技術和網版印刷作為主要的裝飾方式更是得到超越的發展，根據統計移印技術和網版印刷技術在上述行業的應用分別達到27%、64%、51%、66%。移印指被印物為不規則的曲形表面（如儀器、電氣零件、玩具等），使用銅或鋼凹版，經由矽橡膠鑄成半球面形的移印頭，以此壓向版面將油墨轉

印至承印物上完成轉移印刷的方式。移印機適用行業：塑膠業、玩具業、玻璃業、金屬業、電子業、體育用品、文具業、光學業、IC封裝業等。移印機適用範圍：尺、筆、球形物、洋娃娃眼睛、手錶、照相機、吹風機之外殼、陶瓷、醫藥器具、球拍、錄音帶、電子零件、IC、CPU、DRAM、電腦外殼、按鍵、裝飾標誌、手機機殼等之印刷。【1】。在3C的各種產品中一般來說整體外觀的設計絕大部分使用塑膠材料做為產品助要外觀的材質住要原因有二：第一因為材料較便宜且結構較強；第二，塑膠材料重量比起其他第金屬較為輕盈因為這兩重要元素，所以塑膠材料成為大部分電子產品外觀機殼之材料選擇，雖然塑膠材料具有這樣重要優點，但

是有一項重要缺點，就是塑膠材料缺乏外觀設計上最重要的一項必備條件「質感」，為了克服這個缺陷，塗裝技術就成為解決塑膠材料質感這個缺點重要技術。而所有的產品都具備外觀上之設計，除瞭型式設計上需運用模具成形技術與噴塗塗裝製程外，如果在外觀上又文字或是圖案表現需求時，印刷技術就被廣泛運用。在立體外觀設計中住要包含兩種製程：塗裝（Painting）和印刷技術（Printing Technology），印刷領域最常應用地技術有網版印刷、移轉印刷與轉寫印刷，於工作中接觸熱轉印、水轉印、移印、網印、無膜標轉印、曲面印刷，雖然都是方式上的不同，但是所涉及的專業知識與技術是全然不同。就油墨特性而言，耐熱性、親水行、乾燥速度、延展性…等；就被印物材質來說，紙類、塑膠類、橡膠類、金屬類等，涵蓋範圍更為廣泛；將這些基本性質加上色彩應用科技，如此產品的外觀會顯得更多采多姿，更期望將研究成果實際應用於業界，製造雙贏價值為目標。【2】針對影響樹脂移印版印紋網孔深度形成的因素進行探討，建立一套掌控印紋網孔深度的方式，以增進移印製版品質的穩定性，俾提供移印業者作業管控的參考。本研究的重要結果與發現：1、樹脂移印版印紋網孔深度廣泛，實驗處理深度值介於14至77 μm之間，足於應付各類移印作業的印紋深度所需。2、印紋深度與前露光時間增加呈反比，也與網屏線數增加呈反比，製版時可利用減少前露光時間或換取較低的網屏線數底片以增加印版印紋深度。3、兩實驗因子對印紋深度控制有交互作用存在，隨著前露光時間的增加，網屏線數增加對印紋深度值減少的影響愈不明顯，甚至當前露光時間增加至6秒、8秒時，網屏線數的增加對印紋深度值的減少幾乎沒

有影響。同時，隨著網屏線數的增加，前露光時間增加對印紋深度值減少的影響也愈不顯著。【3】針對樹脂版的版紋深度與被印材質表面達因數在移印的製程中，其產品的附著度之探討。研究的結果發現：一、表面達因數越高則附著度越高，附著度與達因數有正因果現象存在。二、版紋深度越深則附著度越低，附著度與版深有負因果現象存在。三、版紋深度與表面達因數對產品附著度有交互作用存在。四、產品附著度的最適化產品附著度最適化為控制版紋深度在20 μm 與30 μm 之間，而被印材質表面能達38dynes/cm²，關聯方程式為附著度 = 17.449 * 達因數 - 7.394 * 版深 + 36.616。【4】主要探討塑料、塗料，與無膜標轉寫印刷所用油墨間交互作用，將其原來特性或本質都是不相關聯，甚至於個別型態上也有固液體差異諸材料，經過深度分析測試及整合。研究結果成效如下：一、可撕膜膜厚實驗將膜厚控制在30 μm~50 μm之間。二、將透明油墨的網目數由250目改成200目。三、硬度為55°的刮刀作為使用工具的最佳狀態。四、密閉對流式烘爐為烘烤設備的最佳選擇。五、使用塑膠合金能夠強化塑膠結構的強度與特性，對於耐溶劑性、耐候性、耐衝擊性與熱變形溫度上，都有加強塑膠合金的物理與化學特性。【施位翰】【5】刮刀在網版印刷上是一個簡單，但卻相當重要的工具。Young M. (1988)認為刮刀至少含有8項變異數，可以影響或控制印刷的階調表現，硬度便是其中一項。對於線條稿，因為油墨透過量的多寡對於滿版濃度的影響並不大，然而對於半色調網點，其網點整合濃度受到油墨厚度、網點面積百分比的影響，所以其網點整合濃度變化比較大，為了維持其濃度的穩定，以達到品管的目的。本研究以刮刀硬度的變化，探

討硬度對印刷品階調品質的影響，包括：網點整合濃度、階調曲線、網點擴大及印刷反差。獨立變數為刮刀硬度，依變數為網點整合濃度。並獲得下列結論：1 刮刀硬度值對各階調印刷網點整合濃度、網點擴大及印刷反差有顯著影響。2 刮刀硬度值對各階調印刷網點整合濃度、網點擴大有顯著負相關，印刷反差則有顯著正相關。3 在不同刮刀硬度值作用下，印版-印機曲線皆呈S型和理想中的印版-印機曲線的U字型有相當大的差異，研究發現，硬度在67.43o以上，曲線變化有規則性。在 67.43o以下，則各曲線有相當大的差異。刮刀硬度值在（67.43～82.7o）之間，其印版-印機曲線，隨著硬度升高，而逐漸下降，且曲線的形狀類似，所以相當穩定。4 刮刀硬度值在（67.43o～82.7o）之間，其各階調網點整合濃度、網點擴大、印刷反差之變化穩定性較佳，符合網版印刷須求。雖然硬度最大的93.27o的印版-印機曲線最符合階調品質之要求，但是卻不符合其它印刷品質的要求。5 另外發現：由於刮刀8項變異數交互作用，使得網點擴大最大點，隨著刮刀硬度由小至大，由50%處轉移到60%。而在硬度值67.43o 以後，即固定於60%處。6 迴歸模型最佳為： $y = b_0 + b_1x_1 + b_2x_2 + b_3x_3 + b_4x_4$ 。

貳、移印技術

1.移印原理

移印的特色在於異形立體凹凸的表面進行印刷，尤其是在小面積且有不規則曲面形狀的物品，具有不可取代的優勢。在日常生活中所使用的物品都是泛用塑膠材質，包括兒童玩具、化粧品容器、食品包裝、電器零件、醫藥用品、家庭用品等。移印技術的理

論基礎源自於網版印刷與橡皮圖章的組合方式，是獨特的印刷工藝。早期使用銅版腐蝕圖文區類似於照相凹版的印刷過程，近年來由於材料與技術的進步，使得圖文區的腐蝕印版表面，將油墨塗佈後經刮刀擦拭乾淨類似於網版印刷。移印並不是直接將圖文轉印，而是經上壓後由移印膠頭蘸凹印版之油墨印紋轉移到被印物上。相類似於橡皮圖章的印刷方式，最主要的不同點是移印膠頭僅轉移圖文影像，而不是直接印刷將圖文印在被印物。

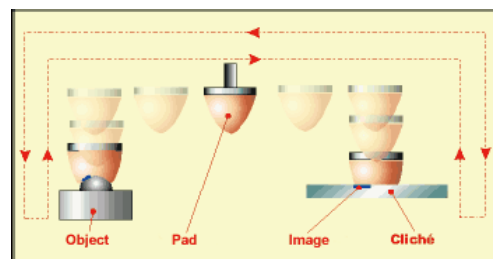


圖1.移印技術之圖文轉印示意圖【6】

2.移印機的分類

移印屬於特殊印刷的一種，其利用可變形與被印物相符的移印頭，將移印版上之圖文轉移至被印物上，在立體凹凸表面和化粧品印刷上佔有重要的市場地位。一般移印機的分類依傳動和印刷色數多寡兩種方式來區分，說明如下：

（1）傳動方式

依移印機的傳動方式，主要可分為機械式傳動移機與氣動機式傳動移印機兩類。

由於氣動式傳動移印機具有結構簡單、操作簡單、運動平穩等方面之特點。是目前移印機市場的主流。

（2）印刷色數

在移印的製程中所完成的印刷色數多寡可將移印機分為單色移印機、多色移印刷機和多色移印機等。

3.移印機的油墨系統

所有的移印機的油墨系統有兩種操作原理：一種開放式的原理，另一種封閉式的原理，以下是流程的步驟。

(1)塗佈(Flooding)圖文的轉移是印版的腐蝕下凹印紋所承載的油墨，是安裝於移印機上的凹版表面塗佈些許的油墨。

(2)刮平(Doctoring)將凹印版表面多餘的油墨刮刮平，僅留下圖文區的油墨，其表面的溶劑會蒸發。

(3)蘸起印紋(Image pick up)移印膠頭向下動作蘸起印紋。

(4)印紋轉移(Print stroke)移印膠頭往上運動，使得印紋轉移至移印膠頭上。

(5)印墨存取(Ink deposit)移印膠頭的圖文區向下動作承印在被印物上。

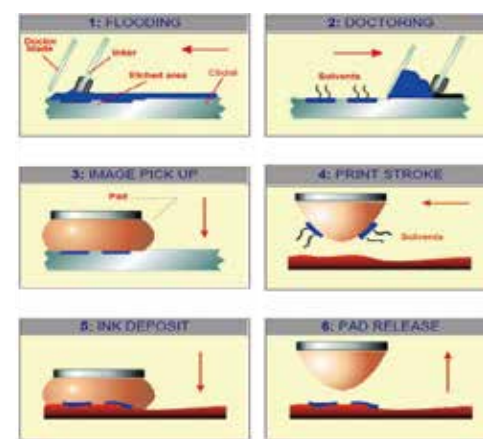


圖2.開放式移印機工作流程【6】

(6)、移印完成(Pad release)移印膠頭往上運動完成印刷，並清洗膠頭而離開；預備下個工作流程。

封閉式系統中，油墨是在容器盒內，位置於凹印版圖文區上方。通常類似於開放式系統刮刀的功能。

4.印刷油墨類型

（1）溶劑型油墨

移印油墨與網印油墨相似，但網印油墨不會快速揮發，否則油墨會在網框裏乾透。移印油墨則需要高度揮發的功能，使油墨能輕易黏上及離開膠頭，具有良有的脫墨能力。在移印技術中以溶劑型油墨為主，其油墨成份包括樹脂（20%）、顏料（17%）、溶劑（60%）、添加劑（3%）。

（2）水性油墨

塑料水油墨是由水性樹脂、助劑、顏料、水等原料組成，在選用材料時，均符合環保要求，生產過程中全部使用純淨水代替有機溶劑。水性油墨不易燃、無味、無毒等優勢，是目前最環保的印刷油墨。水性油墨主要應用Flexo 與凹版印刷中，範圍在食品包裝、煙酒包裝、藥品、兒童玩具等。

（3）UV 油墨

UV 油墨是指在紫外光照射下，利用不同波長和能量的紫外光使油墨連接劑中

的單體聚合成聚合物，其墨膜具有良好的耐磨、耐蝕、耐候等特性。UV 油墨主要應用於平版、Flexo、凹版、網版，目前也逐漸進入移印油墨市場。

各種印刷技術與材料中，應用於不同的被印材質需要有不同的表面能。印刷的過程中油墨的表面能必需大於被印材質的表面能，才能獲得良好的附著度。以使用網版印刷與被印材質聚丙稀為例，不同油墨類型所需的被印材質表面能也不同，如2-2-1所示，UV油墨＞水性油墨＞溶劑型油墨。

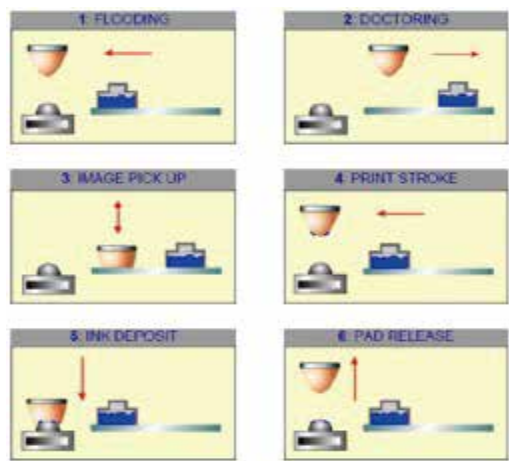


圖3.封閉式移印機工作流程【6】

參、研究問題

本研究應用樹脂凹版在移印過程於聚丙稀材質上所呈現的印刷適性，探討版材深度與被印材質表面達因數對產品的品質特性相關性分析。在移印的過程中，所考慮的各類的相关因數，包括移印機、移印膠頭、油墨類型、刮刀硬度、印刷壓力、版材種類、被印物材質、廠房濕度等。在移印製程中不同變數提出研究問題如下：

(1) 前后蓋移印制程附著力NG改善（如圖4所示）

- 1.油墨、稀釋劑、硬化劑配比及油墨使用時間
- 2.移印機穩定性、隧道烤箱穩定性（立式烤箱溫度穩定性）
- 3.作業人員穩定性（品質意識）

- 4.油墨、稀釋劑、硬化劑儲存條件（車間環境）及烘烤時間。
- 5.調油墨工具（攪拌方式）及油墨調配方式、印刷部位清潔方式。

(2) 前后蓋移印制程改善案（如圖5所示）

- 1.機器：立式烘烤箱溫度不穩定（烘烤隧道溫度不定）、機器穩定性不夠（機器運行中振動大、氣壓不穩定）。
- 2.人：人員未定崗、品質意識不強、人員心態不端正、執行力差、工作不認真、人員技能不熟練、勞動強度大。
- 3.環境：車間溫/濕度高、全檢/自檢區燈光不達標、車間灰塵大、擦完膠水的抹布亂丟、指套/手套臟污法：作業手法不正確、移印輔助用品未密封放置、作業標準不統一、產品表面清潔手法不正確、油墨調試方法不正確、烘烤箱溫度未點檢。
- 4.料：來料變形、來料臟污、漏工序、治具磨損嚴重、產品碰傷。

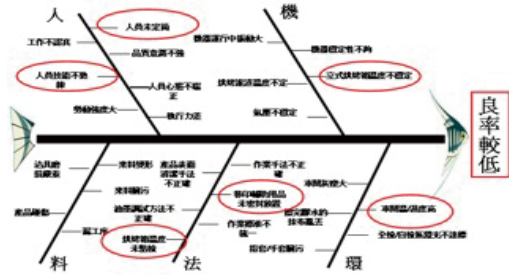


圖4.前后蓋移印制程附著力NG改善原因分析

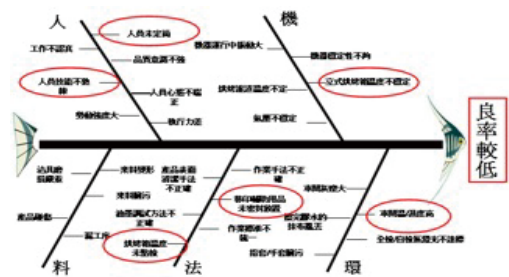


圖5.前后蓋移印制程附著力NG改善原因分析

肆、研究範圍與限制

4.1研究範圍

本研究主要探討在移印樹脂版之適性，版紋深度與被印材質表面達因數對於產品的附著度之檢測。移印大多運用在線條、套色及單色塊的印刷，目前移印業者著重於產品的附著度，在圖文層次的彩色印刷著力甚少。移印工業乃屬於勞動密集產業，企業為了降低生產成本，使用銅版或鋼版作為版材，其製版藥水具有毒性，危害人體健康以及影響生態環境。影響產品的附著度的因素繁多，本研究針對版紋深度與被印材質表面能為重點，其餘例如：印版種類、移印膠頭、油墨類型、刮刀、印刷壓力、乾燥設備等，不在研究範圍內。

4.2研究限制

實驗過程中，為了確定各項製作設定的可利用性與延用性、研究限制如下：

- (1) 印刷油墨以原廠商所提供溶濟型油墨。
- (2) 產品的圖樣設計僅限於單色塊區域。
- (3) 版材的製版條件依作業流程標準程序。
- (4) 移印機的作業包括移印膠頭的形狀、大小、硬度等依標準作業實施。
- (5) 實驗場地以溫溼度控制，生產作業流程皆為恆溫恆濕的環境。
- (6) 產品測試依同一測試條件下進行。

伍、移印適性

5.1、硬度測試

檢驗被印材質墨膜厚度的性質，以硬度實

驗來測試其墨膜表面硬化程度，以鉛筆硬度具有簡單、便捷的特點，所以這種方法在檢測時最常用。用於測試用的鉛筆包括從最硬的9H 到最軟的9B，H 代表硬，B 代表黑，HB 代表硬和黑的鉛筆。最硬的是9H，依次為8H、7H、6H、5H、4H、3H、2H 和H。F 表示中等硬度；然後依次為HB、B、2B、3B、4B、5B、6B、7B、8B、9B 是最軟的鉛筆。測量墨膜表面硬度之抗刮性，應用於實驗分析或控制生產品質。

5.2耐磨性測試

墨層的耐磨性檢測是一種比較柔和的耐磨檢測方法。檢測原理是通過一個具有特定重量（通常是175g）的物件把自身重量通過一個橡皮輪傳遞到接觸被測物件的紙帶上，最後由紙帶對被測物件進行磨耗測試。測試的結果由磨穿墨膜底部時紙袋累計走過的圈數表示。

5.3耐候性測試

產品或印刷物件受自然環境之影響中，對於陽光、臭氧、雨霧、度及溼度退。

色或老化等抗性，可採耐候測試機在短時間之內測得產品之褪色、老化、剝離及接著度，以達到高品質的要求。適用於航空工業、造漆工業、塗裝工業、汽車工業、塑膠工業、印刷工業等。

全球使用最廣泛的耐候試驗機為QUV 紫外燈老化試驗機，應用再現陽光、雨水和露水所生的破壞，通過將待測試產品放在經過控制的陽光和溼氣的交互循環中，同時提高溫度的方式來進行實驗。QUV 採用紫外線螢光燈模擬陽光，同時通過冷凝或噴淋的方式模擬溼氣影響，主要測試產品物件的粉化、開

裂、脆化、強度、氧化等性能，只需要幾天或幾周的時間就可以再現戶外需要數月或數年所產生的破壞程度。提供的數據資可對產品的耐候性作出準確的相關性預測，有助於材料及配方篩選、優化。

5.4附著度

塑料包裝印刷是伴隨著社會商品經濟發展的，在現代的經濟生活中成為重要的組成，塑料包裝商品的消費量作為國家工業水平的重要指標，發展重點是塑料包裝基材和複合包裝材料。泛用塑膠材料之聚丙烯屬於非極性分子，表面張力小，惰性強，不易接受油墨的浸潤，所以印刷前都要進行被印物的表面電暈處理或火焰處理，才能獲得良好的附著度。

Cross-Cut method 是測試塗層附著力最簡單的方法，單層、多層的墨膜均適用。使用標準薄規及刀片，在漆面作 90 度交叉切割，即可評估附著力是否合於標準。又稱「方格試驗機」、或「百格試驗刀表面處理是廣泛用於對塑膠材質以提高表面能來改進油墨、油漆、連接劑及塗料的附著力。它被廣泛採用的原因是效果好、能控制及便於掌握。塑膠表面層之交聯結構比其內層之交聯結構減少，因此其表面層的功能團有較高的移動性。所以，在儲存中，隨著時間的增長，有些塑材會出現表面處理效果的衰退，添加劑由內部向表面遷移，也是使表面能下降，影響附著力的因素。表面處理是改變不少非吸收性基材表面特性的一種有效手段，能使油墨有更好的濕潤及附著性能，即所謂可濕性。這就是諸如油墨、底膠、塗料等對塑膠材質附著的基礎。可濕性決定一種液體在一種固體表面上的展延性。水滴在親水性表面就展延成一薄水層，而在親油性表面卻形成

小水滴。水滴外表層的切線與固體表面間所形成的接觸角，即表示該表面潤濕性能的強弱，接觸角越大，潤濕性能越差。

陸、研究設計

移印技術中的版材選用繁多，本研究採用環保版材樹脂版，由於版紋深度與被印材質表面能為影響產品印刷品質的關鍵因素，尤其是對印紋附著度的變化。影響移印機的印刷品質因素包括選用的油墨、版材的種類、移印頭的形狀與硬度、刮刀硬度、印刷壓力、乾燥設備、廠房的 溼度、被印材質的表面處理等。本實驗研究中操控樹脂版的版紋深度變化與被印材質的表面達因數變化兩項因子，在相同的印刷條件下，以不同的版深度和不同的表面達因數，產生印刷品附著度的變化。

第一節 研究方法

本節主要在探討樹脂版的版紋深度與被印材質表面對於產品附著度之製程分析，在工程領域中，對新產品的設計、製程開發及製程改善上，實驗設計扮演著一個重要的角色。

6.1實驗設計

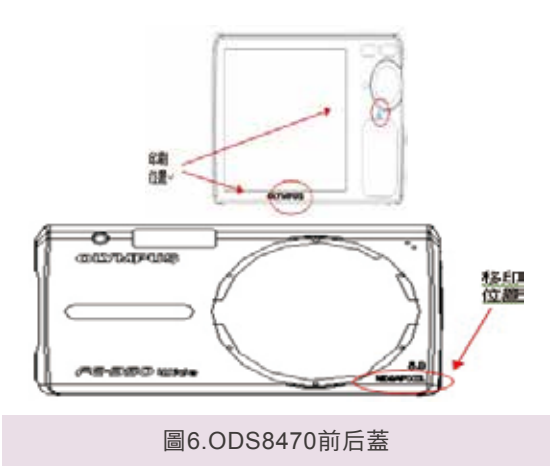
本研究是以ODS8470前后蓋（如圖6所示）移印制程附著力NG進行改善，針對膠帶剝離測試NG以提高附著力，並提出移印性能測試要求（ALL金屬外殼印刷測試）如下說明：

移印性能測試測試要求：

（一）膠帶剝離試驗

使用設備：

耗材（膠帶(NICHIBAN x18mm寬）



試驗方法：

- 1.取待測物印刷面。
- 2.取相同位置進行3回膠帶剝離測試。
- 3.取NICHIBAN膠帶貼附待測試位置上，以指腹推平氣泡。
- 4.對印刷面快速以90度急速剝離。

判定基準：印刷面不得沾起，印刷字體不得斷裂。

（二）耐溶劑試驗

使用設備：

- 1.治具：1000g負荷治具。
- 2.耗材：酒清(乙醇99.7%)金屬品印刷使用。
- 3.去漬油：塗裝印刷使用。
- 4.人工汗液：印刷使用。
- 5.鏡頭紙、白綿布。

試驗方法：

- 1.取待測物各塗裝面(把手部份優先)。
- 2.取白棉布包覆在1000g砝碼上，再沾上人工汗液，對待測物相同面進行10回往復移動。
- 3.取鏡頭紙包覆在1000g砝碼上，再沾酒精，對待測物相同面進行10回往復移動。

- 4.剪下白棉布及鏡頭紙摩擦部份，貼於表格上。

判定基準：1. 印刷部份不得模糊或脫落，或原印刷字體斷裂。

（三）硬度試驗

檢驗被印材質墨膜厚度的性質，以硬度實驗來測試其墨膜表面硬化程度，以鉛筆硬度具有簡單、便捷的特點，所以這種方法在檢測時最常用。用於測試用的鉛筆包括從最硬的9H 到最軟的9B，H 代表硬，B 代表黑，HB 代表硬和黑的鉛筆。最硬的是9H，依次為8H、7H、6H、5H、4H、3H、2H 和H。F 表示中等硬度；然後依次為HB、B、2B、3B、4B、5B、6B、7B、8B、9B 是最軟的鉛筆。測量墨膜表面硬度之抗刮性，應用於實驗分析或控制生產品質。

使用設備：

- 1.試驗設備：鉛筆劃線試驗机(HEIDON-14) 如圖7所示。
- 2.耗材：鉛筆(三菱MITUS-BISHI)。
- 3.F、H，1000g法碼(鉛筆負載)。
- 4.白色橡皮(PENTEL)。
- 5.使用研磨沙紙(2000號)。

試驗方法：

- 1.鉛筆只削木部份，露出3mm的圓柱狀筆蕊蕊的尖端以研磨紙打磨平。
- 2.向印刷表面，使鉛筆蕊的邊部立起45度，並加重1000g法碼在鉛筆蕊邊部。
- 3.鉛筆行進速度：75mm/min,向前推動10mm，然後以橡皮擦拭後，觀察刮痕(滑下線前，先確認筆尖平頭直角)印刷面只滑線1條*10mm。

附注：硬度測試是要對素材材質定義區分測試：1.素材材質為PC、PC+G是用H鉛筆。2.素材材質為PC+ABS、ABS+G、ABS是用F鉛筆。3.金屬品加印是用H鉛筆。

- 判定基準：
- 1.鉛筆硬度測試印刷字體表面不可斷滑或缺滑脫落。
 - 2.測試後字體表面無刮痕則判為OK。

附注說明：鉛筆落下點如有刮痕，不記入判定。



圖7.表面硬度計 ZSH2090

柒、移印實驗設備

(一)移印機（pad printing machine）如圖8所示。



圖8.本研究之移印實驗設備

本機採數位化微電腦觸自動偵控測控制系統，分離式油墨盤及動動式刮刀組可獨立調整。適用範圍：塑膠產品、玩具、手錶表面、電子產品、文具用品、金屬成品及陶瓷玻璃製品等凹凸不平之表面印刷。機構部位說明：1.電腦控制板2.機體3.印頭架4.刀夾5.鋼板放置處6.油墨槽7.操作平台8.工作台升降平台9.絲杆10.腳制開關

1.移印機的工作原理：移印是利用凹版的印刷原理:即將凹版上全部塗上油墨后，用刮刀和墨杯刮掉高面空白部分的油墨，僅剩下凹面的圖紋部分油墨，再用硅橡膠制作的移印頭施以壓力，粘上油墨，然後再轉印到承印物上。移印機是主要的設備，其中移印頭起著轉印的作用，因此移印鋼板,移印頭和移印油墨構成了移印工藝的三大要素，移印的過程是由移印機自動完成的。移印機膠頭的制作原理：移印膠頭是利用室溫硫化硅橡膠在硫化劑等的作用下交聯成網狀結構的彈性體的原理制作而成的。

2.移印機膠頭的制作原理：移印膠頭是利用室溫硫化硅橡膠在硫化劑等的作用下交聯成網狀結構的彈性體的原理制作而成的。

捌、結論與建議

8.1結論

壹、前後蓋移印制程附著力NG改善、改善效果：改善前從1/8量產至1/11出貨全檢段每批抽檢均有字符脫落現象。生產不穩定，影響交貨進度，改善后從1/12至1/16出貨全檢生產前蓋13982PCS後蓋10937PCS，對產品進行100%剝離測試，無字符脫落現象。生產穩定，可按時交貨。

二、標準化：

- 1.作業內容規範化----制訂標準作業文件，指導生產改善作業手法。
- 2.操作熟練化----依標準文件對生產人員進行培訓，提高作業人員操作技能。

8.2前後蓋移印制程改善案

一、通過以上的問題點分析，發現我們仍有很大的改善空間，依照最初的客戶需求計畫，製定出了我們的改善目標。（1.ODS8470前蓋產能由300PCS/H提升至350PCS/H. ODS8470后蓋產能由200PCS/H提升至250PCS/H。2.ODS8470前蓋良率由95%提升至99%ODS8470後蓋良率由93%提升至95%）。

二、改善投入:

¥ 22,80，人工成本Cost Down:¥ 7136，報廢成本Cost Down:¥ 95121，改善成果：Cost Down總金額:¥ 99977。

三、無形績效：

提升員工作業價值、生產品質較為穩定無客訴發生、提升移印加工製造能力。

四、標準化：

- 1.規範各製程作業標準和方法，同時納入SOP管控的範圍內。
- 2.與周邊單位溝通並達成共識製定治具與設備保養及點檢計畫。
- 3.對於每次的試樣都有記錄存在，以便查找差異。
- 4.定期做GRR與技能鑒定考核，對於技能不足的人員利用生產空餘時間進行教育訓練。

參考文獻

1. 1王守鴻，”印刷 中的UV和EB油墨”，印藝，第7期，2003。

2. 鄭榮一”影響樹脂移印版網孔深度形成的相關因素分析”國立臺灣師範大學圖文傳播學系，碩士論文2004。

3. 黎定南”感光樹脂版於聚丙烯之移印適性研究”世新大學圖文傳播暨數位出版學系碩士論文，2008。

4. 莊萬歷”塑料塗裝無膜標轉寫印刷適性之研究”世新大學圖文傳播暨數位出版學系碩士論文，2007。

5. 施位翰”網版印刷刮刀軟硬度對印刷品階調影響之研究”文化大學造紙印刷研究所碩士論文，1995。

6. Pad Printing，民100年1月20日http://www.tosh.it/English/tam1e.html。

AI 優質即戰力企業最愛 視覺人才暑期特訓營



數位化，人工智慧（AI）、物聯網（IoT）、巨量資料（big data）、雲端運算（cloud computing）的技術日新月異，應用已無遠弗屆，而這些技術都需要機器人這個載具來呈現。另，這幾年因COVID-19疫情及少子化等問題，也促成智慧自動化及智慧機器人需求激增。因此廠商非常需要培養更多有能力的人才，來操作機器人並應用AI技術達到智慧化生產等，所以今年智動協會選定，AI智慧機器視覺應用技術人才為暑期特訓營的主題。

機器手臂的視覺在生產製程上與運動控制系統進行整合來達到自動化目的，其中視覺感測器更是最具關鍵性的感測來源之一。加上愈來愈多的人工智慧（AI）深度學習模型，正極度擴展機器視覺的能力，快速增長的能力正引領朝智慧工廠與工業4.0轉型。機器視覺技術成為業界企盼且需求殷切之職能需求。

AI智慧機器視覺應用技術工程師的養成十分不易，需養成先進技術的應用能力，並將所學技術轉換成有效運用的整合能力。因此，在經濟部工業局指導，由本協會辦理「2022 AI智慧機器視覺應用技術人才特訓營」。今年暑期特訓營共邀請到6家優質企業，包含台灣發那科、羅昇企業、勤堃機械、群翊工業、新亞洲儀器及寶元數控共同聯合參與。參與企業皆規劃完善的訓練內容，並指派資深員工及主管擔任指導員。雖然今年招生當下遇到嚴重疫情影響，但仍然收到來自25間大專院校55位學生踴躍報名。從初選後再經企業線上面試，最終僅錄取22位來自台灣大學、中興大學、臺灣科大、台北科大、逢甲大學、勤益科大、雲林科大、南開科大等校的菁英學子，進行為期二個月實務課程與實作的密集訓練。

智動協會希望透過這個活動，讓學生可以從校內課程銜接至廠商實務面，將學校所學透過特訓營補足不足之處，為業界培養出更多AI應用人才，並讓學生提早獲得職場就業方向。前三屆當中已有19位優秀的學員，至台積電、上銀、群光、友達、鴻海及中強光電等企業任職。今年辦理暑期實習活動已經來到第四屆，四年總共培養了64位的學生，本活動更獲得參加過研習的學長姐們的推薦傳承，及深獲參與廠商肯定，期望協會能持續協助廠商到好人才。本年度邀請參與暑期實習的學生分享學習心得，及廠商分享參加經驗。

發那科的實習生活

文 國立臺灣科技大學 何慶軒

有幸能參加發那科的實習是因為無意間在逛學校的臉書社團時，發現有學長張貼出今年的人才特訓營簡章，好奇之下看了看內容，發現這是一個難能可貴的機會。可以去接觸到產業並能在暑假期間進到公司內實習並學習，雖然在日後的必修課程中也有實習的學分，但多一次的機會來接觸產業，也可以讓自己知道自己未來想要的工作形式。

面試的準備過程及心得

準備好要參加這次的特訓營後，開始將自己有關技能的獎狀、證照及資料等等全都整理好後，發現自己其實在比賽的經歷上很豐富，但卻沒有任何面試的經驗。因此在準備的過程中，也思考面試時可能會出現的問題，如對公司的瞭解程度或是對於公司有什麼問題想深入瞭解的，自己更是期許自己能夠好好地完成這次的面試。

在面試過程中，與兩個部門的經理一同面試，當走進會議室時有種跟平常不同的緊張感出現，雖然會緊張但也一直告訴自己「你是可以的！」。在對答的過程中，我也靜下心來認真聆聽經理們所說的內容及所問的問題，經過自己的思考後，也回應了該回答的內容。在面試結束後雖然很擔心自己有沒有被錄取的機會，不過已經讓我更堅定要持續的精進自己的能力，掌握更多的機會學習新的知識及技能。



在發那科學習焊接電子零件

實習生活

面試的過程中，瞭解製造部修理課的工作內容，在收到錄取通知後，心中也有大概對於工作內容規畫出藍圖來。但實際開始進入公司及現場後，發現跟原先設想的完全不同。這個部門雖然配置的人數不多，但大家卻對各項修理的技術、產品等非常熟悉。初期部門指導人員的不厭其詳的講授許多知識，到進入場域實際動手做的階段，我只要有問題都一定會提出向各個學長詢問，他們也很樂意地幫忙找出問題。即便問題難以回答，部門內的人員也願意耐心的查看歷史維修紀錄及相關資料，一一回答我的疑問及提供解決的作法。對於我們來說是完完全全的



完成檢修後的測試

學習新技術，但對於他們或許是持續精進自己能力，及透過問題學習新的解答，我也養成讓自己在遇到問題時，可以更快地找出問題並完成修理。在實習的每一天中都會有不同的挑戰在等著自己，但在身邊有這群學長在，讓我也不會去懼怕挑戰的存在，即便失敗了還有學長們可以一同討論解決問題、一同學習。

實習心得

高三因為學制的關係，曾在業界公司實

習將近一年的經驗，經過大學這三年的重新淬鍊後，再度踏出校園實習這次又帶給我不一樣的體驗。感覺自己變得更成熟、相關的學習知識也更充足。又加上公司距離住家有一段距離，需要在外租屋，生活全部由自己打理，也讓我更為獨立。同時，在這次實習的過程中，更能深刻的體會到未來出社會的工作寫照，規律的生活作息、每天都會有不同的學習及問題需要去解決。雖然學校的環境跟工作場所差異性很大，一開始有些不習慣，但之前的實習經驗，也讓我很快地就適應並跟上公司的步調。

最後也感謝社團法人台灣智慧自動化與機器人協會所舉辦的人才特訓營，因為這個特訓營讓我實際的接觸到發那科公司，讓我更深入瞭解控制器及機械手臂也更認識發那科這公司的技術與企業文化。也因為這次的機會讓我在未來的工作類型選項中，多了一個可以選擇的道路。透過實習的機會來找到自己真的感興趣的工作內容，相信只要在實習過程中認真的去學習，一定可以獲得意想不到的結果！

時的專題製作主要接觸的部分也是這三項，其中圖片的拍攝部分要盡量讓物品的顏色分明、減少過曝的部分。至於調整硬體變數無法彌補的缺陷將可以使用演算法做調整，透過這樣的過程可以使用設計出的演算法從後續相似的圖片中抓出目標特徵。但若有圖片內容與寫演算法時使用的圖片差異過大時，可能會有無法抓出特徵的情況。演算法設計的目標在於穩定，即可以在大部分的輸入圖片中抓出想要的特徵，因此在設計完演算法後，多次測試檢測穩定度是專題製作時很注重的細節。

在職場中擴展視野

在第一次接觸「人工智慧」、「機器學習」時，它以辨識貓狗圖片的形式出現在我眼前，如同科幻電影情節般，電腦也有能力辨識物體，使我對人工智慧萌生了興趣。除了在學校的機器學習、人工智慧概論中學習理論外，也有機會看看視覺辨識的實際應用情況。AI智慧機器視覺應用技術人才特訓營便是我接觸並實作人工智慧的好機會！

新亞洲儀器的視覺辨識

新亞洲儀器為國際上最有實力的AOI部品代理商，能成為視覺部品產業的翹楚，不僅是因為會銷售，同時也為客戶提供視覺影像自動辨識系統所需相關軟硬體規劃。在工程部實習第一件事便是由基礎開始學習，從打光、挑選相機規格、使用HALCON等，透過一系列的課程與實作練習，使我的軟硬體規劃都建立了穩固的基礎。我也從中瞭解原來視覺辨識並非寫程式而已，而是如何讓機器接收到期望的影像，以及如何從影像中挑出期望的目標等問題，才是設計視覺辨識需要注重的。

從零開始到完成專案

實際到公司實習，才知道機器學習和機器視覺是兩回事，兩者是有利弊的工具。機器學習能透過神經網路學習大量的圖片，但與機器視覺才能精準的辨識出目標。而機器視覺不僅需要了解如何配置設計演算法，鏡頭規格、光源大小、工作距離等，數據都不能馬虎。製作專題時使用的是彩色的2D相機，因為要透過物體表面的灰階值辨識瑕疵，以往只有美術課才會接觸到色彩相關的議題，沒想到在機器視覺中灰階值也會成為辨識目標的特徵。此外，不同的亮度也會影響物體被偵測的灰階值，實際測試不同光源，才知道光源的亮度及顏色，與影像的還原程度很有關係。工程師的教育訓練是我們設計演算法的一大助力，從測量到抓取特定顏色的圖像區塊的作業中，漸漸熟悉如何在HALCON中設計演算法，因為有了不同案例的實作與分析，讓我能循序漸進的設計出專題的演算法。

瑕疵檢測

◆ 挑選相機鏡頭

要拍攝物體的圖片需要先挑選相機的規格，再由相機的焦距挑選鏡頭，因為專題需要拍攝的物體為彩色的，需使用Color Camera。挑選鏡頭的步驟是使用公式 $(FOV(視野))/(Work\ distance(工作距離))=(Sensor\ Size)/(Focal\ length(焦距))$ 算出相機的Focal length後，再到Basler網站挑選合適的鏡頭，其中鏡頭又分成C-mount、F-mount、S-mount，而C-mount為較常用的類型。

新亞洲儀器的實習生活

文 國立台北科技大學 詹承偉

前言

機器視覺是使工業設備具有「觀察」的能力，並應用於智慧製造，而在智慧製造中常見的應用像是物品的缺陷檢測、辨識、分

類、測量、定位。從最初的拍攝到演算法設計的過程，大致上分為模擬工作環境的限制、將拍攝器具（光源、相機、鏡頭、配線）架設好、調整變數（曝光時間、鏡頭焦距、光源亮度）、演算法設計。這次的實習

◆ 拍攝物體



物體顏色明顯



有過曝區域

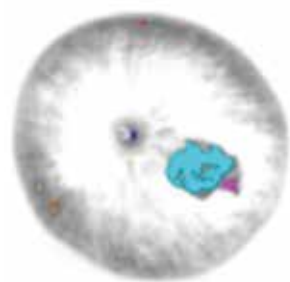
◆ 拍攝環境



◆ 演算法



影像平滑後的蘋果



找到蘋果表面有灰階值在閾值區間的區域

使用的軟體為HAOCON，MVTec HALCON是工業影像處理(機器視覺)產業中具領先地位的軟體庫。專題想檢測的目標為蘋果表面的缺陷區域，而缺陷區域的灰階值大多較低，希望找出缺陷部分可能的灰階值閾值並挑選出缺陷區域。

新亞洲儀器教給我的三件事

客戶的案件需要考慮的除了物體的影像能否被完好的獲取，也要考慮客戶硬體設備裝設的限制，在不同的限制中Try & Error是專題製作中的第一步，總會拍攝到更好的影像但要勇於嘗試；拍攝到的影像會有好多種情況，不一定每一張影像都能被軟體抓出目標區塊；然而透過找出影像中共通點能讓演算法應用於大部分的影像，我學到設計演算法「穩定」便是關鍵，能運用於大部分的例子很重要。

從不同面向思考問題是在使用特徵找出區塊時學到的，一個區域能有很多不同的特徵，但總要思考什麼方法能使特徵在拍攝時或軟體中凸顯出來。這次職場實習使我實際體驗影像辨識的設計，離開時也帶走重要的解決問題的思維，最要的是與不同領域的人交流並互動的經驗，走出校園的兩個月使我有更廣泛的視野學習。

企業感言

AI視覺人才暑期特訓營旨在能讓更多學子學以致用並快速與產業接軌，本次活動實現跨縣、跨校的合作，前後陸續與企業溝通，希望能透過研習營成功發掘人才、培育人才，期待未來與更多的大學院所進行多元的產學合作，並培育AI人工智慧及智慧製造的人才，。

企業參與活動的過程中也引發許多想法與建議，羅昇企業長期積極配合特訓營活動，除了希望能有機會引進實習生以外，也希望能對校園招募更多人才，未來更期待與學校合作促使捐贈教學設備，羅昇表達教育不是只有一種樣式，不論是企業或是學生都很需要此類似的活動，未來也會持續支持。

寶元數控這次除了提供業師進行協同教學，今年度為了不讓疫情影響學員學習過程，也首次打破空間及時間問題，調整為線上實習，讓學習更有效率，寶元也期望透過本次活動拓展企業校園知名度，以增加招募之人才。

勤堃機械拓展嘉義新廠後，希望引進AI智慧機械的新血生力軍，提供在學學生實習機會，讓學生可做中學，學中做，新廠內主管與學員一同探索及解決問題，了解自己的專長，學員更可藉此加強的知識技能，期許參與學生除了專業技術以外，更希望他們能學習到職場所需具備的知識、技能與態度。

群翊工業身為上櫃公司，本於企業社會責任，十分樂於合作本次人才培育，這是群翊第一次參加此類型活動，主要目的是希望能培養企業組織轉型之創新人才，令群翊印象深刻，是本計畫的專業培育人才的具體作為，協助兩

位程度優秀且表現良好的實習生銜接企業文化，將來學員能面對職場時更能得心應手。

新亞洲儀器主要發展視覺檢測技術與演算法，參這本次活動是希望能培養企業研發關鍵人才，對於學員資質感到十分驚豔，也期望未來能以學年制度為主，可拉長研習時間提供學生就業前培養實作能力之機會，也願意聘用即將畢業之新人才，為企業帶來無限創意。

台灣發那科一直以來對於協會暑期研習營都非常支持，因為活動是針對特定科系招募，不同於一般面試管道所找到的人才，所收到的人才更為專業也更符合企業所需，對於招募學員的品質感到十分滿意，台灣發那科除了提供專門業師及規劃機器人課程及外，更提供給學生展現的舞台，培養了學生解決問題的創新能力、溝通協調的實踐素養，提升在未來機器人時代的超前部署競爭力，成為具備相關實務應用能力的專業人才。

此次參與的企業皆感謝經濟部工業局能協助企業培育人才，希望能夠深耕青年學子對AI技術軟硬體技術的研發興趣，透過企業實作與學術研發的資源整合，將跨領域設計思考及學科知識運用發揮到極致，落實產學接軌、促進產業發展，以培養新一代的AI人才，在現在面臨少子化、缺工的壓力下，未來要吸引人才，要讓人才做有價值、有成就感的工作，提高台灣產業競爭力。

用智慧科技 導入指引重檢企業 供應鏈韌性與評估改善方式

文 社團法人台灣智慧自動化與機器人協會

不同的產業對於「供應鏈管理」有著不同的策略重點。在新冠疫情爆發後，不少企業逐漸意識到供應鏈架構與協調對風險之下的順利運作扮演著關鍵角色，因此投入心力探討不同供應鏈風險之下企業最適合的因應策略，然而，許多企業對於供應鏈「韌性 (resilience)」的認知及相關的管理機制，認知仍然有限。

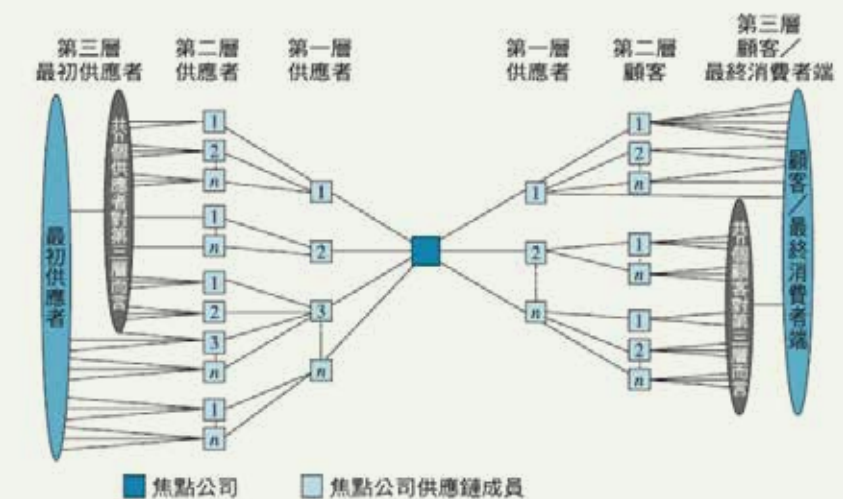
例如，在新冠疫情期間，許多企業發現自家貨物因為塞港與停工等影響，貨物無法運送至目的地，因此希望建立一套供應鏈系統追蹤貨物蹤跡，然而到了執行階段才發現力不從心，因為，從內部而言，供應鏈的運作與許多的功能單位產生連結；從外部而言，供應鏈夥伴包括上級供應商、以及供應商的供應商等角色，這種跨組織、跨部門的合作與整合，並非想像中的容易。

供應鏈管理是企業塑造競爭優勢的寶貴資產，過去許多個案都一再顯示，競爭表現傑出的企業，都將其供應鏈視為一項策略資產，並不斷追求新方法，改良供應鏈以創造策略優勢與價值，使其能在激烈的市場競爭中保持領

先。然而，大多數的企業並沒有將供應鏈提升至策略層級，仍將供應鏈視為一種單純的管理手段，既沒有訂定明確策略、也沒有進行內部溝通，只有在狀況百出，例如：存貨過高造成資產過度積壓、顧客抱怨品質不佳、或是某些關鍵原物料供應商延遲出貨時，才想到要改變供應鏈。在新冠疫情的影響下，許多企業必須為此種認知付出代價。

在強調客製化與多元多樣的需求帶領下，大量製造的模式恐難以維持企業利潤，以高科技電腦產業為例，當產品的生命週期受到壓縮、訂單變得少量多樣化，且交貨期不斷地縮短時，保持高度彈性與提高反應速度，精簡企業組織，乃成為如此高變動市場下的

供應鏈網路架構



資料來源：Douglas M. Lambert, Martha C. Cooper, and Janus D. Pagh, "Supply Chain Management: Implementation Issues and Research Opportunities," *The International Journal of Logistics Management* 9, no. 2 (1998), p. 3.

最佳解方。因此，如何與全球供應鏈進行上下游的串聯，並透過資訊科技提高供應鏈的透明度，是現今整個供應鏈領域的發展關鍵要素，更是企業提高核心競爭力的所在。為強化企業組織的供應鏈競爭力，企業在追求效率上更是無止境的，基於全球供應鏈的專業分工，各級供應商若能配合中心大廠的供應鏈管理模式，並且整合組織內各個功能單位、組織外部的各個供應商或合作夥伴，確保彼此資源與資訊的流通，將可以達成更高的管理綜效。

現代供應鏈管理所面臨的風險與挑戰

然而，在供應鏈中，除了預測經常不準且市場變化快速之外，也會出現許多無法預料的因素而打破供需平衡，例如：原物料品質問題、產品製程的變化、經濟週期循環的改

變、機器設備故障、人員流動、物流運輸壅塞等。在新冠疫情大爆發期間，汽車產業晶片短缺就是最好的例子。

以智能化汽車為例，一台汽車需要的積體電路可能高達 1,400 至 3,000 單位。然而，自2020年開始，半導體產業鏈除了必須面對美中貿易戰所帶來的壓力，也同時必須針對全球蔓延的新冠肺炎做出反應。許多廠區紛紛停工，讓這個穩定多年的產業一下子失去了根基，上、下游都受不同程度影響，並且一層一層如骨牌效應般地擴散至全球。根據高盛 2021 年調查報告顯示，至少有169個行業受晶片短缺影響。

更有甚者，在新冠疫情大爆發的時候，許多車商估計消費者會減少外出，整體市場需求將下滑，因而取消大量晶片訂單；同時，終端消費電子(如：手機、筆記型電腦)因為遠距趨

勢，市場大幅成長，晶片製造商遂將產能轉往消費電子製造商。然而隨著疫情發展趨緩，市場對汽車的需求大增，車商便重啓產線加速生產，希望滿足市場爆增的需求，但卻發現竟然沒有晶片可用，因為晶片產能早就都被消費性電子業搶走了。就整個汽車產業來說，其晶片用量僅佔據全球晶片生產量的15%，相對地個人消費電子佔據了50%，且利潤更大，在供不應求的情況下，晶片廠商因此優先供貨給高利潤的消費電子業。另一方面，車商過往遵循零庫存的管理方式，因此缺乏庫存晶片又搶不到產能，只能看著滿手訂單，卻無產品可以出貨。福特 (Ford) 公司至少有上千台半成品車輛因缺少晶片無法完成；日本豐田汽車 (Toyota) 在2021年9月時也因為晶片、零組件等物料短缺減產了40%。這些都在在反應企業必須在變化快速的消費市場中對可預見或是不可預見的風險即時回應，以持續維持市場中的領先地位。

無論是對於零售業者、批發商、製造商、或是產業鏈上的任何供應商來說，都需要面對供應鏈管理上的兩大挑戰：將成本降到最低、並且提供最好的服務。然而，要能讓對

的產品在消費者想要的時候，出現在對的地方，又要盡可能地以最低的成本完成上述的服務，是非常困難的。供不應求會造成銷售的損失；供過於求又會產生庫存積壓、滯銷的風險，產生額外的成本。因此，企業無不追求在可能的風險之下，得以讓公司資源達到最佳利用，以「剛好」滿足市場需求，達到供給與需求的平衡點。

疫情對全球產業供應鏈的挑戰與衝擊

在許多報章雜誌上，我們經常可以看到「後疫情時代」這樣的字眼，顯然新冠疫情對許多的商業活動來說是很大的分水嶺。在後疫情時代，供應鏈面臨了諸多的困難與挑戰，除了需要提高自動化程度以因應少子化、長期缺工問題，黑天鵝事件更是層出不窮，對企業而言，維持營運穩定、打造韌性供應鏈已是一門必修課程。除了新冠疫情的影響，隨著市場趨勢的轉變，少量多樣逐漸取代了大量少樣的製造模式，產品生命週期也逐漸縮短，這些在在都進一步提高了供應鏈管理與快速回應的難度。對製造業而言，

除了必須控管對內的產銷管理外，企業外部的供應商管理亦存在許多風險，若只管理自身企業，未掌握到第二層、第三層供應商的資訊（例如：原物料溯源、採購合約管理、供應商績效評估等），就很可能就會產生資訊落差的情形，導致企業難以掌控即時營運狀態。

在企業實務上，除了透過掌握供應鏈資訊提高透明度以降低風險外，企業也應考量國際間環保、法規等風險及差異性，例如隨著 ESG（社會、環境、公司治理）概念的發酵、減碳意識高漲，若企業疏於管理永續、能源相關議題，不僅可能會造成品牌形象受損、增加額外成本，亦有可能會導致供應鏈中斷等問題，間接對收益造成影響，這些問題預期在未來都是無可避免的發展趨勢。

我們認為新冠肺炎疫情對全球產業供應鏈所造成的挑戰與衝擊可包括訂單規劃的難度提升、成本與冗餘的取捨問題、全球性通貨膨脹、勞動力短缺。

疫情之後：供應鏈的未來

受到疫情的衝擊，全球供應鏈發生許多重大的轉變，過往企業所習慣的模式，恐怕無法再一體適用，在後疫情時代，設法讓自身企業供應鏈具備抵抗與復原能力格外重要，具有韌性的供應鏈因此能夠緩解大多數供應鏈中斷的衝擊，並降低風險因子可能對企業造成的傷害。新冠肺炎疫情已經讓我們看見，這類國際級的風險災難將如何對供應鏈的研發設計、採購、製造、物流運輸、銷售等環節產生影響。

一、疫情下供應鏈的四個優化面向

要打造自身企業的供應鏈韌性，通常可以由以下四個面向來評估：

1.可視性（Visibility）

可視性是指供應鏈中資訊的透明程度，例如：貨物運輸追蹤系統，讓所有庫存和產品動向的清晰可見。從供應鏈上、下游的合作關係來看，倘若企業對於其供應鏈夥伴僅有片面和局部的能見度，企業就會無法進行有效的管理，這是由於供應鏈企業的決策經常受到上下游供應商的影響。供應鏈夥伴間的合作與互信，往往決定了彼此對資訊的掌握程度，提高供應鏈可視性，是企業用以實現供應鏈管理有效性的方法，供應鏈夥伴彼此間的資訊愈透明、彼此間的決策就承受著愈低的風險。

2.敏捷性（Agility）

敏捷性是指面對供應鏈中可能發生的變化，企業得以快速因應、做出回應。例如：調整生產產能、重新建置供應網路、開啟新的銷售通路等。

3.多樣性（Diversification）

多樣性指企業應針對不同的產品需求，並根據環境變化，選擇不同的合作夥伴，並及時地調整企業戰略、產品特性等，重組供應商網路。

4.應變計畫（Contingency Planning）

應變計畫是指當供應鏈面對不同的危機，導致有斷鏈風險時，企業應有應變計畫，讓危機降至最低。

從供應鏈看企業普遍面臨的問題大致面向

供應商	採購	成本	管理者	客戶
(1)全球化與原物料價格不斷上漲，成本壓力越來越沉重，影響市場競爭力 (2)疫情、天災及政治等因素，造成交期不確定性與成本提升的主要因素 (3)無法精準掌握供應商品質，亦無評鑑優質供應商的機制	(1)不易管理供應商，對於詢價、比價過程與歷史紀錄，無法完整留存 (2)反覆確認浪費時間，不易掌握採購進度 (3)採購成本調降以滿足組織內部的kpi	(1)產線不夠彈性，無法靈活應變產銷計畫 (2)人為疏失報錯工單，影響生產上線時間 (3)備貨數量難以精準預估	(1)內部管理不夠資訊化，資料整合需耗費大量時間及人力 (2)無法掌握各端即時需求 (3)供應商供貨不及，影響產線生產中斷 (4)庫存空間不足，存貨水準偏高	(1)訊息不夠透明，容易溝通不良，造成訂單有誤 (2)無法快速掌握交期與報價 (3)無法提前確認供貨狀況以因應市場變動

傳統供應鏈



資料來源：Deloitte analysis.

數位供應網路



Deloitte University Press | dupress.deloitte.com

讓供應鏈提高韌性，目的不僅是為了抵抗災變和回復營運，透過這四個面向評估供應鏈流程，並善用現代化供應鏈相關科技技術，就能達到預估、提前準備並快速因應未來可能潛在之供應鏈風險，為企業帶來其他競爭優勢與機會。

二、後疫情時代，企業的因應之道

2020 及 2021 年全球經濟表現的重大關鍵莫過於新冠疫情的影響。市場上出現的諸多改變逐漸成為新常態（New normal），過往企業的經營策略恐怕無法再一體適用，面對疫情後的不確定性，管理者到底該如何自處、從那些方面著手改革呢？從長遠來看，未來供應鏈有以下三大趨勢：

(一)數據賦能：打造數位供應鏈

隨著消費者對企業回應速度的要求愈來愈高、需求變得愈來愈多元，代表著市場環境面對消費者的風險也變得愈來愈大；當「及時性」變成維持市場競爭力的基本條件時，業者必須要做出適當的供應鏈轉型，以因應這個龐大的挑戰。數位供應鏈是指透過數位科技建置，並與數據串聯，使整體供應鏈變得更加透明化，同時降低資訊不流通所帶來的風險。流程自動化、物連網數據串接、數據分析預測等都屬於數位供應鏈的一環，企業組織可以透過物聯網裝置的安裝，進行數

據的蒐集，提高分析能力，以達到更精準的預測需求、降低風險與不確定性。供應鏈的透明化亦可以讓企業組織及時發現問題，並在災害發生時立即指示供應商、並制定相關因應策略來減輕衝擊。對於企業組織來說，由於資源有限，因此在數位供應鏈的建置上，可以先從最核心業務相關的部分切入，例如：服裝製造商可以建立線上服裝樣本的3D打樣系統，減少親自前往海外、在製造商與買家間來回查看與溝通的成本。

供應鏈的數位化可以讓企業提升並強化以下四個特性：

- 1.提供可視性：整合供應鏈上的資訊，並且能夠清楚地掌握與運用。
- 2.強化可預測性：透過模型分析風險事件，制定應對方案。
- 3.具備可調適性：建立彈性以迅速回應。
- 4.追求可持續性：將上述做法機制化，與供應鏈上下游結合，達到供應鏈間最佳化的調適，創造信任關係。

提高供應鏈韌性，邁向數位化的實務做法則可分從以下面向進行：

1.數據化的供應鏈合作平台：在製造或企業營運流程中，將風險管理納入考量，當危機發生時可迅速與上下游夥伴達到良好溝通並迅速制定復原策略。

現今已有許多跨國公司開始整合上下游夥伴資訊，蒐集從製造、銷售、到財務端的數據，以評估各區域的產品需求量等市場資訊，以優化相關決策。

本田汽車（Honda）前往歐洲發展時，即與IBM合作，透過整合性系統，將上下游的採購和財務資料，進行分析與整合，並透過儀表板/戰情室讓決策者可以快速發現問題，及時處理異常現象。

2.大數據分析/人工智慧：使用數據進行事件分析，建立模擬模型，預測中斷帶來的影響，制定復原策略。

位於瑞士的航空電信技術公司 SITA 開發了一款飛行應用程式 eco app，這款應用程式可以幫助飛行員分析天氣狀況與飛機耗能等資訊，最大限度地提高燃油效率、減少碳排放，找到最佳的飛行航道、提升航班穩定性，從而實現更安全、更舒適的飛行。該解決方案有助於提高飛機的整體效率。

3.區塊鏈/紀錄追蹤科技：透過科技技術，即時掌握供應鏈風險。

註冊於新加坡的全球金屬貿易商 Trafigura Group，為整合相關 ESG 數據，便於 2021 年與供應鏈來源和排放追蹤服務商 Circulator 合作，利用區塊鏈技術追蹤金屬供應鏈的碳排放，藉此掌握碳排放所產生的氣候成本與風險，逐步將相關數據整合到自身的價值鏈中。

4.預警系統：及早認知風險的出現，並在危機來臨之前預測未來風險發生的機率。

可視性
Visibility敏捷性
Agility多樣性
Diversification應變計畫
Contingency planning

近來全球面臨晶片荒，再加上新興科技的相關應用，逐漸衝高半導體需求，全球半導體資源已被視為關鍵戰略資源。為了防止半導體供應鏈中斷的情況再次出現，美國與歐洲於 2022 年五月宣布將共同建立全球的半導體「預警系統」，期望合作改善半導體供應鏈失衡狀況，讓廠商即時掌握關鍵資源的庫存與晶片動態，以達到產能有效調度、最佳化產能配置並滿足客戶需求的目的。

(二)產業由從精實走向多元彈性，強調供應鏈備援能力與靈活性

過去企業多半強調精實生產、減少浪費，將「庫存」視為必要之惡，這種狀況在汽車產業特別明顯。然而，在新冠疫情發生之後，企業對於「庫存」的估算，不能再只針對倉儲或管理成本為考量，也應該加入風險管理（Risk Management）的觀念，並運用數據與科技，進行更精準的客戶需求預測（Demand Forecasting）。換句話說，零庫存不應再是企業進行相關管理時的終極目標，相反的，企業應轉而尋求更精準的「最佳庫存水準」。另一方面，由於過去全球供應鏈呈現專業分工，許多企業是採單一來源的採購模式，然而，在疫情的衝擊之下，此種單一、少量來源的採購模式卻暴露出極高的風險，一旦單一節點出了問題，就可能造成供應鏈「斷鏈」。舉例來說，通用汽車公司為增加供應鏈的備援能力，便在世界各地（如：阿根廷、波蘭、泰國和巴西）的工廠採用相同的設計、模板和製造流程，以因應單一節點中斷的問題。

(三)永續經營新常態：綠色轉型

現今已有許多跨國供應鏈企業開始要求其供應商配合使用再生能源並加強減碳，不符合的廠商恐將被淘汰。

2020 年，蘋果（Apple）官網一篇公告寫下：「2030 年前，蘋果的全製造供應鏈將達到 100% 碳中和。」這項宣告意味著，對蘋果上下游以數百家計的供應鏈廠商而言，若要持續保有來自蘋果的訂單，勢必得進行相關能源轉型與永續策略的建置。根據蘋果官方統計，該年度至少有 8% 的廠商不符合其《供應商行為準則》，或認為自己難以達成目標，退出供應鏈。

在全球永續發展的趨勢下，各國已開始積極制定相關規範，以達到淨零排放的終極目標。對企業組織來說，綠色供應鏈的轉型勢在必行，企業內部永續政策的管理與規範已從「做了更好」變成「不得不做」的議題。雖然各國的淨零排放路徑不盡相同，但從上述例子中可以發現，永續性問題早已開始擴及整體產業，而不僅僅是影響個別企業。

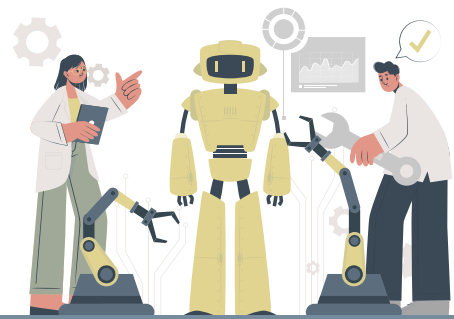
臺灣以製造業出口為主，是全球供應鏈體系的重要一角，因此國際產業發展趨勢及供應鏈佈局方向都將對臺灣企業帶來絕對影響，建議業者做好相關準備，確保自己能成為安全、韌性、信賴的供應鏈重要夥伴，避免於多變的大環境中隨時出局，而在此之前的基礎工作，就是先得掌握韌性供應鏈的涉及範圍與相關技術應用。

特別是從上述的說明，我們可以得知在歷經疫情衝擊後，更加顯露過去的經營模式與管理認知有著相當必要的革新，因為在面對無法預知的環境劇變與挑戰下，即使是老字號企業也可能面臨破產、停業的絕境，唯有學會預測風險，透過數位科技來強化企業韌性，才得以隨時因應外在的變化，即時做出適當的回應。

「看(可視)」就是掌握訊息、現況一個重要的過程與提升供應鏈韌性的基本要件，也是供應鏈上的眼睛，讓人透過最佳的方式，看到正確的數據。可視化主體是透過應用物聯網等相關技術，透過感測器和網路技術來取得設備生產資訊，並連結企業內部的各系統或資料庫，再運用如數據採集、監控系統

(SCADA)或商業智慧軟體(BI)的方式，將企業的所有流程數據進行管控，並以戰情中心動態看板方式展現，幫助管理者即時掌握現況，包括訂單達成情況、人員出席狀況、生產操作率、原物料進出狀況、生產進度追蹤、設備稼動、製程品質分析、能耗等即時訊息，讓資源與製造得以在掌握之中，並協助主管於異常發生時，可以即時進行分析與策略擬定，避免損失或做到停損。這也是指引所希望分享的主軸科技，其中並同時推薦的八個步驟搭配簡易工具，帶領大家快速檢視企業自身供應鏈的問題，並著手構思導入智慧科技，同時搭配運用案例給予各位一個精簡扼要的強化韌性入門參考，現在開放免費預約索取電子檔，歡迎多加利用。(內容轉載智慧科技導入指引)





2022第二屆機器人智動系統優質獎

發掘優秀人才，
開發創新產品，
產業動起來！

文 社團法人台灣智慧自動化與機器人協會

在機器人產業逐漸由單機開發朝向系統整合發展的時刻，為刺激產業創新應用與研發，找出學習參考典範，以及展現政府對機器人產業系統整合人才培育的重視與支持，工業局結合精密機械研究發展中心及台灣智慧自動化與機器人協會，共同辦理「機器人智動系統優質獎」。今年延續舉辦第二屆機器人智動系統優質獎，此次參賽作品也更加多元，包含：人工智慧視覺系統、高精度擺線減速機、中空軸伺服馬達、晶圓載移系統、智能防疫機器人、綠色數位供應鏈系統、機器人控制器等等產品及系統，皆具潛力及特色。應用產業別也非常多元，包含半導體、金屬加工、晶圓製程、點膠及研磨、機器人、物流等等，更有目前產業最需要的ESG應用系統。

競賽獎項分為創新應用研發類及傑出人才類，本屆共計24家公司27件作品參加創新應

用研發類(機器人及關鍵零組件研發組、系統整合應用組)，8家公司9人參加傑出人才類(傑出工程師獎、傑出團隊領導獎)，並經過評審團嚴謹的甄選，最終選出創新應用研發類8件得獎作品及傑出人才類4位得獎者。

機器人智動系統優質獎
獎項介紹

(一)創新應用研發類

系統整合技術、機器人及其關鍵零組件等應用於生產製造之產品與系統服務，就產品與系統整合技術與服務本身品質精進、技術研發、加值應用等創新，從舊有產品與系統改善且和指標廠商相比，趨近或超越同類產品。

- i. 機器人及關鍵零組件研發組：限國產製品，包含機器人及其關鍵零組件，如控制器、

減速機、馬達/驅動器、感測、通訊、軟體技術等自主研发產品。

- ii. 系統整合應用組：提供機器人智動系統整合解決方案，解決方案內需具有智慧製造元素與系統整合技術。系統整合技術包含智慧機械/機器人技術、物聯網技術、網宇實體技術、精實管理技術等。

(二)人才類

機器人智動系統整合人員包含智動化規劃、智動控制系統、機構、資訊等相關技術工程、設計與管理階層人才。

- i. 傑出工程師獎：從事機器人智動化設備/單元、供應鏈、整線、整廠系統整合之規畫設計、技術之開發，具有特殊貢獻，允當楷模者。
- ii. 傑出團隊領導獎：實際帶領團隊進行機器人智動化設備/單元、供應鏈、整線、整廠

系統整合之規畫設計、技術之開發或專案之推動、管理與應用，具有特殊貢獻，足為產業楷模者。

第二屆機器人智動系統優質獎
得獎作品介紹創新應用研發類：
機器人及關鍵零組件研發獎

★特優獎：CRB交叉滾柱軸承/上銀科技股份有限公司



產品介紹：CRB高剛性、高精度與節省空間的特性，工具機多軸加工及四五軸迴轉工作台的產品需求也日益漸增，應用於加工設備或迴轉工作台實績眾多，HIWIN交叉滾柱軸承打破國內加工設備與迴轉工作台製造商需依賴日本進口交叉滾柱軸承的交期不確定性、價格高昂與技術無法支援，累積40家以上的原本使用日系進口軸承轉換為HIWIN的工具機與迴轉工作台客戶，幫助國內廠家提高產品競爭力。

★特優獎：機器人控制器 GRC2-V100/創博股份有限公司



- i. 可控制多種不同構型之工業機器人
- ii. 具備EtherCAT即時通訊功能，可連接各種標準EtherCAT裝置如伺服驅動器與I/O模組



圖2.2022ARSI頒獎典禮經濟部工業局局長、委辦單位、執行單位、評委與創新應用研發類得獎者合影



圖3.2022ARSI頒獎典禮經濟部工業局局長、委辦單位、執行單位、評委與人才類得獎者合影



圖1.2022ARSI頒獎典禮經濟部工業局局長、委辦單位、執行單位、評委與參賽廠商合影

- iii. 提供方便容易操作的配置工具軟體(Nex-Motion Studio)，可依應用需求配置EtherCAT拓撲，廣泛且多元的機器人整合範圍、亦可自由指定軸關節模組
- iv. 配置工具軟體軟體也提供即時模擬分析、試運行與參數調整功能
- v. 提供具備簡單直覺的機器人操作介面軟體(TPUI)
- vi. 教導、編程、參數設定與驗證整合於機器人操作介面軟體中
- vii. 使用者於編程上的邏輯時序反應可達到1ms以內的即時性

★優良獎：LIPS edge™ AE400強固型3D 雙目相機/立普思股份有限公司



產品介紹：將深度影像資訊與RGB 影像畫面同步，讓開發者能精準比對每一禡的2D與3D影像，並套用2D+3D機器視覺演算法，在市面上許多同類型產品無法提供此項功能，因為達到此技術需要相當高的光電整合與視覺校正的能力。LIPSedge™ AE400已量產並提供給多家工業客戶使用。指標性客戶如日本的Kyocera與德國的BMW等，分別用於工廠智能製造與安全應用還有搬運自走車上。

★優良獎：模組化自主移動機器人/緯創資通股份有限公司



產品介紹：以模組化的設計，將移動平台專注於自主移動的功能，上方則搭配不同的應用模組，以適應來自特定場域中不同的應用，軟體部分則為Web based方式開發，可滿足於不同平台，輕巧靈活，採用差速輪設計，可原地迴轉，因此適用於空間較小的場域，例如醫院、飯店、安養院、辦公室等場域，都可運作自如。也可銜接紫外線及噴霧模組，成為消毒機器人。疫情期間可結合噴霧模組於有人的情況下，達到消滅covid-19病毒的作用；另結合紫外線可以累積能量，於無人的狀況下，亦可達到快速消毒的目的。

創新應用研發類：系統整合應用獎

★特優獎：先進製程晶圓人工智慧自動光學檢測系統/均豪精密工業股份有限公司



產品介紹：應用產業別涵蓋半導體、感應元件、感測器、mini/micro LED等多個產業，投入在穩定且大量的生產，除了為均豪帶來營收與獲利以外，並為終端客戶帶來以下好處

- i. 智能化AOI取代流水線的人工檢測與複判，人工檢測可完全自動化，加速生產線速度，節省人力開支。
- ii. 幫助高階產品投入生產的行列，所開發之AOI機台補足客戶原先機台因能力不足而無法生產之新產品，將產品100%導入生產中。
- iii. SECS/GEM節省機台生產需等候人工的批次鍵入或匯入，與由資料庫儲存再取出所耗費的時間，稼動率提升120%。
- iv. 人工智慧瑕疵分類系統的導入減少AOI過殺並提升良率，AI系統可救回95%以上因AOI所過殺的產品，整體良率提升可達10%

★特優獎：晶圓移載系統/上銀科技股份有限公司



產品介紹：晶圓移載系統EFEM為具高潔淨度、高可靠性、高精度控制及高自由度之產品，機器手臂定位精度及晶圓尋邊定位精度皆可控制於0.1mm內，微環境微粒潔淨度可控制在Class1等級，同時也可根據客戶需求，彈性調整機架配置，如電控櫃位置、晶圓載入/出埠數量及安裝位置、一字型或U字型產線等，高自由度的設計快速因應客製化需求。

★優良獎：半導體IC封裝捲帶多功能包裝機/旭東機械工業股份有限公司



產品介紹：台灣第一台半導體IC封裝捲帶全自動多功能包裝機，提升出廠品質，大量降低產出的不確定性，實現生產製造技術增值優化，提升設備智慧製造能量及國際輸出競爭力，以數位轉型、智慧彈性生產為兩大主軸，導入機器手臂製造技術、建置人機共融包裝系統，產出半導體IC封裝捲帶包裝的高效率、高彈性、高穩定性的特性效益。

★優良獎：超高自動倉儲-飛梭車系統/高僑自動化科技股份有限公司



產品介紹：一般倉儲系統高度大多落在15~23M，飛梭車實績高度達43M，目前為世界紀錄保持。主要優勢為無主柱設計及車輛輕量化特性，可提供超高倉庫、更加節能及具有備援機制之解決方案，以達到使用體積最大化，顛覆傳統自動倉儲作法。

- i. 智能化作業：先進先出、物品集中放置、空間利用最大化、快速空間釋放。
- ii. 備援能力再提昇：車輛維修保養時，其他車輛可繼續運轉，不會造成系統停滯。
- iii. 彈性投資計畫：根據量能及分期投資來增補車輛以增加運轉能力，減少無效投資。
- iv. 面積縮小化：利用擴增倉儲高度以減少使用面積，能有效提升容積產能。

傑出的得獎人才與作品，顯示國內機器人智能化系統整合環境百花齊放，經濟部工業局也將持續推動我國機器人智動系統產品與服務的整體能量，全面推升產業發展，敬邀明年第三屆機器人智動系統優質獎廠商參加。



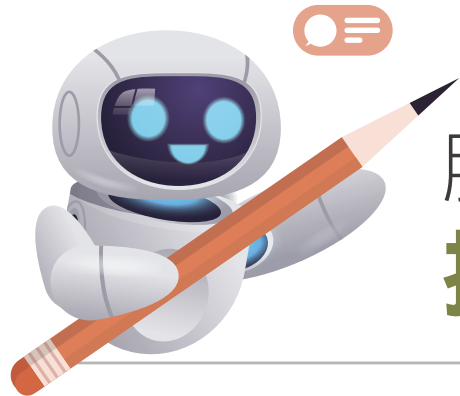
第一、二屆機器人智動系統優質獎產品入圍指南



第一屆機器人智動系統優質獎成果影片



第二屆機器人智動系統優質獎成果影片



服務型機器人創意實證 推進多元場域應用

文 社團法人台灣智慧自動化與機器人協會

為推動服務型機器人產業發展，2018年經濟部工業局結合資策會、智動協會促成服務型機器人聯盟成立，以推進產業上中下游合作鏈結，並自2019年開始推動服務型機器人場域實證，至今執行四年來，分別與大潤發、台中日月千禧酒店、義大世界購物廣場、特力家居桃園館和台南館、清福長照和桃園國際機場等場域合作，促使產學研團隊共同研究發展近60種應用服務實證於飯店、商場、機場、長照機構、展示中心和博物館等，快速擴散多元場域應用案例。

2021年更正式開辦RoBo com服務型機器人創意實證競賽，在服務面向呈現很完善的場域解題成果，顯現各團隊創新思維與設計，實證成果更深獲場域好評。2022年「RoBo com

服務型機器人創意實證競賽」，邀請桃園國際機場及其進駐企業-中華航空、長榮航勤、采盟、和昇恆昌等、以及LEXUS中部汽車及奇美博物館，三大場域業者出題。由禾煜科技、



圖1.2022RoBo com獲獎大合照，邀請經濟部工業局李振隆科長蒞臨頒獎



圖2.第一名：中原大學-粗的不好粗團隊



東元電機、女媧創造、博鈞科技、微星科技五大機器人業者提供機器人實機供入圍團隊免費使用。總計募集75項提案、57組團隊參與，最後共14組優秀的入圍團隊針對場域服務需求提出解決方案，進行機器人創新服務功能開發，並完成實際落地運行。

這幾年疫情造成許多不確定變因，對於服務場域而言，是挑戰也是轉機；目前智慧化服務也已成國際趨勢，服務型機器人更是協助業者落實高品質服務和減輕人力的重要助手，期許未來有更多場域跟進導入，以解決及滿足場域服務需求，更希望透過服務型機器人場域實證提供優秀人才與創意提案落實之平臺，加速服務型機器人產業創新研發，提升產業競爭力。

※獲獎團隊及服務介紹

第一名：中原大學-粗的不好粗

- (1)提案名稱：視覺辨識與滾輪平台輔助行李搬運
- (2)應用場域/機器人：桃園國際機場/微星科技-智能基座機器人AMR
- (3)獲獎原因：解決桃園機場長榮航勤每日需要大量人工載運、處理大件行李卸載，團

隊設計出具視覺辨識與滾輪平台輔助的行李搬運機器人。在智能基座機器人AMR上設計了滾輪平台，讓工作人員輕鬆運送貨物，因本身AMR有加裝避震彈簧，當貨物搬運上去時，會因為本身的重量而下降，使平台高度會因行李重量不同改變。因運送地點的不同，要運送的高度也不同，為了解決這個問題，團隊在滾輪平台下方，安裝了一個升降機台，使平台能根據不同高度抬升。同時重視安全問題，在車輛辨識系統上積極自學運用Yolo和Slam技術以偵測車輛和人，機器人上加裝三色燈，在過車道的時候發出聲音警示，以提醒周遭工作人員機器人的位置，兼具自動駕駛的安全與運送效率。

第二名：僑光科技大學-堤米控蘿蔔

- (1)提案名稱：兵器ROBO風雲
- (2)應用場域/機器人：奇美博物館/博鈞科技-temi機器人
- (3)獲獎原因：運用Temi服務型機器人於奇美博物館服務，團隊為提供更多元化的呈現資訊與模式，加上VTuber的應用結合簡報功能進行簡易式的常設展導覽，也可於大



圖3.第二名 僑光科技大學-堤米控蘿蔔團隊



圖4.第三名 中原大學-中原大學電機工程學系團隊

廳中介紹設施以及進行地點帶位；為提升互動性也設定主動找遊客進行互動、並針對博物館相關資訊設計問答庫，透過語意分析與問答設計，提供前來的遊客獲得相關問題的解答，讓民眾在大廳等待、尋找資訊的期間更增添一份趣味，成為博物館最佳導覽人員。

第三名：中原大學-中原大學電機工程學系

- (1)提案名稱：托盤搬運跟隨車
- (2)應用場域/機器人：桃園國際機場/東元電機-跟隨車控制模組
- (3)獲獎原因：中原大學電機系的團隊，運用東元電機自動跟隨模組於桃園機場行李處

理場的物流推車上，讓推車可以跟著工作人員前進，不需耗費人力去推送，實證時發現場地空間狹小，主動調整設計以符合移動需求，於車身中央設計機構，讓使用者可以順暢快速調整推車位置，機器人運作靈活度佳。

特別獎：中原大學-Twenty

- (1)提案名稱：大件行李搬運
- (2)應用場域/機器人：桃園國際機場/微星科技-智能基座機器人AMR
- (3)獲獎原因：設計AMR與裝載台結合，負責自動運送機場的大件行李，以減輕人力負擔，裝載台採半開放式，讓上下貨物時更加方便。並在車輛派遣系統上，團隊自



圖5.特別獎 中原大學-Twenty團隊



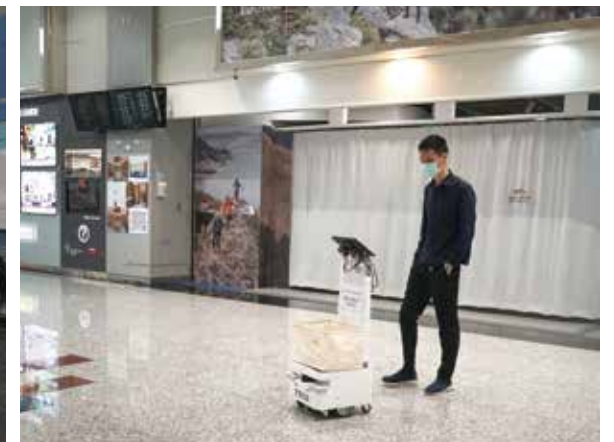
圖6.特別獎 國立陽明交通大學-愛波卡團隊

行開發一路線選擇及問題回報的網頁，並在裝載台上架設平板電腦，讓工作人員藉其下指令給機器人，將貨物送至指定輸送帶。除此之外，團隊開發車輛辨識系統，在運送途中，會自行辨識是否能通過路口，並創新應用光流法等技術來判斷物體移動，避免工作人員需要停下來等機器人通過，同時也在機器人上加裝警示燈，增加行車安全。

特別獎：國立陽明交通大學-愛波卡

- (1)提案名稱：Aircopcart
- (2)應用場域/機器人：桃園國際機場-采盟免稅店區/東元電機-AGV

(3)獲獎原因：在機場免稅區採買時，會使用推車輔助，設計推車能自動化以及具備導航的功能，以提供旅客更棒的選擇。推車將自動跟隨在使用者前方，解決行李安全問題，也更加人性化，隨時可以透過互動介面，轉成導航模式，提高在免稅區的購物品質。並於AGV上應用intel realsense、jetson nano作為基礎硬體設備，基於ROS，並結合human tracking、navigation、以及訓練MobileNet以達到從影像辨識使用者轉彎的意圖，在前跟隨部分，透過tracking與MobileNet確認使用者位置與行為。團隊在控制系統上特別加入了AI來輔助判斷使用者行為，並透過調整參數來適應場域問題，實際解決場域應用問題。





領導者的試煉

600 位執行長的智慧與教訓，
最務實也最殘酷的七堂管理課

卓越領導人必經的七大考驗，
帶領團隊攀向頂峰、打造永續組織！

七堂最有價值的領導課，
透過600位執行長的親身經歷，
看見自身盲點、學會最實際的管理策略。

隨著所有產業的顛覆速度加快，領導也變得
越來越困難。

重責大任、無窮的批評與壓力、行程滿
檔……

儘管領導者享有高薪與福利、權力無人能
及，但背負的義務及壓力也非一般人所能想
像。

凱文曾任安進藥品執行長達20年，帶領公
司將年營收從10億提升至160億美元；

亞當則是擁有30年經驗的資深記者，曾與
全球600多位執行長進行深度訪談。

本書就是兩位作者在過程中累積而成的心血
結晶。

■ 第一項試煉：將複雜事物簡單化

迅速掌握複雜議題的核心，在面對挑戰與
執行策略時清晰溝通，進而成功贏得夥伴的信
任。

迪士尼前執行長羅伯特·艾格自上任第一天
起，便不斷提醒全公司最需重視的優先事項，
他簡單清楚地告訴員工：這就是我們想要去的
目的地，我們要這麼做才能到達那裡。

■ 第二項試煉：創造強大的企業文化

企業文化就像是作業系統，優秀的企業文
化能招募並留住人才，提升整體工作效能與效
率。

亞馬遜創辦人貝佐斯秉持「第一天」的信
念，只用一個詞就定義出清晰的企業文化，藉
此警惕大家永遠懷有創業的初心，並維持前進
的動能。

■ 第三項試煉：組建高績效團隊

即使是頂尖企業，真正適得其所的人員也只
有75%。在公司發展的過程中，團隊也同樣需
要進化，而你必須帶領團隊前進。

安泰人壽前執行長羅恩·威廉斯會使用「前
視雷達」來評估團隊：成員是否能隨著公司的
複雜程度提高而進步？唯有不斷增進自身能
力，才能協助公司執行成長策略。

■ 第四項試煉：成功引導企業轉型

面對轉型危機，領導者的首要任務是坦誠以
對。當你向下屬吐實，願意留下來的人便是那
些想要接受挑戰的人。

紐約時報曾面臨不得不的數位轉型，最後順
利轉危為安。安進藥品也成功度過擴張危機，
省下19億美元的開支，迎來更快速的成長與更
高的利潤。

■ 第五項試煉：真正傾聽他人話語

你必須打破同溫層，真心聆聽他人話語背後
的真正意涵，才能看見問題癥結點與真相。

Aira科技執行長錢德拉塞卡曾說過，無論在
哪個組織，最困難的事就是讓人們對你絕對誠
實。唯有當你認知到傾聽需要承諾和持續關
注，公司才能生存下去並茁壯成長。

■ 第六項試煉：帶領組織度過危機

當危機發生，你必須認清事實、迅速反應、
廣泛溝通，也要解決問題的根本成因。

2020年新冠肺炎爆發，萬豪酒店集團執行
長蘇安勵在第一時間便發出沉重、但人性化的
聲明，宣布自己當年度不領薪、主管薪資減
半，進而安撫員工心情，直面後續挑戰。

■ 第七項試煉：修習領導者的心理素質

領導就像滑雪——你要找到平衡點，隨時順
應環境與地形，不斷調整身軀傾斜度，往不同
方向行進。

身為成功的領導人是矛盾的，你必須既樂觀
又實際、富同理心又苛求、急迫又有耐心，也
要懂得在創造架構的同時給員工自由。

兩位作者在書中借鑑了600位執行長的智
慧、故事和經驗教訓，整理出能幫助領導者茁
壯成長的技能。他們創造出適用於所有領導者
的共通語言，有助於各階層領導者培養達成目
標的能力。

無論你是小主管、中高階主管、董事長、執
行長、經理人，或是欲提升自身優勢、想在組
織內向上爬的人，在面臨最嚴峻的領導力挑戰
時，本書都能指引你走出一條自己的路。

作者簡介

亞當·布萊安特（Adam Bryant）

梅立克公司（Merryck & Co.）的常務董事，該公司
的主要業務是高階領導能力開發與高階主管指導。哥
倫比亞大學的魯本馬克組織特性與領導計畫（Reuben
Mark Initiative for Organizational Character and
Leadership）的資深顧問。

亞當是一名資深記者，於《紐約時報》擔任記者與編
輯18年，曾和600多位執行長與領導人進行深度訪談，
並依據這些訪談內容，從2009年開始在《紐約時報》上
每週刊登〈領導人辦公室〉系列文章。他曾出版過兩本有
關領導力的書，分別是《紐約時報》暢銷書《角落辦公室
裡的內心話》與《快速敏捷》（Quick and Nimble）。

凱文·沙爾（Kevin Sharer）

全球最大的生技公司安進（Amgen）藥品的前任總裁、
執行長暨董事長，帶領公司在20年間將年營收從10億
美元提升到近160億美元。

凱文於2012年離開安進藥品，並在接下來的七年間在
哈佛商學院講授策略與管理，和當時的同事暨如今的奇異
集團執行長賴瑞·卡普（Larry Culp）及哈佛商學院院長
尼汀·諾瑞亞（Nitin Nohria）共同創立了一堂廣受歡迎
的課程，主題是執行長的生活與角色，以及如何領導高階
主管團隊。

凱文曾擔任過雪佛龍（Chevron）、優尼科（Unocal）、
諾斯洛普格拉曼（Northrop Grumman）與3M的董事會
委員。在擔任總經理、董事與導師的期間，曾參與過20
多次成功的執行長轉型，如今依然是許多跨國企業執行長
的顧問。他畢業於美國海軍官校，曾在兩艘攻擊型核子潛
艇上任職。

2023 國際參訪及展覽資訊一覽表



2023 國際展覽行事曆		
01/25-01/27	日本國際機器人研發暨技術大展 (RoboDEX 2023) 東京國際展覽中心	參展優惠
01/25-01/27	日本國際智慧工廠展 (7th Smart Factory Expo) 東京國際展覽中心	
03/01-03/03	廣州國際工業自動化技術及裝備展覽會 (SIAF) 廣州中國進出口商品交易會展館	
04/12-04/14	韓國國際電子製造關連展 (EMK) 韓國首爾 COEX 展覽中心	參展優惠
04/12-04/14	日本名古屋工業製造週 Manufacturing World Nagoya 2023 名古屋市國際展示場 Portmesse Nagoya	
04/17-04/21	德國漢諾威工業展 德國漢諾威展覽中心	
05/10-05/12	日本 AI 人工智慧應用展 (AI EXPO TOKYO)〔春展〕 東京國際展示場	組參展團 擬申請國貿局補助
05/22-05/25	美國底特律自動化技術展 (AUTOMATE SHOW) 美國底特律科博會展中心 (TCF Center)	
05/31-06/03	馬來西亞工具機暨金屬加工設備展 (Metaltech) 馬來西亞 吉隆坡 馬來西亞國際貿易展覽中心 (MITEC)	組參展團、參展優惠
06/21-06/24	泰國國際組裝暨自動化零組件展 Assembly & Automation Technology 泰國曼谷 BITEC 國際貿易展覽中心	
06/27-06/30	德國慕尼黑黑機器人及自動化展 (AUTOMATICA 2023) 德國慕尼黑新國際博覽中心	
07/04-07/07	越南胡志明市工具機暨金屬加工設備展 MTA Vietnam 越南胡志明市西貢會議展覽中心 (SECC)	
08/23-08/26	台灣機器人與智慧自動化展 (TAIROS) 台北國際自動化工業大展 (Automation Taipei) 台北南港展覽館	協會主辦
09/18-09/23	德國漢諾威工具機展 2023 EMO Hannover 德國漢諾威展覽中心	
10/11-10/14	2023 Robotworld 韓國 首爾 KINTEX 展覽館 1-3 館	參展優惠
10/25-10/27	日本 AI 人工智慧應用展 (4th AI EXPO TOKYO)〔秋展〕 幕張展覽館	
10/25-10/27	日本國際機器人研發暨技術大展 (RoboDEX 2023) 名古屋展覽中心	組參展團
11/27-11/30	大灣區工業博覽會 (DMP) 深圳國際會展中心 (寶安新館)	參展優惠
11/29-12/02	日本國際機器人展 (iREX) 東京國際展示場 - 東館	組參展團 擬申請國貿局補助

2023 國際參訪行事曆	
5 月中	美國參訪團：參訪 + 參觀 AUTOMATE 展
6 月底	德國參訪團：參訪 + 參觀 AUTOMATICA 展 (規劃中)
11 月底	日本參訪團：參訪 + 參觀 iREX 展

★ 備註：本表籌組參展為預訂行程，將依實際獲得國貿局補助後執行，歡迎洽詢業務組
★ 聯繫電話：04-2358-1866 #14(Fion)、#22(Iris)、#26(Eva)

社團法人台灣智慧 自動化與機器人協會 — 112 年度課程資訊



開課時間	課程名稱	課程時數	開課地點
02/10	工業 4.0 智慧製造技術概論	6	台中
02/17	物流、倉儲高效邏輯規劃	6	台中
03/02-03/03	AI 智慧物流系統軟體實作演練	12	台中
03/09-03/10	自動倉儲 AGV 的 SLAM 與導航 (ROS SLAM & NAVIGATION)	12	台中
03/16-03/17	精度定位與量測原理實務培訓班	12	台中
03/23-03/24	伺服流體傳動控制技術應用	12	台中
03/30-03/31	智慧機械手臂技術開發與實務應用培訓班	12	台中
04/06-04/07	PLC 與人機介面應用操作實務	12	新北
04/13-04/14	機械設計與公差設計應用實務	12	台中
04/20-4/21	智慧生產數據分析	12	台中
04/27-04/28	智慧自動化系統規劃及 AI 數位模擬分析	12	新北
05/04-05/05	機器伺服控制設計實務	12	台中
05/11-05/12	視覺感測技術與 AI 影像處理應用實務	12	新北
05/25-05/26	物聯網實務：工具機機台數據資產與效能控管	12	台中
06/01-06/02	自動化物流系統與 AGV 智慧搬運	12	台中
06/08-06/09	工具機零組件選配實務	12	台中
06/15-06/16	工具機結構材料選用	12	台中
06/29-06/30	機器人工程師實務應用培訓班	12	台中
07/06-07/07	工具機自動化設計與系統整合實務	12	台中
07/20-07/21	工業用機械手臂與工具機整合實作培訓班	12	台中
07/27-07/28	工具機機台校正與最佳化	12	台中
08/03-08/04	AOI 與視覺感測技術應用實務	12	台中
08/10-08/11	工具機切削技術數位雙生培訓班	12	台中
08/17-08/18	工業物聯網 IIOT 與軟硬體應用	12	新北
08/31-09/01	智慧機器人與機器人作業系統 - 市場應用與系統實務之概述	12	台中
09/07-09/08	PLC 與人機介面應用操作實務	12	台中

◎ 更多課程請上網查詢：http://www.tairoa.org.tw/ ◎ 洽詢專線：04-23581866#51 陳小姐、#52 王小姐

- ★ 貴公司有培訓計畫及需求嗎？智動協會可提供您智慧自動化及機器人領域的「客製化」培訓課程規劃及辦理！歡迎您來電詢問企業包班詳情。
- ★ 智動協會提供海外人才培訓服務，歡迎企業及團體與我們連繫。
- ★ 智動協會保有課程更動權利，並設有最低開班人數 10 人；如未達開班標準，學員自付金額將全數退還。



課程詳情請掃 QR CODE

TAIROA 廣告宣傳服務

這是一本專屬服務智慧自動化及機器人領域的出版品，內容涵蓋產品技術發展、市場趨勢、展覽推廣、國際商情、創新拓銷、學術研究計畫推廣…等內容。我們同時提供廣告版面給廠商，紙本印刷與協會公開性活動（媒合會、展覽等）傳遞到各領域對智能化與機器人有興趣的企業手上，智動產業期刊為您創造最寬廣的廣告效果。

智動產業期刊廣告價目表

項目	一期 （指定 8 月）		一期 （限 3、6、12 月擇一）		二期 （限 3、6、12 月擇二）		全年度（四期）	
	會員	非會員	會員	非會員	會員	非會員	會員	非會員
封面	100,000	125,000	80,000	105,000	150,000	175,000	280,000	305,000
	* 加贈當期一篇主題稿件（須配合當季主題）							
	* 搭配 Automation Taipei & TAIROS 展期 2000 本以上發放							
項目	一期			二期		全年度（四期）		
	會員	非會員		會員	非會員	會員	非會員	
封底	70,000	95,000		130,000	155,000	240,000	265,000	
封面裡	50,000	75,000		90,000	115,000	160,000	185,000	
封底裡	50,000	75,000		90,000	115,000	160,000	185,000	
內頁廣告	30,000	55,000		50,000	75,000	92,000	117,000	
跨頁廣告	45,000	65,000		80,000	105,000	140,000	160,000	

備註 1. 廣告刊登連續超過 2 期 (含)，即享有原訂價 9 折 2. 價格優惠至 2023 年 12 月 31 日止 3. 會員以團體會員為主 幣值：TWD

TAIROA 網站 / B2B 平台廣告價目表

項目	會員	聯盟成員	非會員	期限 / 次數
協會官網活動公告	免費	X	X	1 季 / 1 次
LINE 社群	免費	X	X	不限次
協會每月電子報	15,000	15,000	20,000	3 次 / 季
協會官網大型橫幅 Banner	25,000	25,000	30,000	90 天
協會官網中央方形 Banner	25,000	25,000	30,000	90 天
小型橫幅 Banner (前 4 版位)	30,000	30,000	35,000	一年
小型橫幅 banner (後 6 版位)	20,000	20,000	30,000	一年
TAIROA B2B 首頁大型 Banner (含每月電子報)	15,000	20,000	25,000	30 天
	24,000	32,000	40,000	60 天
	34,000	45,000	56,000	90 天
TAIROA B2B 活動大型橫幅 Banner (含每月電子報)	10,000	15,000	20,000	30 天
	16,000	24,000	32,000	60 天
	22,000	34,000	45,000	90 天
TAIROA B2B 產業地圖 - 精選產品 (含每月電子報)	8,000	13,000	18,000	30 天
	12,800	20,800	28,800	60 天
	18,000	29,000	40,000	90 天
TAIROA B2B 虛擬展館 - 輪播 Banner (含每月電子報)	8,000	13,000	18,000	30 天
	12,800	20,800	28,800	60 天
	18,000	29,000	40,000	90 天
TAIROA B2B 產業消息 - 大型橫幅 Banner (含每月電子報)	8,000	13,000	18,000	30 天
	12,800	20,800	28,800	60 天
	18,000	29,000	40,000	90 天
TAIROA B2B 產業消息 - 新聞稿曝光 (含每月電子報 + 推薦文章置放)	免費	免費	8,000	1 / 季
	8,000	9,600	12,800	2 篇
	10,000	15,000	18,000	3 篇

項目	會員	聯盟成員	非會員	期限 / 次數
TAIROA B2B 活動上架 (含報名系統 + 講者預約系統 + 每月電子報)	30,000	35,000	50,000	1 場
	48,000	56,000	80,000	2 場
	68,000	78,000	112,000	3 場
TAIROA B2B 活動快訊 (EDM 發送)	15,000	20,000	25,000	1 次
	24,000	32,000	40,000	2 次
	34,000	45,000	56,000	3 次
TAIROA B2B 每月電子報大型橫幅 Banner	10,000	15,000	20,000	1 次
	16,000	24,000	32,000	2 次
	22,000	34,000	45,000	3 次
TAIROA B2B 每月電子報中央方形 Banner	8,000	13,000	18,000	1 次
	12,800	20,800	28,800	2 次
	18,000	29,000	40,000	3 次

幣值：TWD

廣告諮詢聯繫

社團法人台灣智慧自動化與機器人協會 張小姐
Taiwan Automation Intelligence and Robotics Association (TAIROA)
EMAIL: iris@tairoa.org.tw
住址: 台中市南屯區精科路 26 號 4 樓
電話: +886-4-2358-1866 # 22
傳真: +886-4-2358-1566
協會網址: www.tairoa.org.tw



服務型機器人聯盟
Service Robot Alliance

成軍於2018年8月，由台灣智慧自動化與機器人協會(TAIROA)與資策會數位服務創新研究所發起，是目前國內結合產業發展的第一個服務型機器人組織，已超過80家業者成為聯盟成員。聯盟期望整合服務型機器人產業鏈的上中下游資源，加速擴大多元場域應用及提升服務價值，以團體戰方式進軍國內外市場。歡迎攜手加入服務型機器人聯盟！



立即加入
服務型機器人聯盟



109 年 串聯產官研產業發展拓銷



照片由左至右為 ROS 機器人工作坊、台韓線上交流會、ROSCON 社群交流活動、ROS 機器人工作坊 DEMODAY

110 年 攜手場域公協會開辦多元活動



照片由左至右為 ROBOCOM 服務型機器人創意實證競賽徵件說明會、台日照護機器人交流會、智慧服務推動委員會

為使產業交流更多元與不設限，

智慧自動化產業期刊自 105 年 3 月改由台灣智慧自動化與機器人協會發行，

這是一本專屬服務智慧自動化及機舉人領域的出版品，

內容涵蓋產品技術發展、市場趨勢、展覽推廣、國際商情、創新拓銷、學術研究計畫推廣…等內容。

刊 期 全年 4 期
發行時段 3、6、8、12 月
發行區域 臺灣、大陸
印 刷 量 1,000-3,000 (視活動與展會量而有所調整)

發行對象 智慧自動化及機器人、各產業機械加工 與製造業等跨產業之經營者、高階主管、採購及行銷人員。

報導內容 包含智動化及機器人產業最新訊息與技術發展、產學合作、市場策略與應用、焦點展會觀察與最新相關統計資料等。

■ 訂閱聯繫

台灣智慧自動化與機器人協會 - 張小姐

電話：04-2358-1866 傳真：04-2358-1566

Email：iris@tairoa.org.tw

■ 付款資訊

銀行：玉山銀行大墩分行

帳號：0288-940-027-199

戶名：台灣智慧自動化與機器人協會

備註：匯款後，敬請提供憑證供會計查核。

■ 廣告訂購提醒：期刊發行單位保有廣告刊登日期協調與是否受理刊登購買之權利。

訂閱戶基本資料表 (支票、電閱訂閱填寫)

訂閱【智慧自動化產業】電子期刊

☐ 一本價格 NT\$ 500 元

收件人： ☐ 先生 ☐ 小姐

收書信箱 (Email)：

收據抬頭： 統一編號：

收據地址：

連絡電話 (日)： 手機： 傳真：

您服務產業別是：

- | | | | | |
|-----------------------------------|-----------------------------------|-----------------------------------|-----------------------------------|---------------------------------------|
| ☐ 01. 半導體 | ☐ 05. 工具機類 | ☐ 09. 電子產業 | ☐ 13. 運輸物流 | ☐ 17. 其他 (請說明) |
| ☐ 02. 零組件 | ☐ 06. 自行車 | ☐ 10. 手工具 | ☐ 14. 學校 | |
| ☐ 03. 產業機械 | ☐ 07. 食品加工 | ☐ 11. 機械加工 | ☐ 15. 公協會 | |
| ☐ 04. 模具類 | ☐ 08. 五金 | ☐ 12. 醫療產業 | ☐ 16. 研發單位 | |

■ 填寫後放大傳真 04-23581566 或 email 至 iris@tairoa.org.tw

掌握未來趨勢

「機器人工程師」「自動化工程師」證照

全台首創機器手臂術科考試

原理 + 實作 + 證照 = 贏得就業先機

機器人術科考試方式及合格場域資訊
請見官網考試資格及規定



學科考試日程

證照名稱	考試時間	報名時間
「機器人工程師」證照 「自動化工程師」證照	5月/11月	3-4月/9-10月



◆ 機器人工程師及自動化工程師書籍



更多購買資訊及證照考試內容請至協會官網查詢
社團法人台灣智慧自動化與機器人協會 www.tairoa.org.tw



智慧製造 X 資安

www.tairoa.org.tw

TAIROA 台中

40852 台中市南屯區精科路 26 號 4 樓
4F., No. 26, Jingke Rd., Nantun Dist., Taichung City 40852, Taiwan
TEL : 886-4-2358-1866 FAX : 04-2358-1566
EMAIL : service@tairoa.org.tw

TAIROA 台北

10059 台北市新生南路一段 50 號 6 樓 603 室
Rm. 603, 6F., No 50, Sec. 1, Xincheng S. Rd., Zhongzheng Dist., Taipei City 100, Taiwan
TEL : 886-2-2393-1413 FAX : 02-2393-1405
EMAIL : service@tairoa.org.tw



印刷品 如無法投遞，請退回至：台中市南屯區精科路 26 號 4 樓

定價
NT\$500

