「智慧邊緣」生意盎然！擴展&資安成角力關鍵

■文：任芷萍

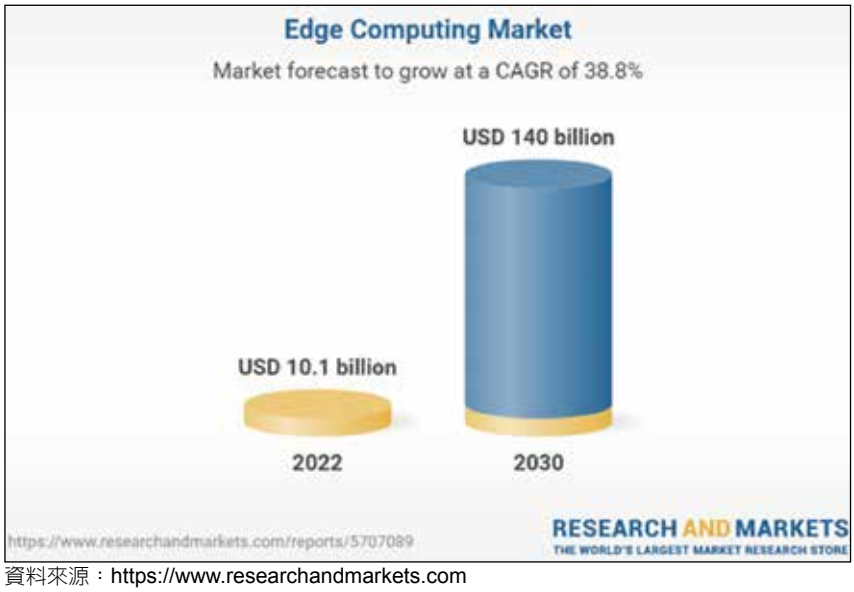
邊緣運算 (Edge Computing) 正處於快速上升時期！就連雲端服務商都不得不積極搶攻邊緣大餅。亞馬遜 (Amazon) 公開宣稱：前所未有的複雜性和資料規模已超過網路能力，邊緣運算讓企業能更有效地收集和分析其原始資料，協助組織提高安全性和效能、自動化程序並改善使用者體驗。研調機構 ResearchAndMarkets 去年底發佈報告指出，2030 年全球邊緣運算市值預估將從 2022 年的 101 億美元成長至 1,400 億美元，期間年複合成長率 (CAGR) 高達 38.8%，而物聯網 (IoT) 和連接設備的採用正在顯著影響市場。

提升速度、頻寬、安全，AI Edge 身懷即時洞察力

邊緣運算需求不斷增長的原因包括：人們對大數據分析的認識提高、智能設備和穿戴裝置數量增加以及電信行業支出不斷增加。研究顯示，依賴雲端運算的公司正轉向邊緣運算，因為它具有較低的延遲和成本可行性，而大企業看中數據處理靠近源頭可提高決策能力，亦正向邊緣靠攏。自動駕駛和聯網汽車的需求不斷增長，亦增加了邊緣運算解決方案和服務的銷量——聯網汽車提供有關惡劣天氣和道路狀況的資訊，協助駕駛員控制和導航。邊緣運算結合人工智慧 (AI) 的「智慧邊緣」(AI Edge) 可有效減少事故發生是支撐市場的重要因素。

COVID-19 促使許多企業開始遠程營運、使頻寬連接需求大增，亦成為邊緣運算的成長動力，旨在提升速度、頻寬和安全並獲取準確、即時的洞察力。大型企業是主要推手，因為所產生大量分散的數據需要進行分析並轉移到其他業務中——物聯網和工業物聯網 (IIoT) 所產生的大數據需要連接廣域網，可望促進分衆市場的增長。例如，需要體積小、儲存容量大的硬體支撐，智慧工廠與智慧城市皆為市場做出重大貢獻。在營運商網路內部或邊界處，智慧邊緣通常具有以下強項：低延遲、高頻寬、設備處理、數據卸載以及可靠的資源運用。

圖 1：2022 ～ 2030 年邊緣運算市值預估



資料來源：https://www.researchandmarkets.com

Maxim + OtoSense 助攻，ADI 打造智慧邊緣模組

終端用戶行業中，5G 和 IIoT 服務應用亦不斷增加；工業 4.0 從遺留系統、智能設備再到智慧工


照片人物：ADI 台灣區業務總監徐士杰

廠，皆為智慧邊緣平台開啓絶佳機會之窗。從 ADC/DAC 資料轉換器的核心優勢出發，亞德諾半導體 (ADI) 在收購美信 (Maxim) 後，對於連結實體 (physical) 和數位 (digital) 世界以及邊緣設備的認知有深入觀察。ADI 台灣區業務總監徐士杰表示，區域據點在將營運數據上傳總部資料中心前，藉由智慧邊緣先行篩選、預判將更有效率，包括定義哪些數據是確切有用的；在將日常視訊、音訊轉化成可供分析數據的過程，智慧邊緣位居要角。

例如，將它置於馬達上，持續偵測運轉資料就能預測機器健康狀態、供做預防性維護，而這個智慧邊緣設備也是台灣工業電腦業者的商機所在。事實上，ADI 目前有高達 50% 的營收是由工業市場所貢獻；自從將知名 AI 解決方案公司 OtoSense 納入旗下後，在工業監控的實力更為精進。OtoSense AI Edge 解決方案透過硬體和軟體優化生產環境，將診斷數據化為具體的操作指令或建議，讓用戶能預測維修週期，減少故障發生，實現諸如降低資產維護成本、延長設備壽命和增加正常執行時間等，避免意外停機。

ADI 第二塊高度看好的是汽車應用。徐士杰說明，受惠於汽車

圖 2：ADI OtoSense 智能馬達感測器可檢測設備異常和缺陷以便預測維修週期，避免工廠意外停機


資料來源：ADI；https://otosense.analog.com/

圖 3：ADI 智慧邊緣 MCU 特點

資料來源：ADI

自動化程度越來越高，感測器與邊緣設備亦隨之蓬勃，且正掀起產業革命。此外，消費電子與醫療級照護也是智慧邊緣的重點領域。為因應不同垂直應用所需，ADI 也從單純元件商轉型為解決方案供應商。為降低終端裝置直通雲端平台的負載，越來越多企業傾向在其間加入智慧邊緣 中介層，以提供可擴展、可靠、安全的高效控制和資源儲存。然而，智慧邊緣卻因缺乏安全框架而暗藏風險。徐士杰亦同意：「資安」幾乎是所有用戶共同的擔憂；若是單靠軟體防護，被駭危機高。

資安多一重保障！MCU 硬體安全碼建構獨特防護機制

ADI 在併購 Maxim 後也順勢取得微控制器 (MCU) 硬體資安防護能力，為邊緣設備多添一重保障。ADI 的安全微控制器憑藉其 ChipDNA PUF 電路所產生的金鑰可實現強大的防物理攻擊能力，確保系統保護的金鑰不落入駭客手

中。ADI 的安全微控制器是硬體解決方案，可補足軟體缺陷，且相較於在電腦上運行的複雜軟體，基於硬體的專門加速器速度更快！最重要的是，這些安全微控制器更同時具備低功耗、小尺寸的特色。簡言之，安全微控制器就如同額外的防護罩，將使用者關心的資料牢牢鎖在其中而不遭到任何洩漏。

NXP：解決「易用性」和「互通性」是當務之急

照片人物：恩智浦全球銷售執行副總裁 Ron Martino

2022 恩智浦半導體 (NXP) 技術論壇亦以「Enabling intelligence at the edge 推動智慧的邊緣」為題聚焦相關應用。恩智浦全球銷售執行副總裁 Ron Martino 認為，雲端運算加上安全、連結的邊緣智慧，讓許多裝置搭載運算、類比、連結能力與安全，推動並執行有意義的任務。節能、永續就是很好的例子，最佳化能源的生產、儲存、配送與使用，結合邊緣與雲端，不管是家庭、電網、車輛皆能有效率互動，以創意方式管理所有的能源活動。與其將所有數據皆上傳雲端處理會消耗大量能源，何不就近在本地處理或預處理？

「邊緣處理協同雲端處理」無疑是最佳解，也能及時理解環境或情境當下發生的事件，先決條件是：解決延遲、實現即時運算，同時要能高效率理解環境。再者，傳統資訊科技 (IT) 與營運科技 (OT) 系統無法無縫配合、系統架構也不同，未經最佳化就無法實現真正安全的資訊，保護個資、商業資料並防禦攻擊。智慧家庭更是如此，若想催生剛性需求——如：協助節省生活開銷、促進健康安全並簡化設備維護，首先要解決的是「易用性」和「互通性」。看好智慧家居和智慧城市應用，恩智浦在 2022 年年底推出一系列專為上述應用而設計的 MCU。

照片人物：恩智浦半導體資深行銷經理黃健洲

恩智浦資深行銷經理黃健洲介紹，他們面向智慧家居和智慧城市應用推出的系列產品，涵蓋四種不同基於 Arm Cortex-M 的 MCX 微控制器，共有 N、A、W、L 四個系列，皆構建在一個通用平台

表：恩智浦 MCX 產品

產品型號	特色
MCX N 系列 (高性能系列)	可滿足機械手臂、智慧電梯、智慧門鎖這類對智慧運算有更高預測性要求的設備，工作運行頻率為 150 ～ 250MHz，並首次將 NPU 和 DSP 置入 MCU，並嵌入恩智浦特有的安全系統 EdgeLock
MCX A 系列 (基準系列)	可滿足各類智慧家電產品的需求，作為入門款 MCU，工作頻率在 48 ～ 96MHz，內建計時器、低引腳數、單引腳電源，並對該系列之成本受限的應用進行優化
MCX W 系列 (無線連接系列)	整合 BLE 模組以及週邊器件，降低整個材料清單 (BOM) 與板載整合難度，可應用於如遊戲手把這樣需要無線連接能力的產品，工作頻率在 32 ～ 150MHz
MCX L 系列 (超低功耗系列)	滿足穿戴裝置等續航敏感的產品所需，整合原 LPC 低功耗技術，擁有超低的動態功耗和非常低功耗，工作頻率在 50 ～ 100MHz

資料來源：恩智浦

上並由 MCUXpresso 提供支援，非常適合需要一定水準的處理能力、又不消耗大量能源的邊緣運算應用；從入門級到整合神經處理器 (NPU) 與數位訊號處理器 (DSP) 的高性能 MCU，到集成無線連接能力和低功耗的型號一應俱全，可搭配的記憶體選擇亦多——從 4MB Flash (快閃記憶體) 到 1MB SRAM (靜態隨機存取記憶體) 皆是選項。

時間敏感網路：保證資料在最小時間精準傳輸

恩智浦認為，低延遲、高頻寬、彈性但具高隱私及安全、符合各項通訊協定，並有 AI 與機器學習 (ML) 功能是建購邊緣運算的要件。黃健洲以工業應用為例，工業 4.0 時代，工廠不再是一個簡單的流水線生產場所，而是發展成一個相互配合、具備強大邊緣運算、即時交互能力的龐大系統。要實現這樣的工作模式，便需要生產系統能融合機器學習能力、強大的視覺、工業級的即時通訊以及精準的自動化控制。恩智浦近日在官網發佈了技術展廳客戶體驗平台，其中在工業 4.0 背景下，演示的是融合機器學習與時間敏感網路 (TSN) 技術的智慧工廠運作模型。

「時間敏感網路」允許週期性與非週期性資料在同一網路傳輸，保證資料在準確時間內以最小時間進行傳輸。借助 TSN 技術，利用乙太網作為現場匯流排 (Fieldbus) 可實現高效流量分配，對於高優先順序的資料系統能自發傳輸，經由更精準的時間同步控制，可最大程度利用匯流排頻寬。以電機控制為例，恩智浦支援乙太網與 TSN 的工業級 MCU——i.MX RT1170，採用主頻達 1GHz 的 Cortex-M7 內核和主頻達 400MHz 的 Arm Cortex-M4 內核，自帶 2MB SRAM 且集成 MIPI 顯示與攝影機介面，可提供一定的即時監控與圖像捕捉能力。

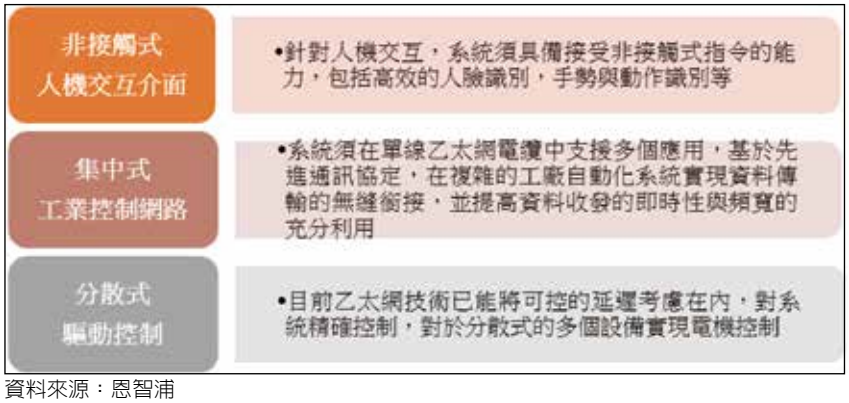
ETSI/EN 303 645：CE 物聯網之 Cybersecurity 專規

物聯網日益普及，網路資安 (Cybersecurity) 議題越發受到重視。挪威商聯廣驗證 (Nemko) 資深經理路龍輝表示，歐盟有鑑於此，已決議在原有 GDPR (一般資料保護規範) 之外，針對消費電子 (CE) 將資安納入 RED(Radio Equipment Directive) 管轄範疇，於 RED article 3.3 版本明訂無線通訊產品須避免網路環境誤用、影響原有網路品質及駭客入侵，且須確保個人資料和隱私權，擬於 2024 年 8 月 1 日生效。以兩年的產品生命週期 (EOL) 回推，亦即 2022 年 8 月開始設計的產品就須導入網路資安概念以求合規，屆時尚在銷售狀態中的庫存產品也無法豁免。

照片人物：挪威商聯廣驗證 (Nemko) 資深經理路龍輝

現行 CE 物聯網的網路資安基礎標準是 ETSI/EN 303 645，內容包括：無通用的預設密碼、漏洞測試及管理、敏感的參數和資料是否被安全儲存等。除了 GDPR 和 RED，還有一項正在草擬的強制法規亦須密切關注——EU Cyber

圖 4：智慧工廠生產系統必備特性



資料來源：恩智浦

照片人物：安華聯網 (Onward Security) 技術服務處副處長潘勤強

Resilience ACT (EUCRA)，未來可能取代上述 RED article 3.3，預估在 2025 年公告，兩年後強制實施。主要訴求為：須為產品軟體和韌體的版本、使用方式、內容、應用、更新時程羅列清單，針對漏洞測試或不當訊息使用須提供更新及修復方式，並提出管理報告；若抽測未過，最高罰金可達 1,500 萬歐元或該項產品年營收的 2.5% ！

值得留意的是，EUCRA 消費性產品允許廠商自我宣告，但工控、醫療、防爆等危險等級較高的產品須通過驗證機構授證才算數！但路龍輝強調，現階段對進軍歐洲的廠商而言，ETSI/EN 303 645 才是重點工作。安華聯網 (Onward Security) 技術服務處副處長潘勤強進一步說明，ETSI/EN 303 645 主要面向閘道器、偵測器、智慧手機系統元件等消費性物聯網產品而訂，隸屬 2019 年啓動的 EU Cybersecurity Act (EUCSA) 法案的基礎條款，而電池供電、運算力較低的產品另有規定，至於行動應用、雲端服務及第三方應用程式介面 (API) 則不在規範之內。

「無通用的預設密碼」強制要求，體現「硬編碼密碼」優越性

照片人物：安華聯網 (Onward Security) 核心技術處開發總監李育杰

其中，「無通用的預設密碼」明定：所有 CE 物聯網設備在使用密碼且處於出廠預設值以外的任何狀態時，密碼應不同或由使用者定義，且不可重置為通用預設密碼；若使用預先安裝的每個設備的唯一密碼，則應使用一種機制生成這些密碼，以降低對一類或類型設備的自動攻擊風險……，這也逐漸讓 ADI + Maxim 旗下 MCU「硬編碼密碼」(Hardcoded Passwords) 的優越性更被體現。安華聯網核心技術處開發總監李育杰補充，2023 年物聯網資安有四大態勢：1. 鎖定 IoT 裝置的攻擊增多；2. 資安法規趨嚴；3. 強化 IoT 裝置本身安全；4. 加強 IoT 網路安全。

為此，安華聯網推出資安合規自動化測試方案——Hercules SecDevice + SecSAM。前者作為黑箱測試工具，發崛 IoT 未知問題；後者是開源軟體 (OSS) 風險管理系統，透過分析產品組成並建立軟體物料清單 (SBOM) 找出並管理專案或產品之第三方元件的弱點、授權等問題並建議弱點修復解方，亦可介接至追蹤管理系統進行 CI／CD 整合。最後，李育杰分享今後物聯網資安走向：預估至 2025 年全球物聯網設備節點數 (不包括手機和電腦) 將達到 754 億個，但截至 2020 年，仍有 98% 的物聯網裝置流量未經加密，面臨嚴重資安威脅。

與此同時，Covid-19 疫情又成物聯網成長助力……，在在都突顯物聯網資安的刻不容緩。細究資安風險來源，有 26% 是由使用者習慣造成，當中又有 13% 歸因於密碼問題。也難怪，從通訊協定、矽智財 (IP)、晶片到系統層級相關業者，皆有志一同競相鞏固資安措施。 CTA