硬體「安全可信任根」為 IoT 嵌入系統構築護城河

■文：任芷萍

照片人物：英飛凌 (大中華區) 數位安全解決方案事業處經理江國揚

物聯網 (IoT) 的概念已推行多年，以車聯網 (V2X)、智慧家居、智慧製造、智慧醫療、穿戴裝置等為主要應用場景。隨著應用落地，業界對於完整架構——尤其是安全考量，越來越重視。嵌入式產品與人的生活息息相關，各種聯網方案帶來方便，也為駭客攻擊帶來了各種切入點。英飛凌 (Infineon) 大中華區數位安全解決方案事業處經理江國揚不諱言：「安全和方便從來都是矛盾的」，建議在產品設計之初，就做整體考量，尋求安全、方便及高性能之間的平衡。

IoT 安全防護範疇：設備自身、網路連接、資料傳輸

另一方面，物聯網產品的生命週期都在五年以上 (汽車甚至長達十年)；而技術發展讓駭客的攻擊手段也在不斷更新，深謀遠慮是必需的。江國揚指出，IoT 設備作為物聯網的一個端點，需從「設備自身、網路連接、資料傳輸」三方面提高安全防護能力。

- 設備自身：物聯網設備本身就是一個子系統，需要考慮安全啓動，即從開機到系統啓動過程設備的完整性校驗，確保設備本身運行在一個可信賴的而不是被篡改的系統上，另設備的韌體也要考慮安全升級問題；
- 網路連接：設備端需要確保連接到合法的雲端，而雲端或其他設備需要該設備時，同樣需要提供訪問者的合法身份，就需要實現雙向認證；
- 資料傳輸：敏感資料需要加密後再發送出去，確保資料不被協力廠商竊取。

他解釋，依據不同的攻擊目標，駭客會選擇不同的攻擊方式：軟體攻擊、通訊攻擊、硬體攻擊都是駭客可選的攻擊介面。就目前已知的攻擊案例來看，針對硬體的攻擊呈現日益上升的態勢，且此類攻擊對用戶帶來的影響通常更為隱蔽也更為直接。江國揚揭示，物聯網安全圍繞「機密性、認證性和完整性」三個主要概念：1. 敏感資料在傳輸與儲存的過程中是否受到保護？ 2. 如何鑑別物聯網系統 (設備、伺服器等) 的成員身份？是否透過數位技術偽裝？ 3. 物聯網元件是否受到損害或感染？

英飛凌認為，採用硬體安全晶片作為系統各組成部分的「安全可信任根」，是解決上述問題的最好方式。因此，開發出 OPTIGA Family 一系列產品，包括：OPTIGA TPM (可信平台模組) 標準化安全解決方案，以及 OPTIGA Trust 系列 (Turnkey 方案)。為經由蜂巢式無線實現安全的機器通訊 (M2M)，英飛凌為工業應用提供 SLM76 微控制器 (MCU) 和 SLM97 SOLID FLASH 產品；SLI 76 和 SLI 97 系列則是面向 eCall (emergency call) 服務、空中更新 (OTA) 和車聯網等汽車應用。這些安全晶片非常健全，具有擴展的溫

圖 1：英飛凌 SLM76 MCU 系列將 SIM 功能導入 M2M 應用；SLM 97 安全晶片則是專為要求高耐用性及穩固性的工業 M2M 應用而設計，採標準嵌入式 M2M 封裝與標準 SIM 卡模組

資料來源：英飛凌提供

度範圍規格，並符合工業和汽車產業標準。

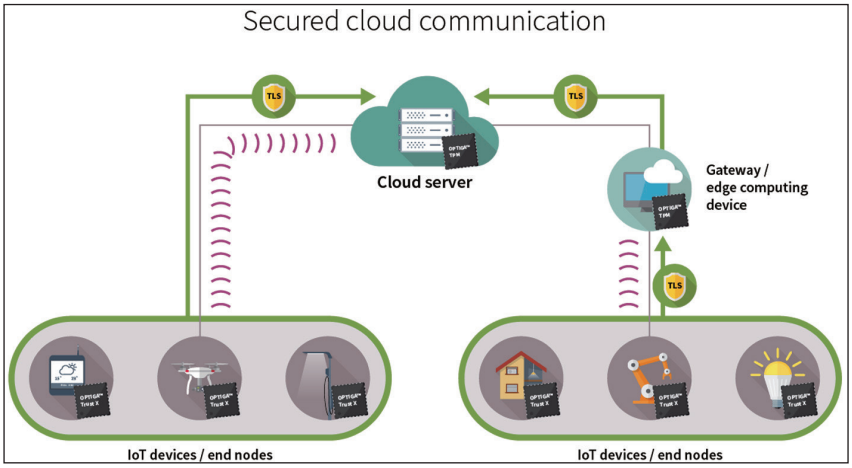
TPM「可信賴運算群組」用途：降低資料風險&生產損失

物聯網敦促英飛凌不斷拓展 TPM 應用領域。OPTIGA TPM 2.0 系列為商用電腦和資通訊、智慧網聯汽車及智慧工廠等提供基於 TPM「可信賴運算群組」(Trusted Computing Group, TCG) 硬體的安全方案；除傳統商業消費應用外，英飛凌也積極拓展 TPM 在工業和汽車行業的新興安全應用。為保護智慧工廠和雲端之間的通訊，英飛凌率先為工業 4.0 提供全球首個專門用於工業應用的 OPTIGA TPM 2.0，可保護工業 PC、雲端運算、工業控制器或邊緣運算閘道的完整性和身份，加強對智慧化連接／自動化工廠之敏感資料的安全訪問和保護。

江國揚重申，TPM 充當連接設備中敏感資料的信任根，可降低網路攻擊造成的資料風險和生產損失。用戶的利益不僅限於安全性，因為 TPM 還有助於縮短上市時間和降低工業應用程式的成本。借助英飛凌經過審核和認證的 TPM，工業設備製造商可達到更高的 IEC 62443 標準的安全級別並加速認證過程，還可透過安全的遠端軟體更新降低設備維護成本。該 TPM 的使用壽命可達二十年，能持續更新晶片韌體、應對工業環境可能遇到的長期安全風險，並滿足嚴格工業要求和品質——符合工業 JEDEC JESD47 標準。

車載電腦、聯網汽車則受益於 IT 行業經驗。在軟體、網路和雲端之間複雜的相互作用中，安全硬體為實現安全通訊奠定堅實基礎。為實現聯網汽車更堅固的網路安全，英飛凌亦率先將專門用於汽車應用場合的 TPM 投放全球市場；全新 OPTIGA TPM 2.0 涉及從聯網汽車的生產到回收等各個環節，汽車製造商可採用敏感的安全金鑰，確保以受保護的方式在汽車中分配存取權限、進行身份驗證和資料加密，還可對 TPM 進行韌體更新，在車輛整個使用壽命期間保持最新安全等級。

圖 2：英飛凌基於硬體的安全方案專為強化身份並保護連接設備的完整性而設計，涵蓋：雲端服務和平台提供商、ICT 伺服器設備／大功率邊緣設備 (如：閘道器) 製造商，以及連接工業／消費類 IoT 設備及感應器等 IoT 終端節點的設計人員



資料來源：英飛凌提供

圖 3：借助英飛凌經過審核和認證的 TPM，工業設備製造商可達到更高的 IEC 62443 標準的安全級別並加速認證過程

資料來源：英飛凌提供

怎麼防範隱私資料洩露、安全防護風險？

為加強物聯網設備的安全設計，英飛凌力倡藉由引入硬體安全晶片來分別加強雲端基礎設施、傳輸鏈路、終端設備的安全防護，形成端到端的閉環安全架構，以應對伴隨網路連接及設備智慧化而來的隱私資料洩露和安全防護風險。與此同時，英飛凌也強調凝聚生態系統內各個合作夥伴的價值主張和能力體現，在逐漸形成共識的前提下，能在標準演進、方案落地及商業化方面形成更加緊密的合作態勢，以更好地服務客戶並為其商業和品牌營運提供防護。從技術層面來說，越來越多的廠家正在加強嵌入式系統對分離式安全硬體晶片的理解和導入。

以 TPM 為例，其標準化組織 TCG 正在積極推動傳統 PC 行業之外的廣泛應用，而結合 5G 加快商業化進程、加強通訊設備的可信賴運算能力等議題越發受到關注。另有鑑於雲端和邊緣運算在工業物聯網 (IIoT)、車聯網等行業的深入，如何結合嚴苛的工業和車載環境進行安全架構部署，也是未來重要的技術演進趨勢。因此，英飛凌率先推出安全參考設計，並於 2019 年上半年發佈可量產的工規級和車規級安全晶片。整體而言，英飛凌的安全晶片具有高規格安全認證、獨立的硬體晶片與其他功能隔離，可為整體架構建置護城河，確保物聯網安全。 CTA

英飛凌雷達技術助力 Google Pixel 4 智慧型手機實現手勢控制功能

英飛凌科技開發出一款 60 GHz 雷達晶片，實現了全新的人機互動方式。利用整合式天線系統，它能以高精準度感知人與物的存在與移動，亦可測量距離與速度。該晶片是 Google Soli 技術的基石，目前已首次整合至智慧型手機中，實現了手勢控制。

英飛凌的雷達技術最初應用於汽車領域。數十年來，雷達感測器已在汽車駕駛過程中有效測量距離、速度及移動。英飛凌更進一步針對小型裝置進行功能開發。60 GHz 晶片是一個完整的雷達系統，其天線的佔用面積極小 (5 x 6.5 mm)，同時具備低功耗的特性。它可以感知房間內物體的移動，還能以極高的精準度測量毫米範圍內的物體距離。透過適當的軟體，就能將這些動作的數據轉換為功能，使用者無需觸碰裝置，即可透過手勢進行操控。」

英飛凌開發的感測器與晶片具有類似人類的感官功能，可識別環境，處理所獲得的數據。其目的在於實現輕鬆的互動方式，同時透用各種智慧化的操作功能，讓生活更便利、安全且環保。而在一個裝置中融合多個感測器，則可創建出全新的解決方案，例如測量並改善空氣品質，或實現防盜保護的智能化。除了語音控制助理，「智慧型」家電或穿戴式裝置、建築 (特別是智慧樓宇) 等，都將變得具有互動性。感測器可偵測房間內的人數或調整光源需求，以提升安全性與能源效率。