“硬”對資安威脅

■文：馬承信

物聯網安全無疑是當今世界最熱門的話題之一。隨著物聯網設備數量激增，安全性漏洞和大規模網路攻擊的威脅呈指數級增長。嵌入式安全性是物聯網的關鍵要求，僅靠不斷更新軟體已無法解決所有不安全硬體中存在的漏洞。因此，硬體元件能為裝置安全提供第一道防線。從低功耗感測器到高性能 IoT 裝置，晶片都必須內建安全機置以確保穩固的安全基礎，晶片之安全已成為最重要的問題。

萊迪思 Mach-NX FPGA 強化互聯網安全機制

如今多數互聯系統都需要網路保護恢復裝置 (Cyber Resilient Control) 的輔助，多數問題如網路保護恢復即時效能、韌體成為攻擊目標、硬體中實現可信任根都可同時掌握，保護廠商不再受到網路方面攻擊和盜竊。

為瞭解決所有市場區隔需要網路保護恢復和供應鏈安全，萊迪思 (Lattice) 近期推出安全控制 FPGA 系列第二代產品 Lattice Mach-NX。建立在 2019 年所推出的 Lattice MachXO3D 系列產品基礎上，Mach-NX FPGA 進一步強化安全功能和快速、高效能的處理能力，進而在未來的伺服器平臺、運算、通訊、工業和汽車系統中實現即時硬體可信任根 (HRoT)。

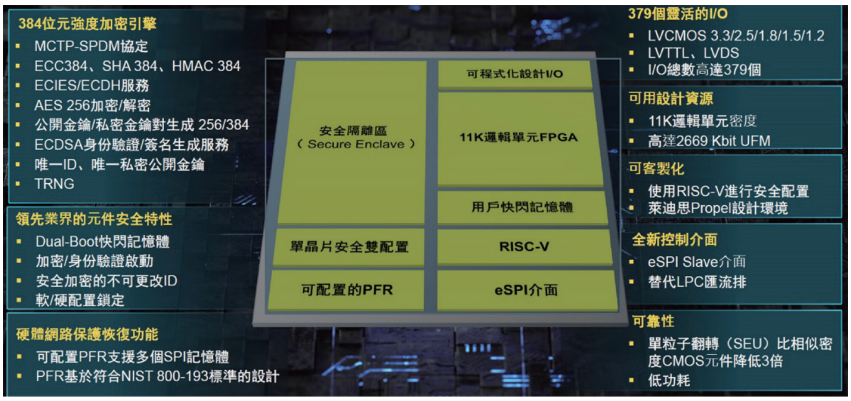
萊迪思半導體亞太區應用工程總監謝征帆表示，Mach-NX 是萊迪思在一年內推出第三款基於 Nexus 技術平臺的產品，Mach-NX 保護系統免於被未經授權的韌體存取，不僅是在啓動時建立硬體可信任根，還要求構建系統的元件在全球供應鏈中運輸時不受影響。配合 SupplyGuard 安全服務提供的額外保護，Mach-NX 可以在系統的整個生命週期內實現保護，從供應鏈運輸、首次產品組裝、最終產品運輸、整合，到產品的整個使用週期。

Mach-NX 目的是實現可程式化設計系統控制的新一代硬體安全元件。主要目標分為四大類：網路保護恢復系統控制、符合可靠的標準和協定、即時動態端對端的保護以及快速客製化。

謝征帆表示，以 Mach 系列產品的系統控制功能為基礎，結合了一塊安全隔離區 (Secure Enclave) (一種 384 位元基於硬體的先進加密引擎，支援可重新程式化設計的位元流保護) 以及一個邏輯單元 (LC) 和 I/O 模組。安全隔離區可保

照片人物：萊迪思半導體亞太區應用工程總監謝征帆

圖說： Mach-NX FPGA 分為幾大重點區，並延用傳統 FPGA 模塊以及功能



障韌體安全，LC 和 I/O 模組則實現電源管理和風扇控制等系統控制功能。Mach-NX FPGA 可以驗證並安裝 OTA(Over-the-air) 韌體更新，保證系統符合不斷發展的安全標準和協定。Mach-NX FPGA 的平行處理架構和 Dual-Boot 快閃記憶體配置實現近乎瞬時反應，便於偵測攻擊和從攻擊中恢復 (其效能等級超越其他硬體可信任根平臺，如 MCU)。Mach-NX FPGA 將支援 Lattice Sentry 解決方案集合，為一款包括客製化嵌入式軟體、參考設計、IP 和開發工具的強大組合，可加速實現符合 NIST 平臺韌體保護恢復 (PFR) 標準 (NIST SP-800-193) 的安全系統。

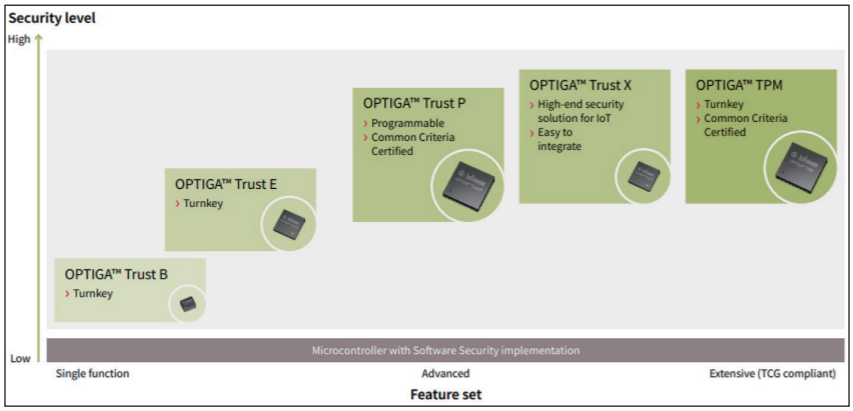
萊迪思表示，具備安全功能和效能的伺服器平臺，與惡意入侵者試圖利用韌體漏洞入侵，這兩者之間的鬥爭從未停歇。保護系統不僅需要即時的硬體可信任根，還須支援更強大的加密演算法，以及更新、更可靠的資料安全協定。

英飛淩採用專用安全晶片 OPTIGA 應對資安問題

來自英飛淩 OPTIGA 的安全硬體家族通過保護代碼的處理和存儲加密，故障和操縱檢測的手段，以及安全的代碼和資料存儲。英飛淩認為安全可以保護您的商業模式和 IP，避免服務中斷和品質問題，還可以建立對品牌的信任並名聲，助長增長和盈利能力。

為此，英飛淩 OPTIGA 系列

圖說：OPTIGA™ 系列安全級別



可提供易於集成，可擴展和可定制的交鑰匙解決方案，以應對的物聯網安全挑戰。OPTIGA 系列產品結合硬體安全晶片與軟體，以提升嵌入式系統的整體安全性，包括物聯網終端節點、邊緣閘道器及雲端伺服器。最新的安全技術可以節省部署通過避免計畫外的成本和收益。

OPTIGA 產品組合通過支援以下三個關鍵的安全關鍵功能：

- ■**認證**：OPTIGA 安全 IC 對人員進行身份驗證，設備，以便在授權之間交換資訊僅個人和設備
- ■**加密**：安全控制器通過以下方式保護敏感資訊對其進行加密並安全地存儲金鑰
- ■**誠信**：Infineon 的安全晶片檢查平臺，機器和設備完整性以識別操縱和檢測未經授權的變更，通過建立對安全架構的信任根

安全需求因其複雜而千差萬別。OPTIGA 系列安全解決方案易於整合到嵌入式系統中。基於硬體的安全解決方案從基本驗證擴展複雜實現的功能以滿足不斷變化的需求。

OPTIGA Trust 和 OPTIGA TPM 產品系列提供了行之有效的可靠的物聯網安全性能。交鑰匙或可程式設計 OPTIGA Trust 系列解決方案為您帶來便捷的整合好處，同時提供最合適的安全性級別以保護業務模型，流程知識和 IP。您可以依靠 OPTIGA Trust 產品來保護嵌入式系統，以防偽造，未經授權的產品，有意的攻擊和無意的攻擊操作員錯誤。OPTIGA Trust M 時，可在英飛淩的安全工廠將用於識別裝置的關鍵資產 (例如憑證和金鑰配對) 燒入晶片中。此統包式配置可藉由提供加密工具箱、受保護的 I^2C 介面及 GitHub 的開放原始碼，大幅減輕嵌入式系統的設計、整合及部署作業。此外，其高階安全晶片已通過 CC EAL6 + (高) 認證，並提供先進的非對稱加密。

Silicon Labs 借助 PUF 和 Secure Vault 技術軟硬兼施

Silicon Labs 推出安全功能新套件 Secure Vault 技術，是因應

IoT 開發人員面臨安全情勢的快速變化產生越來越大的壓力，以協助連接裝置製造商因應不斷提升的物聯網 (IoT) 安全威脅及監管壓力，提升裝置安全性並滿足不斷演變的法規要求。Silicon Labs 的 Wireless Gecko Series 2 平臺運用 Secure Vault 將一流的安全軟體功能與物理不可仿製功能 (PUF) 硬體技術相結合，藉以大幅降低 IoT 安全性漏洞和智慧財產權受損風險。Secure Vault 運用目前用於 IoT 無線 SoC 之最先進整合式硬體和軟體安全保護來簡化開發、加速產品上市時間，協助裝置製造商開發因應未來的產品。

圖說：Secure Vault 技術

Secure Vault 的硬體功能可為具備成本效益之無線 SoC 解決方案提供優化的安全級別。安全子系統 (包括專用核心、匯流排和記憶體) 係與主機處理器分離，獨特硬體分離設計，可將關鍵功能 (例如安全金鑰儲存管理及加密) 隔離至各自的功能區域中，進一步提高整個裝置安全性。新型安全功能組合非常適合致力於解決新興監管措施的公司，使其能因應如歐洲的 GDPR 和美國加州的 SB-327 等法規。

Secure Vault 以獨特的硬體和軟體功能組合提升 IoT 安全性，讓產品製造商更容易保護其品牌、設計和消費者數據。整合安全系統與無線 SoC 可協助設計人員簡化開發過程，並在產品生命週期內對連接裝置安全地進行無線 (OTA) 更新。藉由向連接產品提供正版、可信賴的軟體或韌體，將有助於減輕無法預料的漏洞、威脅和監管措施。

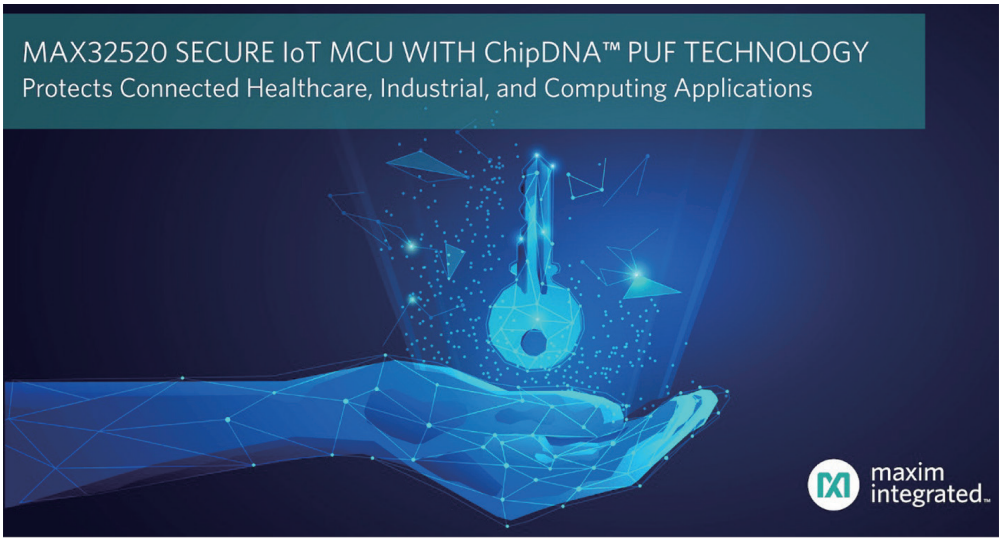
Maxim 的 IoT 微控制器已前置部署 ChipDNA PUF 金鑰保護

Maxim 生產了一種稱為 ChipDNA 的物理反複製技術 (Physically Unclonable Function；PUF) 技術。ChipDNA 根據 MOSFET 半導體元件的類比特性自然發生的隨機變化和失配而工作。這種隨機性源於：氧化物變化，閾值電壓之間的器件間失配，互連阻抗以及晶圓製造中通過不完美或不均勻的沉積和蝕刻步驟而存在的變化。ChipDNA 還通過獲得專利的方法進行操作，以確保每個 PUF 電路生成的唯一二進位值具有較高的加密品質，並保證在溫度，電壓和設備的使用壽命內具有可重複性。

基於 ChipDNA 的 MAX32520 透過其 PUF 技術提供多層保護，採用業內最先進的金鑰保護技術為加密操作提供最安全的金鑰。元件使用防篡改 PUF 金鑰進行快閃記憶體加密，安全導入功能支援信任根和串列快閃記憶體模擬。此外，當系統遭受惡意攻擊時，PUF 金鑰固有的物理防護功能無需電池即可主動銷毀金鑰。迄今為止，即使最安全的保護方案也需要在電池供電的前提下才能實現這一最高等級的金鑰保護。

Maxim 內建物理反複製技術 MAX32520 ChipDNA™ 安全 Arm Cortex-M4 微控制器，符合金融及政府應用要求的安全微控制器，可

圖說：採用 ChipDNA 技術的安全物聯網微控制器



廣泛用於 IoT、醫療健康、工業和計算系統。Maxim 的 PUF 技術提供多層保護，是最先進的高成效金鑰保護方案。

意法半導體旁路 STSAFE 安全元件提供安全保障

意法半導體 (ST) STSAFE-A110 安全元件 (Secure Element，SE) 導入新的資料安全功能，透過嚴格的驗真防偽技術，防止產品被仿造假冒，以保護物聯網 (IoT) 環境中的消費性和工業裝置。

該晶片配有嵌入式安全作業系統，而硬體透過了 Common Criteria Evaluation Assurance Level 5+ (EAL5+) 認證測試。每個晶片均配有唯一裝置識別碼和 X.509 證書，便於裝置安全連接到網路或其他設備。量身定制的命令集可確保強大設備身份驗證，以監視設備使用情況，以協助附近的主機建立秘密頻道 (TLS)，並維護主機平臺的完整性。

STSAFE-A110 具備最先進之經標準認證的安全保護功能，並為使用者提供雲端證書安全載入使用權限，能夠大量註冊連網裝置，確保只有授權的裝置才能使用線上服務。這個重要的安全個人化過程可以在意法半導體的安全工廠完成，使連網裝置製造過程中的保密資料管理變得更簡單和安全。

此外，意法半導體最新的 SE 安全模組與 STM32Cube 開發生態系統整合，可與需要身份驗證和安全連網能力的新 STM32 設計專案合併在一起。X-NUCLEO-SAFEA1 擴充板則可以加快應用研發速度，並支援所有的 STM32 Nucleo 開發板，以及免費的 X-CUBE-SAFEA1 和 X-CUBE-SBSFU 套裝軟體。STSAFE-A110 生態系統可實現無縫安全。

圖說：STSAFE-A110 無縫安全生態系統

法規與技術並進

目前各國都加快了資安相關的法規制定，已經落地的比如歐盟的 GDRP《通用資料保護條例》，國際系會 (ISA) 標準與聯邦諮詢安全管理法 (FISMA) 等等，針對 IoT 設備的安全問題，陸續有美國加州 SB327 法案、美國國家標準與技術研究院 (NIST) NISTIR 8259 以及歐洲電信協會 (ETSI) 的 TS 103645 等等。但這些法案引用的到 IC 上仍然過於籠統，缺乏明晰地規格，而難以區分。因此具體到產品上的時候，仍依各自對資安問題的理解進行設計。技術方面仍然以 RoT(root of trust)，ARM 核心則從 trustzone 結構走向 PSA 安全認證體系，最新的 ic “指紋” 級技術 ---PUF，我們看到像 Maxim Silcon Labs 公司亦開始部署產品。而 ST 半導體除了 Saft-A110 系列專用安全晶片之外，其最新的 STM32WL MCU 已經採用了自研的類似 trustzone 結構，增強 IoT 邊緣節點設備的安全功能。

另據某大廠透露的消息，ARM 有可能在下一代內核的 ip 中部署 PUF，以降低這一技術的使用門檻，進一步提升 IoT 設備的安全能力，同時也增加了中小型公司在這一領域的競爭力。 CTA