萊迪思助力硬體安全及網路終端 AI 設備效能提升

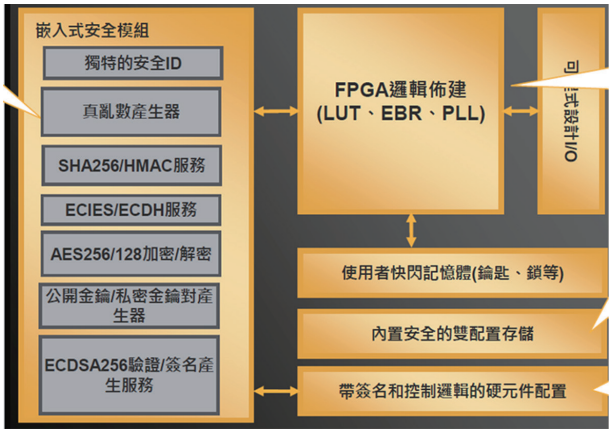
■文：馬承信

照片人物：萊迪思半導體亞太區事業發展協理 陳英仁

元件的韌體已逐漸成為網路攻擊最為常見的目標。在 2018 年，超過 30 億各類系統的晶片由於韌體安全性漏洞問題，面臨資料竊取等威脅。不安全的韌體還會因為分散式阻斷服務攻擊 (DDoS 攻擊)、設備篡改或破壞等隱憂，受損韌體的潛在危害尤其嚴重，因為這不僅會讓使用者資料易受到入侵，而且會對系統造成永久性損壞，大幅度的降低了使用者體驗，讓 OEM 廠商遭受財務損失和品牌聲譽受損等問題。

萊迪思半導體 (Lattice Semiconductor) 為此推出用於眾多應用中保障系統韌體安全的全新 MachXO3D FPGA。不安全的韌體會導致資料和 IP 盜竊、產品複製和過度構建以及設備遭未經授權篡改或劫持等問題。MachXO3D 可以在系統生命週期的各個階段 (從生產到系統報廢) 在元件韌體遭到未經授權的侵入時，對其保護、檢測和恢復。

萊迪思半導體亞太區事業發展協理陳英仁表示，MachXO3D 改進了生產過程中的元件配置和程式設計步驟。這些優化搭配 MachXO3D 的安全特性，保障了 MachXO3D 和合法韌體之間的安全通訊，從而較好地保護了系統。這種保護從系統的製造、運輸、安裝、運行到報廢整個生命週期中都能有效保護。



圖說：MachXO3D 可完美呈現安全與靈活性

IHS 預測，截至 2025 年，網路終端運行的設備數量將達到 400 億台。由於運行延遲、網路頻寬限制以及資料隱私等問題，OEM 廠商在設計即時線上的網路終端設備時希望能夠最小化傳輸到雲端進行分析的資料量。萊迪思 sensAI 的低功耗 AI 推理功能可以針對 OEM 的應用要求進行優化，幫助他們與現有設計無縫接軌。由於只需要發送相關資訊即可做進一步處理，使用本地智慧處理能夠降低雲端分析帶來的成本。

陳英仁表示，萊迪思開發 sensAI 是為了滿足網路終端 AI 設備日益增長的需求。sensAI 提供了全面性的硬體和軟體解決方案，是在為網路終端的智慧設備實現低功耗 (1mW-1W)、即時線上的人工智慧 (AI) 解決方案。未來將逐步拓展合作夥伴產業體系，包括設計服務和完整產品開發流程，加速產品上市。CTA