有無數理由推動打造值得信賴且安全無虞的物聯網世界

維安、安全及隱私是基本的必備需求

■作者：Marc Vauclair/ 恩智浦半導體資深安全系統架構師

我們在家中、車上、行動通訊裝置及付款系統使用的物聯網裝置，在醫療保健及工業領域的普及程度持續成長。一般預期物聯網裝置將在 2025 年之前達到 750 億個，而這些無數的連網裝置，將成為駭客的主要目標。因此我們必須努力打造物聯網，並使其成為安全無虞的「信賴網」。

最近 Mirai、Meltdown/Spectre、Roca、Heartbleed 及 Rowhammer 等知名的攻擊手法，讓各界對物聯網未來發展的信心蒙上陰影。前述攻擊不但可能造成財務影響，也可能威脅生命，因為物聯網裝置不僅負責感測環境，也會在其中實際運作。例如物聯網裝置可能會依據血糖機等其他物聯網裝置測量的血糖濃度，在人體運作胰島素幫浦。

物聯網挑戰

確保如此龐大數量的連網裝置擁有值得信賴的維安、安全及隱私，是一項非常艱困的挑戰。這類裝置配備感測器及制動器，在真實的實體世界中運作。例如所謂「智慧型」植入式胰島素幫浦，是一種物聯網裝置，可在預定的特定限制範圍內，於符合特定條件的情況下，自主決定將胰島素注入患者體內。在其他情況下，則由物聯網網路其他地方的監測儀要求注射胰島素。如果駭客成功危害這類幫浦適當運作的能力，就會對生命造成威脅。「維安」表示必須確保駭客無法成功執行惡意計畫。「安全」代表不論駭客是否成功，都要確保任何功能異常不會對生命造成威脅。「隱私」則是確保無數裝置處理的 ZB 規模資料，無法讓人公開取得。

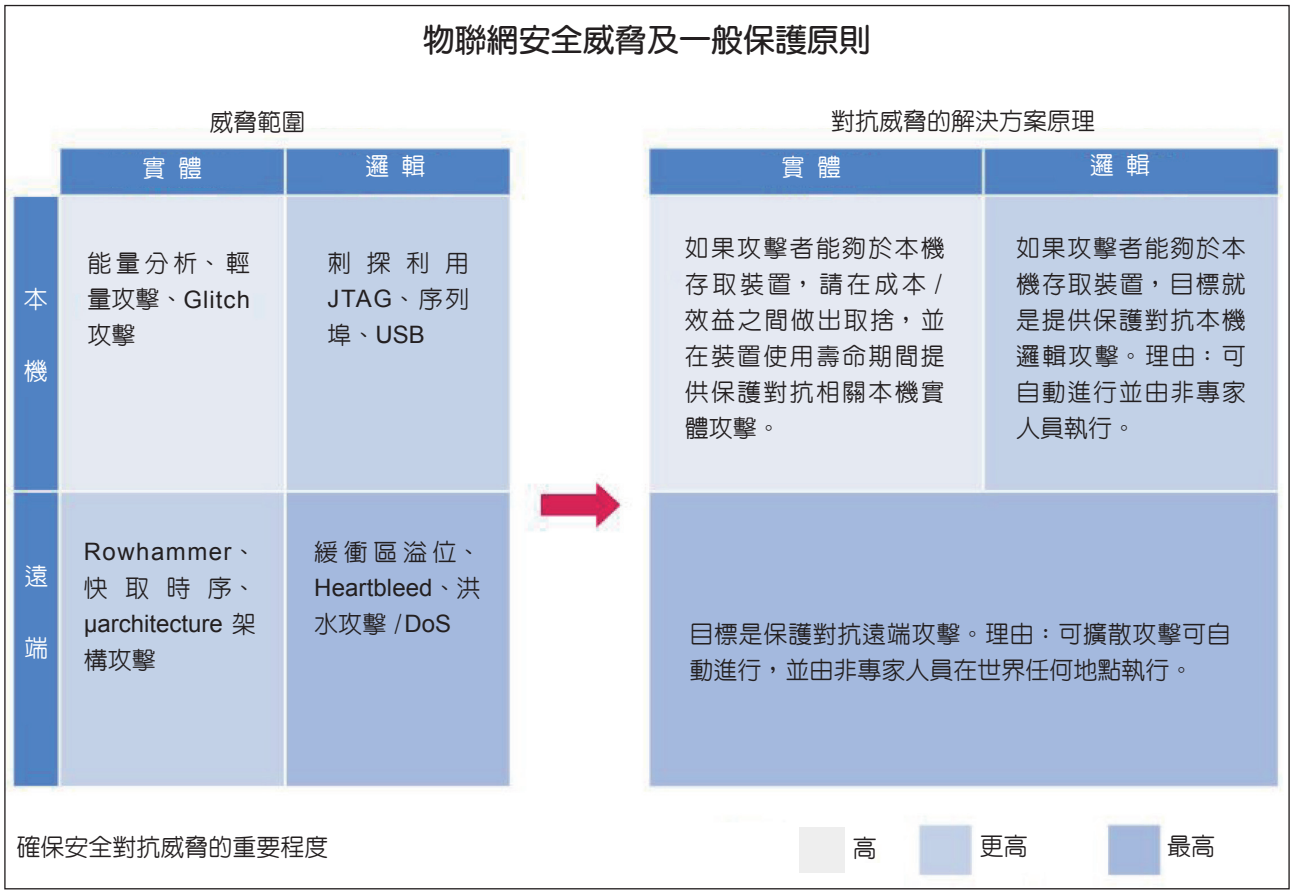
另一個例子則是未來的自動車：如果駭客成功從遠端控制所謂的線控驅動 (drive-by-wire) 功能，就能在不當時機變更車輛駕駛方向。前述裝置是以半自動的方式行動，在完成註冊、設定及初始化等程序後，就會開始執行工作，並盡可能減少與終端使用者之間的互動，以便營造易於使用的智慧型物聯網裝置體驗。

裝置所感測的資料，以及依據前述資料所做出的決定，都必須值得信賴，在裝置完整的使用壽命期間都必須如此。不過使用壽命無法預測，有些物聯網裝置可能使用 10 年以上。駭客技術與時俱進，每天都出現新的攻擊手法。攻擊範圍目前已經涵蓋攻擊系列的四個象限：「本機」和「遠端」以及「邏輯」和「實體」。

本機攻擊是以實體存取裝置的方式執行，而遠端攻擊則是透過網路連線於遠端傳送指令進行。執行本機攻擊所獲得的知識，可能用於進行未來的遠端攻擊。雖然擬定遠端攻擊可能需要相當多的專業知識，但這類攻擊可自動進行，並由單純的攻擊方大規模執行。這代表遠端攻擊是可擴散的。

遠端攻擊有可能從單一裝置起始，然後在短時間內影響數百萬個目標裝置。針對裝置、網際網路服務或組織進行的邏輯攻擊，是以刺探利用實作中

圖 1: 安全威脅的四象限矩陣



弱點的方式進行，主要位於軟體中。這類攻擊的執行方式，是存取有線及無線的標準介面，不但可自動執行，在熟悉作法之後，並不需要許多技能就可大規模進行。

實體攻擊駭進裝置的方式，是在裝置運作期間刺探利用已知或學習得知的實體特性，並破解維安措施的關鍵部分 (例如密碼金鑰)。遠端實體攻擊是於軟體實作，例如過去幾年興起的 Rowhammer、Meltdown/Spectre、快取攻擊和電源域控制器遠端攻擊。

這代表現今設計的裝置，應能預見因應未來 10 年以上依然未知的攻擊手法。這不是件容易的事，代表所有裝置都必須具備功能因應未來需求，在使用壽命期間執行安全及通過驗證的更新作業。

邁向安全無虞的「信賴網」

必須運用強力原則，推動物聯網成為安全無虞的「信賴網」：「維安設計」、「安全設計」及「隱私設計」等要素必須和諧結合，以達成「信賴網」的最終目標。

「維安設計」是指讓「維安」成為系統屬性，深植於系統全部零件及子零件的所有功能之中。這代表從構思新型物聯網裝置的「歸零日」開始，就要將「維安」因素列入考量。維安是以資料的機密性、完整性及驗證性為基礎，但也用於資料處理，因此會採用執行階段監控、安全開機及安全更新等機制。其中也納入找出攻擊的偵測可用性機制 (請記住沒有 100% 安全的系統)，可觸發必要的回復機制。

以上所述就是另一項維安基礎：恢復能力，此時「安全設計」就會在這樣的情境下發揮作用。不論攻擊者成功破壞裝置或系統的程度為何，裝置或系統行為都一定不能對生命或財務造成威脅。「維安設計」和「安全設計」代表裝置、系統或解決方

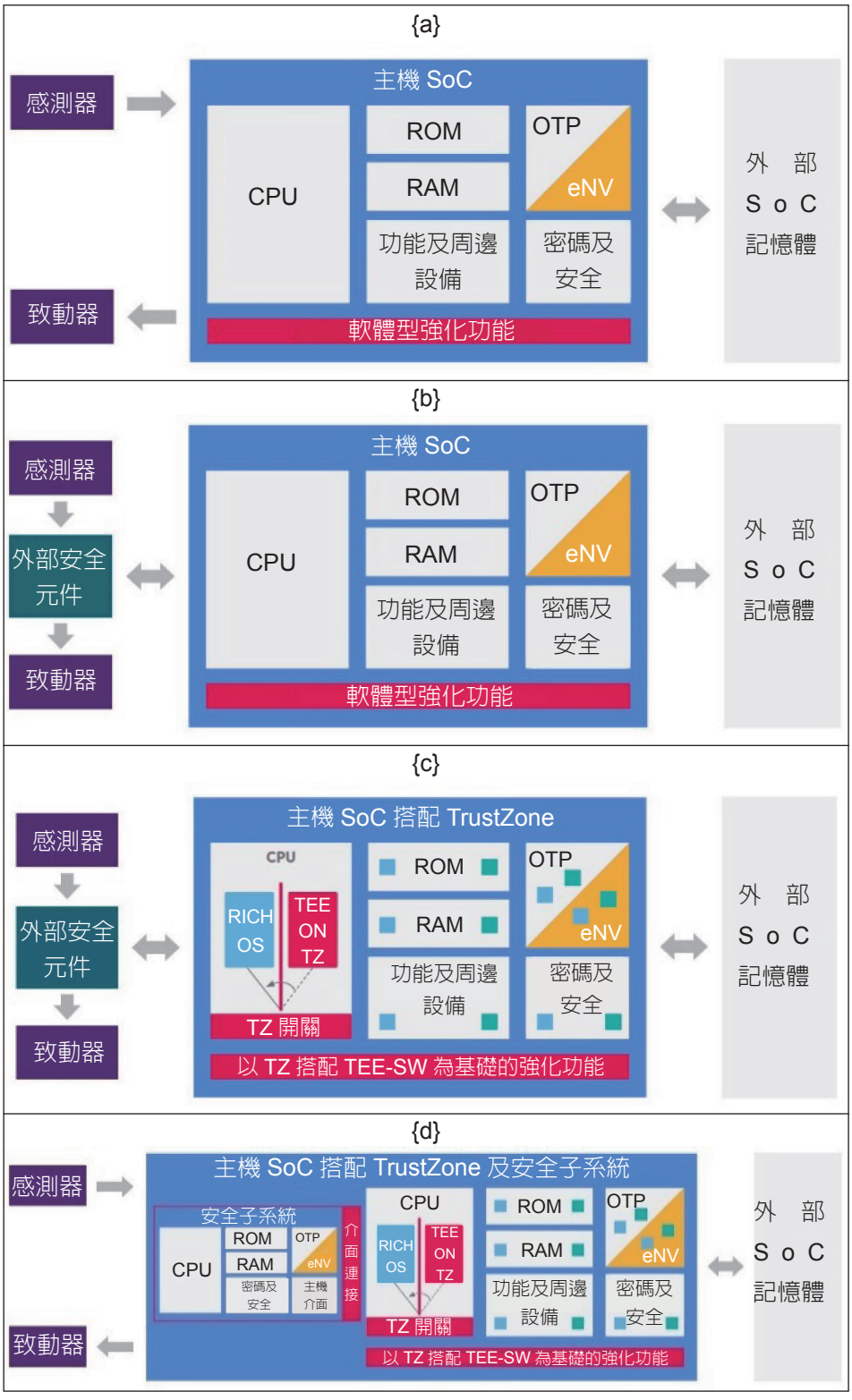
案廠商，都必須由外部的檢測實驗室及認證機構進行客觀評估，判定所達成的維安及安全層級。例如恩智浦這樣的公司，供應給政府機關使用的產品及付款解決方案，在通用標準認證方面都具有良好記錄。不過物聯網裝置安全認證情境持續改變，例如業界認可的現有方案，並不適合新興的物聯網生態系統。恩智浦、STMicroelectronics 及其他廠商為了協助提升整個業界的標準，在 GlobalPlatform 的支援下提出一項方案，要導入全新的「物聯網平台安全評估計畫」(SESIP) 認證方案，其中延續通用標準之中成熟且獲得信賴的特性，但也讓所有物聯網裝置在成本上能夠負擔。

「維安設計」的另一項重要特色，就是軟硬體都要列入考量，因為沒有理想方式能夠實作僅限軟體的物聯網安全措施，符合目前及未來的系統維安期望。

「隱私設計」是指產品／系統／解決方案採用維護隱私的設計方式。例如使用者的個人資料及其他項目，會以強制及／或適當的方式保證其匿名性及不可追溯性。「隱私」議題的重要性與日俱增：像是歐洲 GDPR 等法規就在全球許多地方實施，目的是保護物聯網裝置使用者及其他對象的隱私。

有一點很重要，就是其中提供的維安、安全及隱私，必須與詳細的風險及威脅分析結果進行比對，並且必須對額外功能的

圖 2：說明恩智浦半導體處理不同物聯網架構的方法。



成本提供可靠估價，以便與需要保護的價值進行比對。

「製造」及後續追蹤

提供安全無虞且維護隱私的產品，並不是只靠資料表的核對清單就能達成，而是以一致及成熟的安全方法，處理產品的架構、設計、實作、製造、測試、佈建及經銷事宜；此外也必須管理產品壽命終止事宜。

現在已經不可能存在只要出售就「安全無虞」的產品，而是必須以透明及快速回應安全事件的團隊持續支援產品。

在圖 2 中，可結合多種不同層級功能的產品達成維安目標：以 MCU 為基礎建構的精巧節點，利用安全開機及安全更新功能因應未來需求；以 MCU 及 MPU 為基礎建構的邊緣節點，則是以多核心及信賴子系統因應未來需求 (例如高階汽車閘道使用處理器整合車對基礎架構通訊 (V2X))；高階運算密集行動裝置的通訊或多核心應用程式處理，則是以竄改偵測、軟硬體隔離、硬體安全儲存及硬體密碼加速等功能因應未來需求。高階 MCU 及 MPU 的硬體防竄改安全功能，可利用高度安全的獨立嵌入式安全元件加以補強。外部安全元件最好直接連接感測器及致動器，以保證感測結果的真實性，而致動器只有在指令為真時才會採取行動。前述安全功能將於圖 5 概述。

圖 3: 智慧鎖

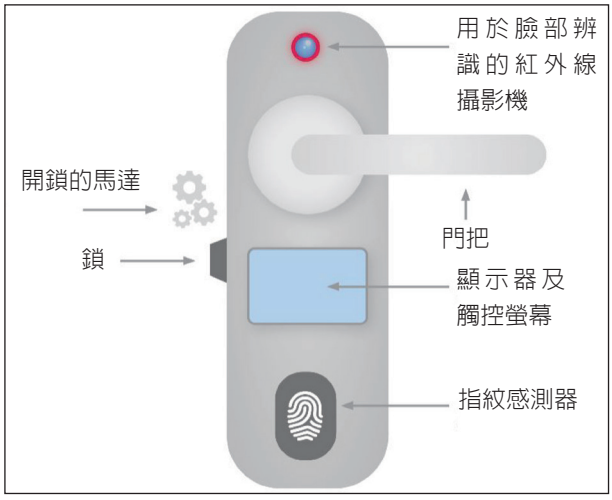


圖 4 ：智慧鎖安全生物辨識架構

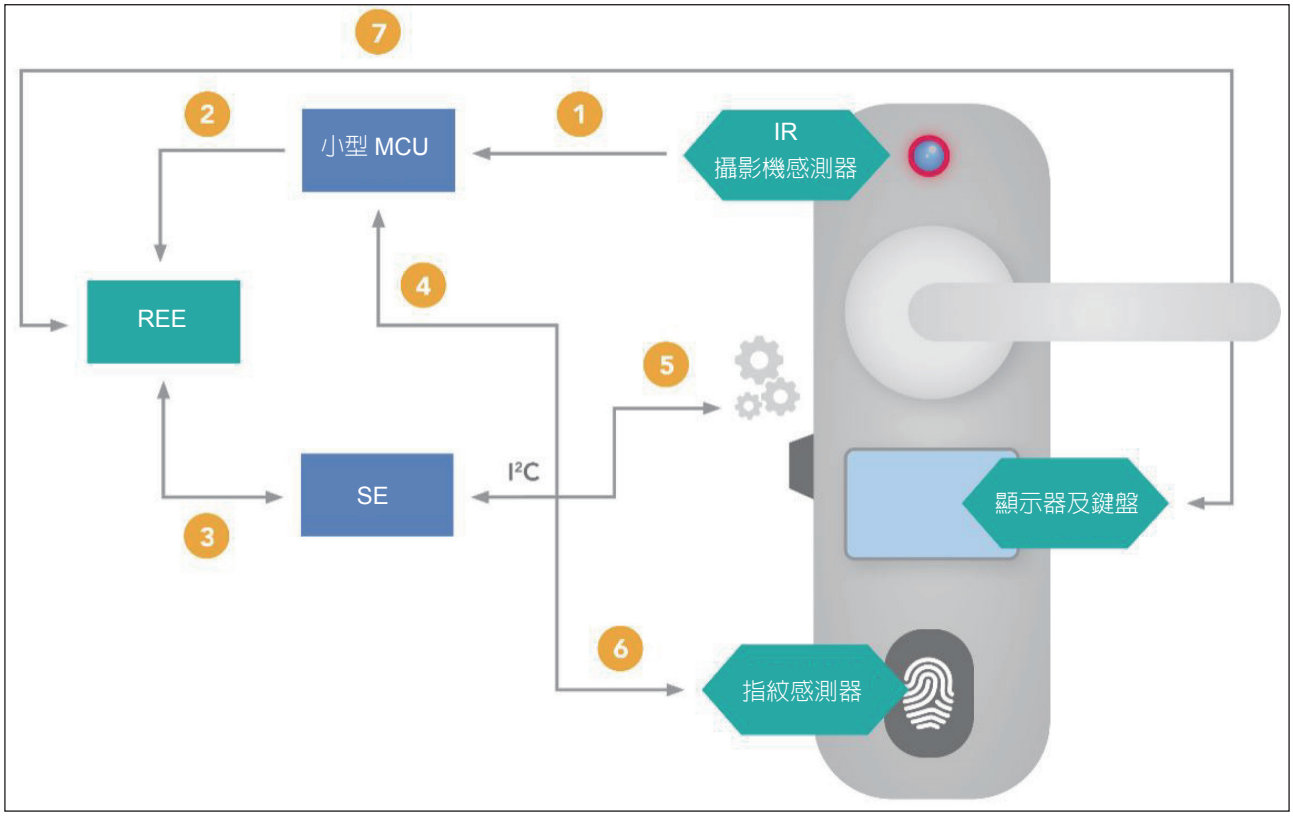
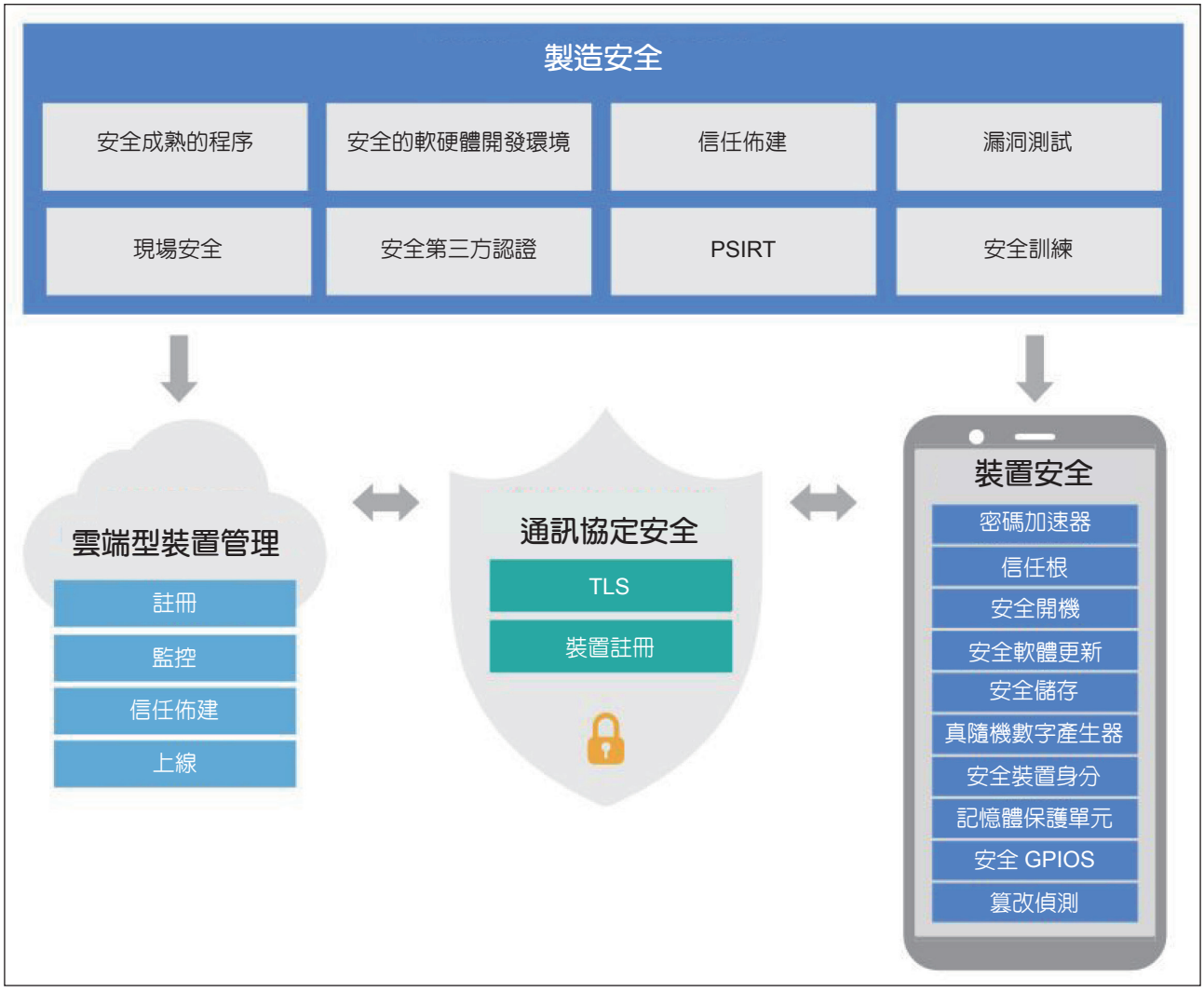


圖 5: 維安設計工具組



此外，RFID 型標記產品可協助部署安全物流鏈，對抗仿冒及複製等問題。

為了在製造裝置設計考量過程中和諧整合 MCU 及 MPU，也需要使用信賴佈建服務及雲端上線服務，以便在非特定安全環境中開發，但卻可整合至安全系統中。

圖 3 為智慧門鎖示意圖，圖 4 則畫出了使其安全無虞的架構。

嵌入式產業必須持續提升標準，遵循業界標準及最佳實務採取全方位的維安及安全方法，繼續朝向「信賴網」的目標邁進。

關於作者

Marc Vauclair 是資深安全系統架構師，擁有 35 年以上的豐富研發經驗，在恩智浦半導體主要負責創新的嵌入式系統安全架構。恩智浦針對物聯網、工業及汽車市場供應各種安全產品組合，並參與安全標準化組織及聯盟，協助推動安全無虞及網路安全的世界。如需本文更多詳細資訊，請參閱從物聯網邁向信賴網 (https://www.nxp.com/docs/en/white-paper/nxp-from-iot-to-iotrust-wp.pdf)。CTA