IAR 白皮書

物聯網產品安全解決方案

■ IAR

概述

本文針對目前嵌入式開發的需求、安全現狀總結出安全未來的展望，並提出可行的解決方案。目標讀者為嵌入式安全產業的開發者。

我們是嵌入式系統開發和安全解決方案和服務的全球領導者。我們致力於為客戶創造並保護已有的產品，同時持續投入創新以迎接未來的挑戰。

背景

近日，ENISA 在網路彈性法案 (Cybersecurity Act) 上的進一步動作讓越來越多的 IoT 開發人員關注到了產品的安全性能。

從目前的消費級物聯網產品安全標準 ETSI EN 303 645 V2.1.1 內容來看，安全範圍的定義與中國市場傳統上理解的網路安全 (Cybersecurity) 有所出入。除開傳統的網路安全特性 (例如密碼規範、安全通訊、網路安全檢測 / 防禦等) 還加入了另一類關乎嵌入式系統底層安全的要求，例如保證軟體更新 (Keep software updated)、安全敏感資訊的安全儲存 (Securely store sensitive security parameters)、確保軟體完整性 (Ensure software integrity)，可攻擊面的暴露最小化（Minimize exposed attack surfaces) 等要求。這些不屬於傳統網路安全範疇的要求，因為嵌入式系統不僅需要從系統外部防護網路攻擊，也要從嵌入式系統本身做防護，可以理解為嵌入式安全。

市場需求

貝恩公司 (Bain&Company) 的研究發現，如果企業客戶對網路安全風險的擔憂得到解決，他們會購買更多的物聯網設備，比他們可能購買的設備多至少 70%。此外，調查的 93% 的高管表示，他們會為安全性更好的設備平均多支付 22% 的費用 *。

2017 年麥肯錫的調查報告顯示，目前市場上對於物聯網安全的擔憂主要體現在四個方面：

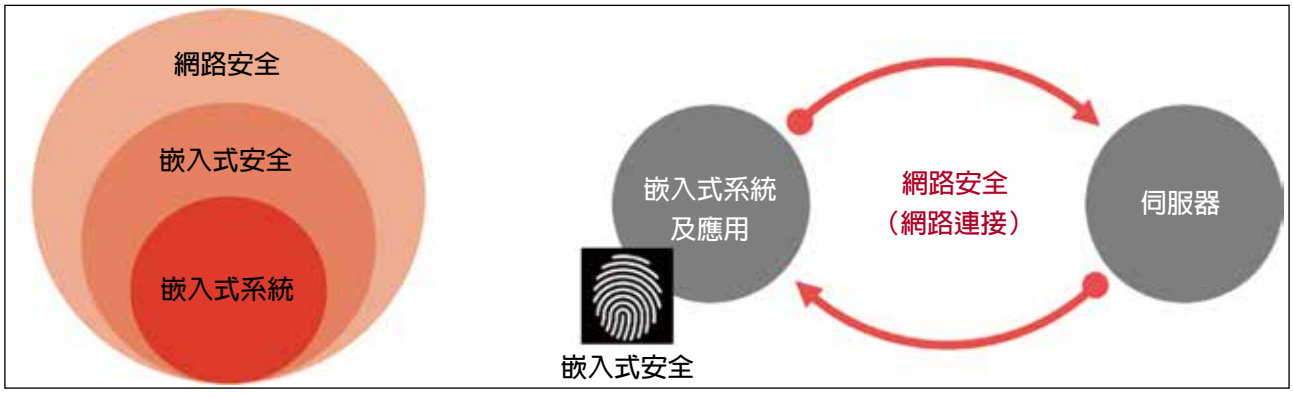
■技術成熟度差距；

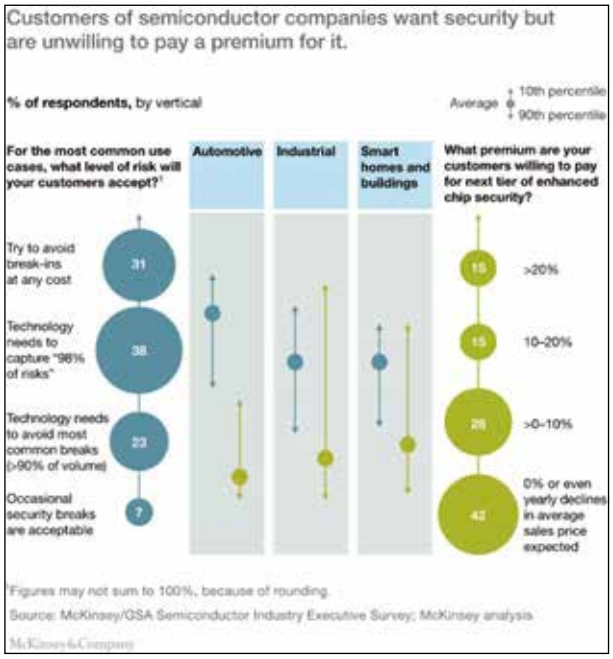
■標準不成熟；

■客戶和最終使用者將物聯網安全視為商品；

■半導體公司很難從安全中獲利。

從調查結果來看，93% 的用戶對物聯網安全有





需求，但是對於安全付費的意願較低，僅 15% 的使用者能夠為了安全接受產品售價 20% 的溢價。

結合需求和市場情況，如何用較低的成本實現安全，或者提高用戶為安全付費的意向，將是未來物聯網產業的發展的關鍵。

用戶價值

安全特性對於用戶來說也是有需求的，並且在不同行業中，安全需求的急迫性不同。從客戶付費意向的角度分析，客戶為安全買單的重要因素是對安全所能創造的價值的認可。

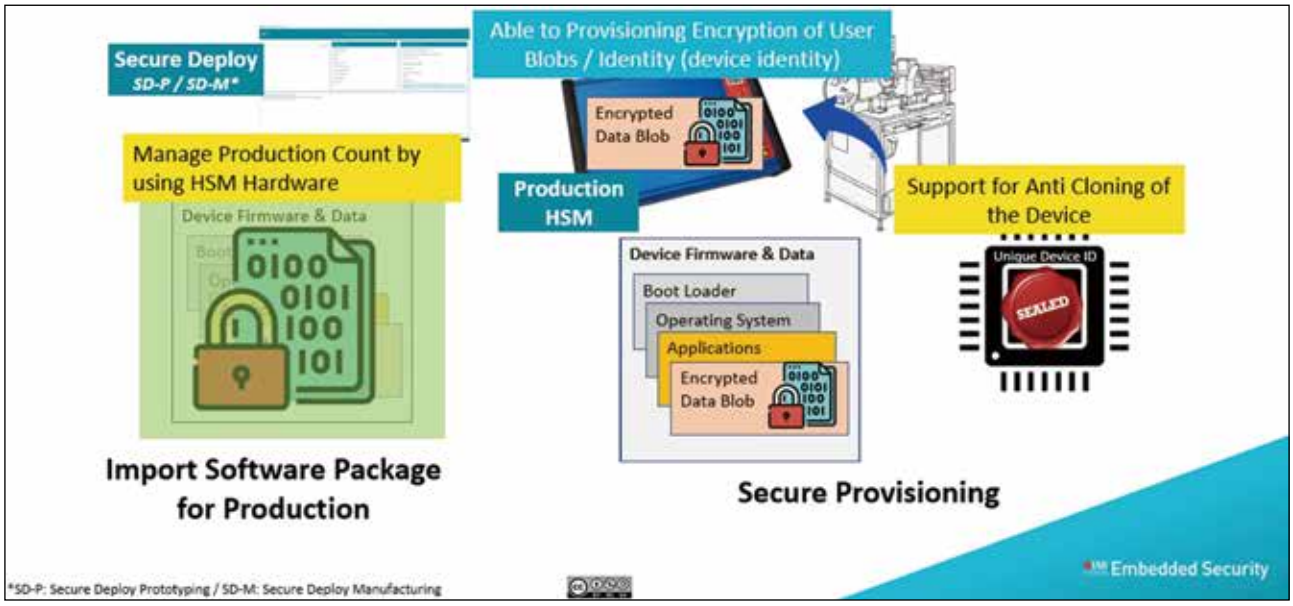
從產業上看，對於人身和財產有安全風險的行業更願意為安全付費。

例如在企業用 IoT 的市場中，工業物聯網，商用資料中心，商用智慧建築，商用醫療設備等行業對於安全的需求顯著。在消費類 IoT 市場中，目前除了和人身安全有關的行業比較關注安全，其他非關鍵領域的安全功能例如用戶隱私保護等，用戶普遍付費意向較低。

廠商價值

從 IoT 產品 / 服務供應商的角度，如何從安全獲利一直是為產品部署安全功能的重要出發點。安全的價值往往在發生風險時才能評估，預先難以估算。但是從以往典型的安全事件中，可以確認的是安全問題造成的損失有大有小，從很小的個體損失，到巨大的商譽損失，都是可能的：

■個人隱私數據被盜取；
■個人財產、人身安全受損；
■公司財產受損；
■因安全問題造成的罰款



■公司商譽受損。

2019 年 6 月，全球最大飛機零件供應商之一 ASCO 的生產系統被駭客攻擊破壞，造成系統癱瘓，德國、美國、加拿大、比利時的工廠被迫關閉，上千名工人停工。

2019 年 6 月，伊朗軍事系統受到美國發動的網路攻擊，部分軍事指揮、控制系統和導彈控制系統受到破壞，國家安全受到嚴重威脅。

2019 年 3 月，Facebook 和環球易購旗下跨境電商網站 Gearbest 的使用者資訊洩露後，市場對其公司的信任度大打折扣。

如果按照風險評估，安全的價值將是是巨大的！為了維護市場地位，規避巨大風險，適當的安全措施是非常必要的。

安全特性的價值對於廠商來說，也可以保護廠商的 IP(智慧財產權)，這方面的價值目前是普遍的盲點。合理的安全設計不僅可以保護最終用戶，也可以防止廠商 IP 在生產環節被盜取，甚至可以透過安全功能來管控外包生產商，大幅降低廠商本身的生產成本和管理成本。

IAR 的 Embedded Security 方案中就包含 Embedded Security IP，可以協助廠商安心授權生產部分的工作給外包廠商，並且管控生產數量。

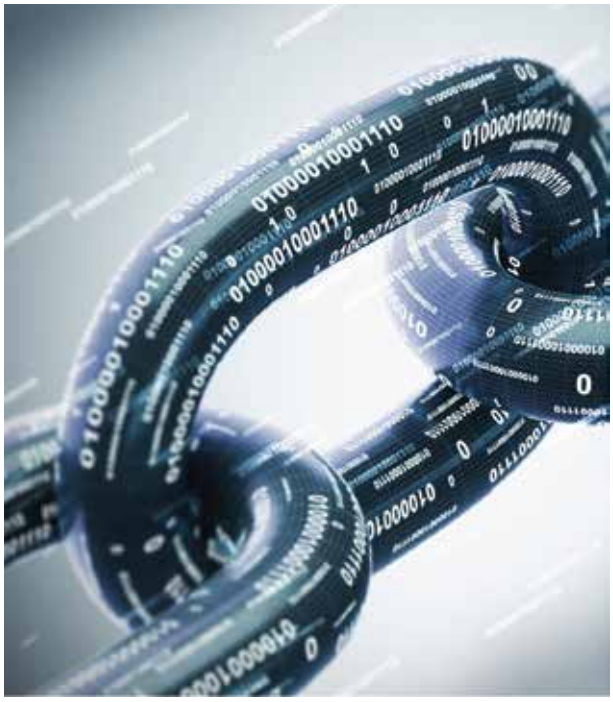
合規要求

面對市場對物聯網安全的需求，目前普遍的應對方式有兩種：

■部分企業為了保障自己的產品領先，保護商譽，應對部分客戶的安全需求，會主動部署安全功能；

■其他企業一般採取保守策略，等待市場普遍需求和強制標準的頒佈，再部署安全功能。

以上兩種應對方式雖然看起來不同，但是核心



出發點是一致的，即根據企業實際情況應對市場。當安全成為產業普遍需求，安全標準變成事實標準或強制標準的情況下，如何快速實現安全是關鍵。

然而安全的發展是長期的，在安全標準成為強制標準之前，企業符合安全標準的投資回報率應如何評估，一般可以參考安全問題造成的實際損失。在安全立法標準較為領先的歐美市場，在安全標準成為強制之 前，一般會有相關法規頒佈，法規中會有關於安全問題罰金的規定。目前的安全合規方面，體現在安全規 範上，很多行業已經有了較為成熟的規範。例如：

■在工業上，有國際標準 IEC 62443，我國也有工信部主導的《物聯網基礎安全標準體系建設指南》；

■醫療行業的 ISO 14971，也已經建立了對應的安全評估標準；

■汽車行業的 ISO 21434 和 R155，R156 標準；

■在物聯網行業，也有類似 PSA，SESIP，ETSI EN 303 645 等標準。

以上這些安全規範是針對行業的，而針對市場的法律規範，目前對應的安全立法仍在比較初步階段，且沒有明顯的產業屬性，法規涵蓋的市場面非常廣，且主要關注在安全紕漏的懲罰上。例如：

■**英國** — 產品安全法案《Product Security Law》規定安全問題的罰款上限可達 £10M 或企業全球收入的 4%；

■**歐盟** — 歐盟網路和資訊安全局 (ENISA) 正在制定相關標準，產品安全問題將產生罰金。相關標準將在 24 個月內開始實施；

■**美國** — 所有聯邦機構必須購買符合 NIST IR 8259 標準的設備；

■**歐盟** —《通用資料保護條例》(GDPR) 規定對違法企業的罰金最高可達 2000 萬歐元 (約合台幣 6.7 億元) 或者其全球營業額的 4%，以高者為準；

■**中國** —《關鍵資訊基礎設施安全保護條例》規定因資訊安全問題導致危害網路安全等後果的，對運營商處 10 萬元以上 100 萬元以下罰款，對直接負責的主管人員處 1 萬元以上 10 萬元以下罰款。

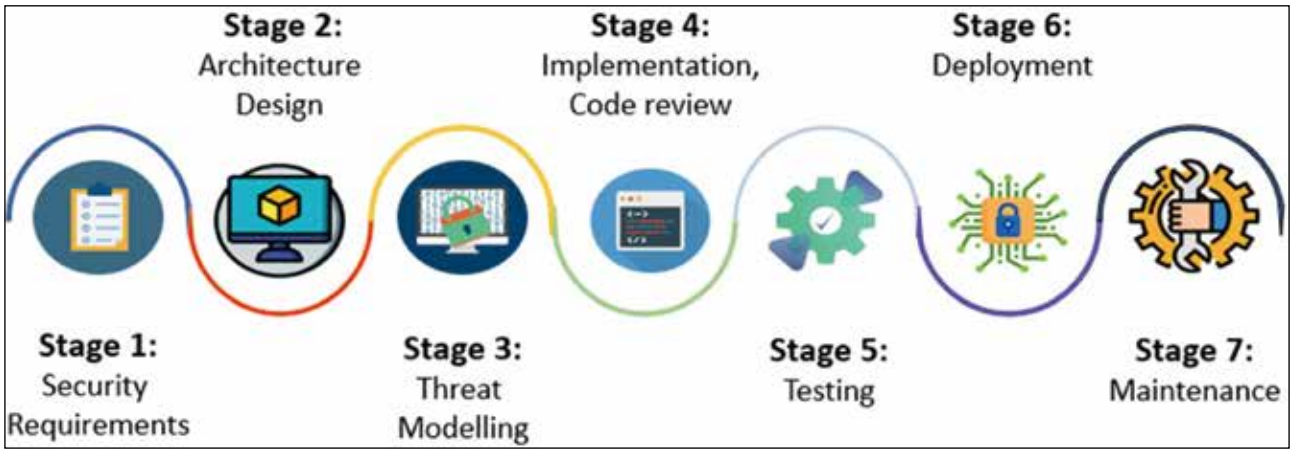
可以預見的是，隨著法規的推進，市場針對產品安全屬性的需求將會愈發明確，而如何解決目前供需雙方在成本、時間、實現複雜度上的矛盾，將是問題的關鍵。

痛點

如 2.1 章節中總結出的市場痛點，對於供應產品的廠商，面臨的具體問題是：

1. 客戶付費意願低，如何低成本實現安全；
2. 新的方案和建置所需要投入的週期長，且風險高，如何快速、低風險實現安全；
3. 多數廠商因為缺少專業的人員和知識基礎，無法系統性推進安全產品的開發和應用，如何獲取足夠的安全開發技術支援。

眾多廠商在面臨具體的安全需求時，到底怎麼應對需求，是從頭搭建安全框架，重新開發產品，



還是基於原來的項目上透過修補增加安全功能，其風險和投入都是未知的。過多的未知和不可控導致廠商對於安全的開發意願不高。

對於一個安全產品的開發，系統性地看可以分為 7 個階段：安全需求確認、安全架構設計、建立威脅模型、安全功能實現、測試、部署、維護。

開發人員是否掌握系統性的開發方法，或者目前在某個階段上遇到瓶頸，都可能導致整個專案進度停滯，這種延期對於商業專案的研發是難以接受的。如何讓整個專案的開發做到風險可控、成本可控、時間可控，是安全產品能否在市場上取得成功的關鍵。

另外，針對使用者付費意願較低的問題，整個產業鏈增強安全市場教育，提升使用者的安全意識，在產品宣傳上增加安全特性作為賣點，可以提升使用者的付費意識，將安全從成本轉化為利潤。

可行方案

針對目前安全產品的市場和研發痛點，IAR Embedded Security Solution (ESS) 為安全產品的

	用戶需求	IAR ESS 產品及服務
第一階段： 安全需求確認	分析 IoT 產品如何符合安全法規和認證標準 針對產品應用場景如何設計安全方案 SESIP 認證 PSA 合規	諮詢服務和方案匹配 諮詢服務和方案匹配 提供關鍵的安全性群組件，幫助滿足 SESIP 認證要求和 PSA 合規要求
第二階段： 安全架構設計	產品安全功能方案設計 防產品偽造，防盜取智慧財產權 安全連接和設備身份認證	全生命週期的產品安全方案框架 防偽造和正品認證方案 Security Profile 定義和基於 X.509 證書的網路安全身份認證體系
第三階段： 建立威脅模型	PKI 搭建和整合 通用網路攻擊和威脅的知識	公開金鑰基礎設施 (PKI) 整合 基於多年安全行業經驗的諮詢服務，IAR ESS 團隊是 IoT Security Foundation (IoT SF) 安全聯盟成員
第四階段： 安全功能實現	安全開發環境建立 安全啓動的實現	支援 IAR 開發環境和其他基於 Eclipse 的整合式開發環境 根據需求自動生成安全啓動管理器 (Secure Boot Manager)
第五階段： 測試	實驗室環境內測試軟體安全性 方將金鑰和證書 provisioning 流程建立和驗證與 DevSecOps 平台整合	使用者產品原型驗證階段的安全開發和生產 IAR ESS 提供相應的軟硬體套件 IAR ESS 提供 API 與協力廠商 DevSecOps 平台整合 IAR ESS 有成熟的量產方案和生態
第六階段： 部署	安全產品量產 防止竊盜生產，保護智慧財產權 為不支援安全啓動的設備添加安全屬性	整合的安全燒錄服務供應商、設備；同時也提供協力廠商整合服務 提供整套安全生產方案 提供安全服務庫，保護關鍵資料
第七階段： 維護	具備安全升級的能力	防版本 rollback 和安全升級方案

開發提供了靈活的開發解決方案，無論用戶處於任何開發階段，具體是什麼嵌入式安全的需求，都可以為用戶提供對應的解決方案和服務。

可行方案

IAR ESS 針對從開始設計就考慮了安全需求的用戶，提供了端對端的解決方案：

在研發方面，使用者可以根據自身需求快速客製 SBM (安全啓動管理器)，透過 IAR 的 Embedded Trust 平台自動生成既符合自身需求，又符合安全標準的 SBM 程式碼，透過 Embedded Trust 平台客製生成的代碼體積更小，啓動更快，且整個配置生成過程僅需幾分鐘，節省了長達數年的安全系統開發成本！

- 在安全生產方面，IAR 提供完善的安全量產方案，可以幫助用戶以最低成本，快速安全地完成產品生產。整個生產流程符合供應鏈安全的要求，並且杜絕了過度生產、盜生產、提取 Firmware 或關鍵資料等問題，保障了智慧財產權和資料產權。
- 從專案管控方面來看，使用 IAR Embedded Trust 方案可以安全無風險的達成安全目標，說明使用者專注在自身應用的開發。

針對開始未考慮安全需求的用戶，IAR 也提供 Embedded Security IP，協助使用者在後續彌補產品的安全特性。甚至 Embedded Security IP 可以為不具有安全模組 (例如 TrustZone) 的晶片提供安全能力。無論客戶是在開發中途需要添加安全功能，還是為已經完成開發的產品新增安全功能，Embedded Security IP 都可以提供方案。並且在安全生產方面，Embedded Security IP 也提供與 SFI 同樣的安全保護！

總結

對於嵌入式產品，尤其是物聯網產品而言，安全的需求是顯著的，無論是廠商和用戶，都對安全有所需求。但是市場的實際情況要求廠商以更低的成本、較快的速度、風險可控的方式實現產品的安全，並且教育用戶，提交用戶對安全的意識和付費意願。

IAR 憑藉在嵌入式開發和安全領域的豐富經驗，幫助嵌入式開發以最彈性、最快速，最低的成本實現安全需求，致力於嵌入式系統安全的普及，保障產業健康發展。

參考文獻：

- ISO/SAE 21434:2021 Road vehicles — Cybersecurity engineering
- ISO 14971:2019 Medical devices — Application of risk management to medical devices
- UN Regulation No. 155 - Cyber security and cyber security management system
- UN Regulation No. 156 - Software update and software update management system
- 5G C-IoT 終端安全測評體系和技術研究 http://www.gjbmj.gov.cn/n1/2021/1209/c411145-32304004.html
- 關鍵資訊基礎設施安全保護條例 http://www.gjbmj.gov.cn/n1/2021/0903/c409088-32217028.html
- 年度資訊安全事件盤點 http://www.gjbmj.gov.cn/n1/2020/0120/c409082-31557379.html CTA