安全快閃記憶體

網聯汽車和工業應用中安全問題的解決之道

隨著汽車和工業市場中自動化和互聯革命的推進，邊緣節點正在迅速成為網路攻擊的目標。軟體更新、遠端捕獲診斷資料以及遠端端點與基礎設施之間的通信變得越來越普遍，因此容易遭受網路攻擊和其它安全威脅。

■作者：Sandeep Krishnegowda
賽普拉斯半導體快閃記憶體產品總監

隨著半導體技術的進步，製程尺寸不斷縮小，將快閃記憶體嵌入到包含硬體安全模組 (HSM) 的 MCU 中也變得越來越困難，因此外置快閃記憶體的需求不斷增加。當快閃記憶體外置於 MCU 時，儲存的代碼和資料將更加容易受到攻擊，所以設備必須設計安全啓動流程和其它基礎設施，以確保儲存和檢索的內容可以信賴。

本文探討的是，當快閃記憶體外置於擁有 HSM 模組的 MCU 時，但仍然保持硬體信任根時，新一代安全設備的設計會面臨哪些挑戰和安全要求。本文涉及的其他內容還包括：加密安全存儲、快速安全啓動、安全固件遠端更新和管理合規。

引言

在一個日益趨於嵌入式和互聯的世界中，安全問題正在變得舉足輕重。每一個嵌入式系統都擴大了攻擊面，從設備和車輛到辦公室和工廠，一切都更加容易受到攻擊。在汽車電子、工業系統等應用中，功能安全上升到了至關重要的位置。

設計工程師深知，對安全和隱私與日俱增的關注已成為影響購買決策的一個主要因素。消費者和企業輕易採用新技術的日子已經一去不復返。如今，慎重取代了信任，這促使每個供應商都必須在某種程度上保證其產品和服務的安全性。

設計工程師還意識到，保障嵌入式系統的安全將變得越來越困難。原因是，隨著 SoC/MCU 在應對複雜的即時應用方面越來越強大，它們開始向較小尺寸的 CMOS 技術 (例如：16 奈米或 7 奈米) 過渡，以加快速度和降低功耗。但是在較小尺寸的條件下，目前還沒有可用的可重程式設計非易失性記憶體 (NVM) 技術。這就導致了 eFlash (MCU 的嵌入式快閃記憶體) 的整合，需要一種天然安全的架構，並且支持外置快閃記憶體。這就需要制定特殊的規則以確保其安全運行。

本文還分析了設計安全嵌入式系統的挑戰，包括嵌入式快閃記憶體的去集成所造成的挑戰。最後則探討了利用安全快閃記憶體保護嵌入式系統的新一代架構。

嵌入式快閃記憶體面臨去集成

為了應對日益增長的安全問題，晶片供應商將硬體安全模組 (HSM) 功能集成於 MCU。HSM 位於安全的處理環境中，其中含有一個基於硬體的信任根，用於保護敏感性資料、處理器狀態、開機載入程式、加密金鑰和應用安全服務代碼。嵌入式儲存 (eFlash 和 RAM) 也是安全處理環境可信邊界的重要組成部分，因此足以抵禦常見威脅。

片外儲存 (例如：外置快閃記憶體) 並非天然

可信，並且容易受到持續攻擊。應對措施一般是對外置快閃記憶體中的資料進行加密，然後在執行代碼之前，將其從外置快閃記憶體下載至 MCU 內置的 RAM 進行解密和驗證。這種方法儘管足夠強大，可以抵禦大多數攻擊，但是會導致性能下降 (啓動時有可能會出現問題) 和成本上升 (需要更多的內置 RAM 和更高的功率)，甚至有可能仍然容易受到持續攻擊 (例如：回滾攻擊)。

隨著 MCU 逐步應用于先進的技術節點以提升性能、提高性價比和降低功耗，快閃記憶體的去集成有可能帶來更大的威脅，以前被 eFlash 全部或部分克服的某些可信存儲挑戰也許會捲土重來。此外，由於嵌入式系統的普及所造成的威脅性環境也會帶來新的挑戰，而使用外置快閃記憶體則會讓這些挑戰變得更加難以克服。

為了確保外置快閃記憶體的安全，需要解決的主要威脅包括：

- 類比快閃記憶體晶片的授權資料訪問
- 篡改快閃記憶體晶片存儲的內容
- 重放通訊指令以解析快閃記憶體晶片的內容
- 在不安全環境進行設置以獲取金鑰
- 在快閃記憶體晶片通訊時進行窺探 (中間人) 攻擊
- 通過旁路攻擊或故障注入來公開 (獲取或觀察) 快閃記憶體晶片的內容和金鑰
- 以電子方式損害快閃記憶體晶片的完整性
- 克隆快閃記憶體晶片

為了解決上述及其他對外置快閃記憶體的威脅，有效地使其成為安全處理環境可信邊界的組成部分，該設備必須提供以下三種功能：

- 基於硬體的信任根，可防止攻擊對存儲的代碼和 / 或資料造成的修改、操縱、複製或其他潛在影響
- 通過 MCU 或雲端提供安全更新，綜合利用各種措施進行端到端保護，包括通過匯流排的加密驗證，通過讀 / 寫存取方法實現的安全區域，安全金鑰存儲空間，以及非易失性防回滾計數器
- 低成本，無需額外的安全設備 (例如：可信平臺模組)，也無需更改電路板，包括支援 x4 SPI 和 x8 HyperBus 標準

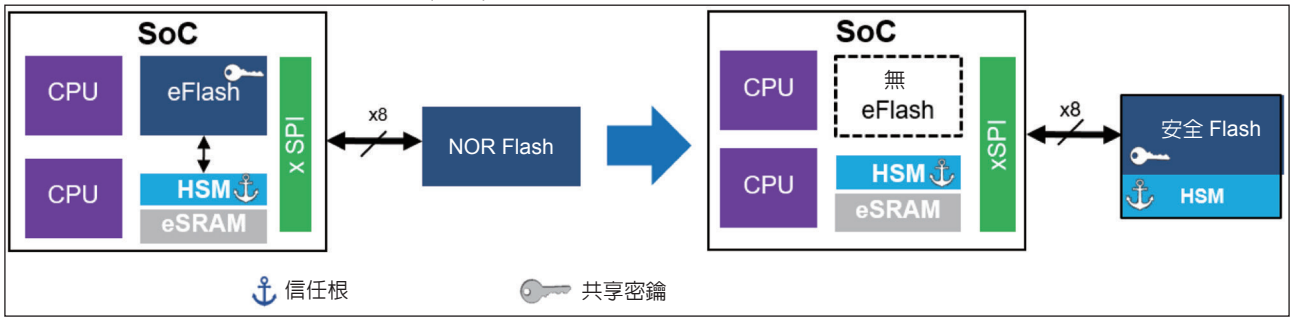
圖 1 顯示了專門設計的安全快閃記憶體 (見第 IV 章) 如何提供上述三種功能。實際上，安全快閃記憶體通過標準匯流排從外部擴展了 MCU 嵌入式快閃記憶體集成的 HSM 功能。還請注意，圖 1 也同時展示了安全快閃記憶體如何取代普通的 NOR 快閃記憶體，從而繼續使用現有的電路板。

值得一提的是，使用外置快閃記憶體還具有一些其他優勢，首先是它能夠更加輕鬆地適應不斷增加的代碼長度。嵌入式系統常用的標準快閃記憶體容量規格可以支援 1Gbit 甚至更大的存儲空間，遠高於 eFlash。外置快閃記憶體還可以容納更多的 CPU 內核 / 負載，以應對機器學習、人工智慧等複雜技術所需的更密集、更即時的處理。這些變化有助於簡化設計工作並加快產品上市，從而提供不同的型號以便更好地滿足價格、性能或其他標準方面的需求。

利用外置快閃記憶體設計安全的嵌入式系統

無論是使用 eFlash 還是外置快閃記憶體，設計安全的嵌入式系統都是一項越來越繁重的工作。

圖 1：eFlash 的去整合需要拓展硬件安全模塊 (HSM) 的功能，以確保外置快閃記憶體的安全性



這裡介紹一些重要的注意事項，以幫助指導設計和開發工作。

通常，針對端到端安全而設計的系統必須具備三大要素：

■保護機制，用於保護代碼和關鍵資料的完整性，防止各種方式的刪除、更改或破壞

■檢測機制，用於揭示代碼和／或關鍵資料何時被以某些未經授權的方式更改

■恢復機制，用於恢復被以某些未經授權的方式更改的代碼和／或關鍵資料的完整性

工程師設計的系統應能夠應對 STRIDE 模型已驗證的所有威脅。下表概述了此模型，它提供了一種實用的方法，以瞭解各種潛在的威脅以及如何使用各種安全措施來應對各種威脅。

安全產品設計需要建立基於信任根的可信執行環境 (TEE)。在使用所有元件和子系統之前，TEE 提供了驗證真實性和完整性的方法。創建這種安全設計的部分最佳方法如下：

■實施硬體信任根以創建安全基礎

■通過驗證和加密鞏固這一基礎

威脅	說明	安全規定
欺騙	假裝是別的人或別的東西	驗證，以確定消息發送者的身份
篡改	惡意修改資料	防篡改，以確保資料準確無誤，未經檢測和／或授權不得修改
否認	否認先前執行的操作	不可否認性，以確保消息發送者無法否認發送了消息
資訊洩露	向無存取權限的個人公開信息	保密性，以確保資訊不會提供或披露給未獲授權的各方
拒絕服務	拒絕向無效使用者提供服務	可用性，確保資訊不會提供或披露給未獲授權的各方
許可權提升	非特權用戶獲得特權	授權，以確保服務僅提供給已獲授權的各方

圖 2：實施信任根的方法有很多，不同設計均需權衡風險與成本

■保護所有連接、網路和雲元件的端到端價值鏈
■提供防禦旁路攻擊和故障注入技術的能力
■對系統進行獨立的漏洞和風險評估
■持續即時監控異常情況
■實施應對流程 (例如：安全更新)

圖 2 顯示在系統中實施信任根時如何權衡風險和成本。可以預料，基於軟體的設計成本最低，而安全性也最低。圖 2 沒有顯示不安全嵌入式系統的間接成本，而這些非常實際的成本可以輕鬆地證明，基於硬體的設計可以將安全性最大化。

美國國家標準技術研究院電腦安全資源中心解釋了在硬體中實施信任根的優勢：“ 信任根是執行特定關鍵安全功能的高度可靠的硬體、固件和軟體元件。因為信任根天然可信，所以必須通過設計來確保它們的安全。為此，許多信任根都在硬體中實施，這樣惡意軟體便無法篡改其提供的功能。”

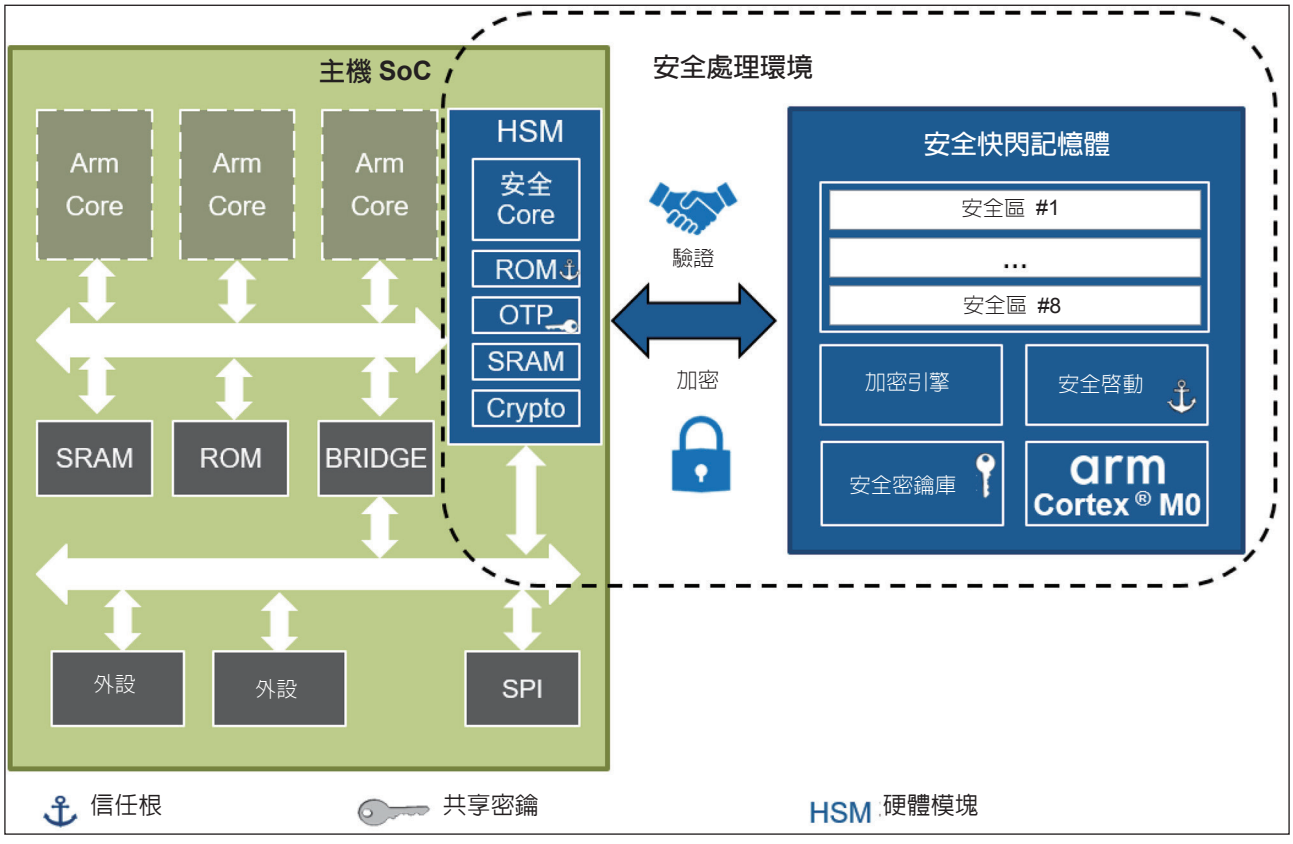
技術的進步不斷推動 IC 成本下降，集成新一代 IC 的系統成本也隨之降低。外置快閃記憶體也是這種情況，安全 “ 智慧快閃記憶體 ” 的出現，減少了在硬體中實施信任根並納入其他必要功能所需的工作。

安全快閃記憶體：新一代智慧儲存

半導體廠商想方設法尋求小尺寸的嵌入式快閃記憶體，但是還沒有可行的解決方案出現。小尺寸 RRAM 和 MRAM 技術已作為 eFlash 的替代品得到了廣泛研究，但由於資料完整性和成本方面的挑戰，它們目前都還不可行，尤其是不適合要求高溫高可靠性的關鍵任務應用。截至本文撰寫之時，尚不能確定這些技術或其他相關技術何時 (或是否) 能夠交付批量生產的嵌入式存儲。

尺寸縮小導致變化不可避免，因此產生了對新型安全通道的需求。在這種通道中，資訊交換發生在 MCU 內部的 HSM 和外置存放裝置的加密安全區之間。一種前景不錯的解決方案是捨棄目前的做法，不將各種類型的儲存整合於處理器，而將處理器整合於儲存 IC，是為智慧儲存。圖 3 顯示了安全快閃

圖 3：安全快閃記憶體可兼容產業標準介面，從而為現有與新型嵌入式系統提供更強的安全支持



記憶體如何與主機 MCU 建立經過驗證和加密的安全處理環境。

新一代智慧儲存的這種發展趨勢有可能為電子行業帶來革命性的變化。就嵌入式系統而言，技術發展將集中體現在 NOR 快閃記憶體上。NOR 快閃記憶體是一種理想的非易失性儲存，儲存代碼具有持久性，並具備快速隨機讀取性能。

安全 NOR 快閃記憶體，或更簡單的安全快閃記憶體，可為安全金鑰、證書、雜湊密碼、特定應用資料、配置資料、代碼版本資訊和生物識別感測器資料提供硬體保護的安全儲存，以便用於驗證。安全快閃記憶體還支援經過驗證和加密的交易，以防止未經授權的訪問和其他安全威脅。

相比之下，當前基於狀態機的儲存架構則無法提供與嵌入式處理器相同的多功能性和性能。例如，強大的安全需要強大的加密，進而需要強大的處理能力。嵌入式處理器還支持其他安全要求，包括 HMAC 金鑰生成和儲存以及防回滾計數器，並可保護固件、啓動鏡像和系統參數免受攻擊。

在儲存中嵌入處理能力有助於整合邏輯，以添加特定功能和 / 或減輕系統主 SOC/MCU 的工作量。例如，嵌入式處理可以實現硬體信任根的創建，從而防止對儲存的代碼和資料進行修改、操縱和其他安全攻擊。或者，處理器也可以對原始資料運行各種演算法，包括機器學習演算法，然後儲存系統其他功能所需的結果。

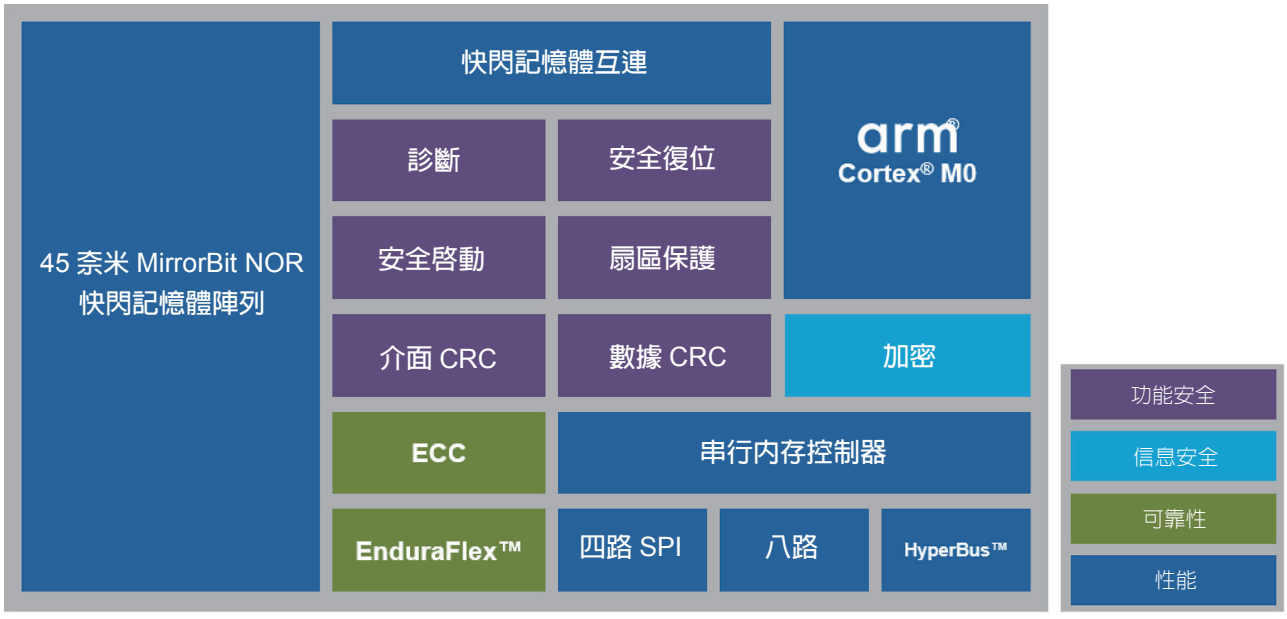
此外，針對可以通過智慧儲存的嵌入式處理器運行代碼而全部或部分認證的安全法規，新系統能夠更加輕鬆地獲得認證。這樣，通過簡化所需的設計和開發工作，我們可以極大地加快新產品的上市速度。

圖 4 顯示了內置了智慧化安全的快閃記憶體如何滿足嵌入式系統所需的性能、可靠性、安全性和功能安全。通過使用包括 x4 SPI (QSPI) 和 x8 HyperBus 在內的標準匯流排協定，智慧安全快閃記憶體可以與主控晶片配合，以達到要求嚴苛的互聯應用所需的安全級別，同時仍然完全相容現有的主控晶片儲存控制器。

對於不允許發生故障的關鍵任務應用，安全快閃記憶體可以確保系統的安全啓動，記錄關鍵的資訊，並擴展重要功能的工作儲存。此類“故障保護”應用的示例包括：高級駕駛輔助系統 (ADAS)，可攜式醫療設備，工廠自動化，國防級感測器，以及高級無線通訊系統。

無故障的一個重要方面，是對存儲的代碼和資料進行加密，以防遭到更改或破壞。通過集成加密

圖 4：將處理器嵌入 NOR 快閃記憶體，可使外置快閃記憶體更加智能，從而提供嵌入式系統所需的性能、可靠性、信息安全和功能安全



引擎和嵌入式處理器，資料能夠以安全的方式進行存儲。考慮到存儲所增加的邏輯門數遠小於 CPU 和專用計算引擎所需要增加的邏輯門數，因此在智慧安全快閃記憶體中以相對較低的增量成本實施加密和其他高級功能更為可行。

安全快閃記憶體創建的硬體信任根，可提供一個安全環境或與安全 MCU 提供的 TEE 整合。信任根有一個至關重要的作用，就是確保系統正常啓動，理想情況下應基於可信計算工作組的設備識別字組合引擎 (DICE) 標準。安全啓動流程對快閃記憶體和主 SOC/MCU 進行相互驗證，以確保穿越匯流排的所有交易的機密性，從而實現端到端的保護。而且因為快閃記憶體是智慧的，所以經過驗證的啓動過程可以在某些應用領域需求的不到 100 毫秒時間內實現。

能夠將代碼安全地更新至最新版本，是安全啓動流程的另一個重要方面。這就要求確保 FOTA 或其他形式的更新在沒有任何篡改或損壞的情況下完成，無論是有意還是意外的損壞。如果通過版本認證或其他方式檢測到任何篡改，那麼可以利用備份功能還原以前已知有效版本 (雖已降級) 的代碼。同樣的功能也可用于保護非安全生產設施或服務中心可能存在的任何設備配置。

嵌入式智慧使得安全快閃記憶體除了保護儲存的代碼和資料之外，還可以處理其他任務。例如，支援 XIP 功能使得作為可信環境的安全快閃記憶體可以直接執行代碼，從而減輕主機 MCU 的負載。這樣也可以減少 MCU 所需的片上 RAM 的數量，從而有助於降低成本和功耗。

在最嚴苛的安全性和功能安全需求推動下，汽車和工業自動化市場率先採用安全儲存。因為嵌入式系統的潛在漏洞可能導致遠端攻擊，並最終威脅到乘客或工作人員的安全，所以，如果不能確保強大的安全性，就無法實現系統的功能安全。因此，安全關鍵型應用的所有半導體元件 (包括外置快閃記憶體設備) 都必須符合 ISO26262 高級駕駛員輔助系統 (ADAS) 標準和 IEC 61508 工業系統標準。

持續監控現場設備狀況，執行遠端診斷和預防性維護，也都非常重要。快閃記憶體設備容易出現幾種故障模式，包括由於電荷損耗或宇宙輻射引起的快閃記憶體單元故障、時延、功率損耗故障等，這些故障都必須即時加以解決，以確保在 20 年以上的使用壽命中提供較高的可靠性。

結論

智慧安全快閃記憶體作為 eFlash 的替代產品已經逐步得到了人們的接受，隨著它的製程尺寸縮小到 28nm 以下，eFlash 的使用必將變得日漸稀少，直至完全消失。晶片可以集成 eFlash、但集成 HSM 功能的安全快閃記憶體方案更具有優勢。在這兩種設計中，安全快閃記憶體都可以通過行業標準匯流排，以加密安全的方式，在受保護區域和主機 MCU 的 HSM 之間傳輸代碼和資料。

可以預期，採用安全快閃記憶體的設計將變得越來越普遍，對於滿足不斷發展的安全需求來說甚至必不可少。如今，攻擊行為正在變得日漸廣泛和複雜，各項法規預計將會越來越嚴格，自動化程度的提高也將進一步提升安全性和功能安全的重要性。為了滿足這些不斷發展的需求，同時最大程度地加快新功能的上市速度，設計工程師將越來越依賴僅智慧安全快閃記憶體可以提供的便捷性。

關於作者

Sandeep Krishnegowda 是賽普拉斯半導體公司快閃記憶體業務部的產品總監。他在賽普拉斯的記憶體產品部門工作了十多年，擔任過各種工程、管理和行銷職務。他擁有倫斯勒理工學院的電子和通信碩士學位，以及韋斯科技大學的電子和通信學士學位。CTA