面對與日俱增的威脅需要動態信任機制來保障硬體安全

■作者：萊迪思半導體 供文

對動態信任機制的需求

電子產品如今已遍佈各個市場，對於設計這些設備的開發人員而言，保護產品設計免於韌體攻擊至關重要。國家資訊安全性漏洞資料庫報告指出，2016 年至 2019 年，韌體漏洞數量增長了 700%以上[1]。產業分析公司 Gartner 報告指出，截至 2022 年，將有 70%未執行韌體升級計畫的組織會由於韌體漏洞而遭到入侵[2]。

這些漏洞不僅會破壞部署在現場的最終產品。獨立元件在當今變化莫測的全球電子供應鏈中運輸時也可能會受到影響：從元件最初的生產、運輸到外包製造商，再到系統整合和元件的整個運行週期。不法分子可能會利用這些漏洞，並帶來一系列安全問題，如數據盜竊、資料損壞、木馬病毒或遭惡意軟體植入、設備劫持、複製和設計盜竊等。對平台韌體的成功入侵可能導致系統永遠無法運行，或者利用系統進行勒索、資料盜竊和劫持。由於這些操作在作業系統下層實施，所以在造成破壞前有可能不被偵測到。上述攻擊都有可能對公司的財產或聲譽造成嚴重影響。

保護電子系統硬體免於未經授權的存取並非新的問題。現有的解決方案只能防止未經授權的

圖 1：由於一系列的潛在威脅，確保元件在供應鏈運輸過程中的安全變得更有挑戰性。

使用者存取元件韌體。然而由於這些解決方案通常採用馮．諾依曼架構微處理器 (Von Neumann architecture microcontrollers)，在元件受到攻擊時，缺乏管理多個元件的即時處理能力。而 FPGA 本身的並行處理能力能夠同時監控、保護和恢復多個元件，反應時間可達奈秒級。

即便採用當今最好的 TPM 管理和作業系統安全解決方案，系統韌體仍然可能在系統製造之前、當下或之後受到攻擊。此外，由於系統元件通常會在作業系統以及任何軟體安全解決方案 (例如啓動後驗證檢查) 運行之前載入韌體，因此很難偵測到損壞的韌體。受損韌體接著會繞開靜態啓動後整合檢查，躲過安全和惡意軟體掃描。

電子系統需要持續優化，以適應不斷變化的新威脅，且能在偵測到韌體受損時自動採取適當行動。為了保護系統韌體，安全解決方案需要「動態信任 (Dynamic Trust)」機制：採用平行、即時、快速反應的解決方案抵禦韌體攻擊，在系統的整個生命週期中提供全面的韌體保護，從元件在整個供應鏈中的運輸、最初的產品組裝、最終產品運輸、整合到產品的整個運行週期。

全新 NIST 標準

OEM 廠商如何保護自己免受不斷變化的威脅入侵？幸而，美國國家標準暨技術研究院 (National Institute of Standards and Technology；NIST) 意識到韌體威脅的緊迫性，發佈了 NIST 平台韌體保護恢復 (PFR) 標準 (NIST SP-800-193)，強調正確實施 PFR 的重要性。該標準描述了一系列安全機制，保護平台免於未經授權的更改、偵測已發生的未經授權更改並快速安全地從攻擊中恢復，提高了平台的防禦力。

此標準通過下列三個原則保障平台安全：

■**保護**：NIST 的保護標準包括了多種機制確保平台韌體和關鍵資料的完整性，防止遭到損壞，其中包括了一項確保韌體更新可靠性和完整性的流程。此標準更要求在系統運行時同時監視所有受保護的外部記憶體及其介面匯流排 (反應時間為奈秒級)，並對所有韌體實施嚴格的存取控制。

■**偵測**：平台韌體程式碼和關鍵資料遭到入侵時的偵測機制。這需要受保護的 IC 在啓動之前自動對韌體進行驗證。

■**恢復**：在偵測到入侵發生時，即便是服務阻斷攻擊 (Denial of Service) 和重送攻擊 (Replay Attack)，也將平台韌體程式碼和關鍵資料恢復到已知完好、經過認證的正常狀態。這種恢復機制需要自動、即時進行以保持系統線上，同時最小化支援資源的使用。

為了應對快速發展的市場和標準，萊迪思半導體推出了全新的高附加價值安全解決方案集合和供應鏈防護服務，極大擴展了其硬體安全產品的功能。Lattice Sentry 解決方案集合透過為系統中的所有可程式化設計元件提供即時、動態保護、偵測和恢復功能，最大程度地減少了系統內韌體攻擊漏洞。Sentry 採用萊迪思 MachXO3D FPGA 提供完整、經過充分驗證、易於客製化、符合 NIST 800-193 的 PFR 解決方案。該解決方案集合包括一套即時可用、經過量產驗證的可靠 IP 核心，可用於保護和監視系統中的 SPI 和 I^2C 元件及其匯流排。Sentry 還包涵展示板和參考設計，用於測試和展示 PFR 功能。可用的軟體工具包括萊迪思最新的 IP 生態系統和開發環境——Lattice Propel。Propel 可以讓非 FPGA 用戶修改 RISC-V 處理器 IP 的 C 程式碼，幫助他們客製化 PFR 實現方案，同時還能視覺直觀地佈局所使用的 IP，創建完整系統。該系統可以導入 Lattice Diamond Tool 中生成配置位元流。Sentry 擁有完整的 PFR 參考設計，具有易於修改的 PFR 管理程式碼，用於 SPI/QSPi 的快速切換原理圖、清單生成器和處理器指令模擬器。

Lattice Sentry 解決方案集合可以大大縮短產品上市週期 (Time-to-Market)。如果沒有預驗證的 IP 核心和參考設計，開發此類解決方案可能需要耗費幾個月。有了 Sentry，開發人員可以修改管理 FPGA 即時操作的範例 C 程式碼，開發出符合 NIST

圖 2：萊迪思 Sentry 解決方案集合

800-193 標準的完整解決方案。還可以使用 Lattice Propel 軟體將預驗證的 IP 與運行 C 程式碼的 RISC-V CPU 整合到 FPGA 的配置位元流中。這些都無需 FPGA 設計經驗。此外，有興趣開發 FPGA IP 的客戶還可以將其 IP 整合到 Sentry 解決方案中使用。

除了 Sentry，萊迪思還提供 SupplyGuard 端對端供應鏈防護服務。SupplyGuard 是一個具有開拓性的訂購服務，該服務通過提供出廠鎖定的萊迪思 FPGA 來防止篡改、木馬植入、過度生產、偽造和 IP 盜竊，從而在供應鏈各個環節保障客戶的 IP 安全。該服務幫助客戶確保儲存在 FPGA 上的配置位元流和外部韌體認證金鑰不被篡改。透過 SupplyGuard，開發人員可以在整個供應鏈中保護產品。SupplyGuard 以安全、客戶專有的方式實現安全金鑰提供和設備所有權轉移，從而提供保護，有別於當前市場上其他的供應鏈解決方案。

SupplyGuard 服務開啓後，萊迪思將特定客戶的產品編號對應到客戶的 FPGA。每個客戶的對應 FPGA 都在萊迪思工廠使用客製化的加密憑證進行程式設計，僅允許客戶使用配置位元流和身份驗證金鑰對該 FPGA 進行程式設計。當 FPGA 在供應鏈中透過一般運輸公司運輸以及在第三方廠商工廠中進行系統組裝時，該服務將持續維持信任和發揮保護作用。由於晶片從萊迪思工廠出廠時就完全鎖定，因此只有客戶才擁有解鎖 FPGA 所需的憑證。萊迪思使用 FIPS 140-2 認證的硬體安全模組 (High Security Modules, HSM) 生成解鎖憑證並提供給客戶，然後客戶使用自己的 HSM 來解密憑證。在整個供應鏈中其他人均無法存取這些憑證。客戶的 HSM 擁有加密和簽名客戶自訂配置位元流和身份驗證金鑰所需的憑證。此外，客戶的 IP 和加密金鑰絕不會以任何形式洩露給萊迪思或供應鏈。

一旦使用 SupplyGuard 服務鎖定，客戶的 FPGA 在供應鏈中將成為在供應鏈中移動的「迷你堡壘」：被鎖定且無法存取，直到使用客戶的配置位元流進行程式設計為止。客戶經加密和簽名的位流是唯一可以載入到這些自訂鎖定 FPGA 上的位元流。同時，客戶的位元流也無法載入到另一片 FPGA 上，進而保護客戶的 IP 及其身份驗證金鑰，

圖 3：萊迪思 SupplyGuard 服務在全球供應鏈運輸中保護萊迪思 FPGA 免於未經授權的存取。

免於遭到複製和過度生產。對客戶的位元流進行程式設計的過程則將晶片的加密控制從萊迪思的出廠鎖定狀態轉變為客戶鎖定狀態。該所有權的轉移在萊迪思 FPGA 中以受保護的加密狀態進行，並使用標準的批量工廠程式設計設備在標準的生產線上進行。配置位元流始終保持安全和加密，且受到保護的所有權轉移在生產環境中無需任何特殊的安全程序、人員或設備 (例如 HSM)，避免了其他工廠金鑰提供解決方案中所需的額外時間和成本。

FPGA 實現安全系統控制

Sentry 和 SupplyGuard 的全新安全功能基於萊迪思革命性的 MachXO3D FPGA 產品陣容，實現安全系統控制。MachXO3D 是業界首款用於系統控制應用的小尺寸、低功耗 FPGA，旨在保護各類運算、通訊、工業和汽車應用中的韌體。MachXO3D 與萊迪思廣受歡迎的 MachXO 系列腳位相容，並讓設計人員得益於一半以上通訊系統和伺服器中已採用的可靠架構。MachXO3D 使用 NIST 獨立認證的加密功能，包括 ECDSA、ECIES、AES、SHA、HMAC、TRNG 和公 / 私金鑰生成，來保護其自有的配置位元流並實現系統安全。MachXO3D 元件均有單晶片快閃記憶體 (支援安全、經身份驗證的雙重開機配置)、用於外部韌體身份驗證的公開金鑰記憶體以及唯一的 ID。如果原始韌體由於任何原因遭到破壞，MachXO3D 將自動回滾到經過身份驗證的版本並保持系統繼續運行而不中斷。透過使用 Sentry 解決方案集合，MachXO3D 可以對其保護的外部韌體持續進行身份驗證檢查和韌體恢復。

MachXO3D FPGA 的加密功能符合 NIST SP 800-90B 規範的真亂數產生 (True Random Number Generation, TRNG) 和加密演算法驗證程式 (Cryptographic Algorithm Validation Program, CAVP)。MachXO3D 的 CAVP 功能經過獨立認證，符合聯邦資訊處理標準 (FIPS)，亦即美國聯邦政府所制定的加密軟體標準。

Sentry 和 SupplyGuard 讓動態信任成爲可能

萊迪思 Sentry 解決方案集合配合

圖 4：此圖展示了基於萊迪思 Sentry 的 PFR 應用如何即時保護系統中的所有韌體實例。

SupplyGuard，可為設計人員提供構建高防禦力、端對端的動態信任解決方案所需的一切資源。SupplyGuard 透過保護 MachXO3D FPGA 和開發人員的位元流以及開發人員的安全憑證，建立了供應鏈中的初始鎖定關係，進而保護平台韌體。此 FPGA 能夠在工廠程式設計期間轉移安全所有權，將保護許可權無縫轉移到開發人員經過簽名、加密的配置位元流，從而實現 Sentry PFR 功能，在系統啓動之前、操作期間以及之後的每次啓動和操作期間都能保護平台的韌體安全。系統可以在幾奈秒內對任何惡意行動作出反應，同時仍保持正常運作。利用 Sentry 和 SupplyGuard 構建的系統可以補足現有基於 BMC/MCU/TPM 的任何架構，因此開發人員可以繼續使用現有的硬體安全解決方案，滿足客戶在安全和供應鏈方面的特定需求。

結論

當今的硬體安全局勢正迅速發生變化。駭客能夠在當今的供應鏈中輕易地利用系統韌體漏洞來竊取資料和設計、劫持產品並創建複製品以在灰色市場上出售。開發人員該如何應對？答案就是實施符合 NIST 800-193 標準的全新高附加價值硬體安全產品和服務，並採用端對端動態信任措施保障硬體安全。全新萊迪思 Sentry 解決方案集合和 SupplyGuard 供應鏈防護服務可幫助他們快速輕鬆地實現上述目標。

參考文獻

[1] 資料來源：國家資訊安全性漏洞資料庫 (2016 年 https://nvd.nist.gov/vuln/search/statistics?form_type=Advanced&results_type=statistics&query=firmware&search_type=all&pub_start_date=01%2F01%2F2016&pub_end_date=12%2F31%2F2016)；和 (2019 年 https://nvd.nist.gov/vuln/search/statistics?form_type=Advanced&results_type=statistics&query=firmware&search_type=all&pub_start_date=01%2F01%2F2019&pub_end_date=12%2F31%2F2019)

[2] 資料來源：Gartner，2019 年 7 月 CTA