新聞稿

意法半導體STM32U5通用微控制器獲得PSA 3級和SESIP3安全認證

【台北訊，2021年8月13日】— 服務橫跨多重電子應用領域的全球半導體領導商意法半導體（STMicroelectronics，簡稱ST；紐約證券交易所代碼：STM）宣布STM32U585*通用安全微控制器通過PSA 3級和SESIP[1] 3安全認證，透過了邏輯、電路板和基礎實體抵抗等三項防禦測試，證明該微控制器的網路保護達到十分高的層級。

由於加強防篡改和軟體保護功能，STM32U585適用於控制PIN交易安全（PIN Transaction Security，PTS）設備，這種設備必須滿足支付卡產業安全標準委員會（Payment Card Industry Security Standards Council，PCI SSC）的技術要求。作為一種安全通用微控制器，STM32U585為開發者提供了一個簡化銷售和自助支付終端之設計生產的整體解決方案。

獲得「PTS官方核准裝置」標章的產品通常需要帶有防禦線上攻擊和旁通道攻擊的安全晶片，還要單獨使用一個微控制器（MCU）管理鍵盤、顯示器和USB連線等功能。現在，STM32U585單晶片整合了所有上述功能，並簡化了產品設計，同時還優化從採購和庫存管理到最終組裝的生產物流。終端製造商還可以根據PCI PTS v6之標準，更快速、更輕鬆地測試認證產品。

STM32U585符合Arm® Trusted Base System Architecture（TBSA）可信賴基礎系統架構之要求，採用

[1] Security Evaluation Standard for IoT Platforms 物聯網平台安全評估標準

Arm TrustZone®體系架構，具有保護連線裝置所需之各種典型安全功能，其中包括加密演算法加速器、安全資料存儲、安全韌體安裝、安全開機和安全韌體更新。

附加的安全功能使新產品的網路保護功能超越了典型的通用微控制器，其中包括在發生干擾攻擊時清除機密資料的內部監控，這有助於滿足PCI SSC的POS應用要求。其他的保護功能包括：增加旁通道攻擊（Side-Channel Analysis，SCA）分析，強化對稱和非對稱公開金鑰加速器（AES、PKA）的加密功能；保護資料存儲安全的唯一硬體金鑰；以及內建主動篡改偵測。

在確保注重成本和功耗之連網裝置能具備卓越的網路保護功能，同時，STM32U585還提供出色的內核性能和外部周邊整合度。先進的Arm Cortex®-M33嵌入式內核配合豐富的外部周邊，包括兩個類比數位轉換器（ADC）、兩個數位類比轉換器（DAC）通道、兩個運算放大器、兩個比較器和多個計時器，包括通用低功耗計時器和PWM馬達控制計時器。意法半導體自主開發之先進40nm製程和專有功能可節省電能，可以提升處理性能。這些功能包括在主電路休眠時維持運作的節能智慧外部周邊，以及可動態降低功耗到19µA / MHz以下的穩壓器。

作為STM32產品組合中的通用安全微控制器，STM32U585是意法半導體STM32Trust布局中的重要一環。STM32Trust是意法半導體的安全框架，其整合了知識、STM32MCU和MPU、通用標準認證的STSAFE安全模組、開發工具、硬體和軟體以及設計服務，協助開發人員保護產品設計，確保連線安全和系統的完整性。

STM32U585現已量產，其採用7mm x 7mm UFBGA169封裝。

更多關於STM32U5 MCU相關資訊，請造訪：https://www.st.com/en/microcontrollers-microprocessors/stm32u5-series.html。

關於意法半導體

意法半導體（STMicroelectronics; ST）擁有46,000名半導體技術、產品和方案的創新和創造者，掌握半導體供應鏈和最先進的製造設備。作為一家獨立的半導體設備製造商，意法半導體與逾十萬客戶、上千合作夥伴一起研發產品和解決方案，共同打造生態系統，一同攜手應對各種挑戰和機會，滿足世界對於永續發展之更高的需求。意法半導體的技術讓人們出行更智慧、電力和能源管理更高效、物聯網和5G技術應用更廣泛。詳情請瀏覽意法半導體公司網站： www.st.com。