

指定支援 Wi-Fi MCU 時的注意事項

■作者：Alex Li

Microchip Technology 無線解決方案產品部資深市場行銷工程師

工業物聯網的發展趨勢是縮減在一個 SoC 方案而非靠使用多個離散式元件的組合，以精簡物料清單、降低設計風險、減少佔用空間。Wi-Fi MCU 即是一個典型案例，它將 Wi-Fi 連接與處理器及所需 GPIO 整合在一起，以滿足多種應用的需求。在指定其中一個元件時，需要考慮多個因素，並需審慎進行選擇，因此務必對這些元件有所瞭解。

當今市場上存在低成本的 Wi-Fi 連接方案，但通常會以周邊數量和整體效能為代價。這意味著選擇最佳 Wi-Fi MCU 充滿挑戰和風險，因為 Wi-Fi MCU 必須兼具穩健的 Wi-Fi 連接和高效能 MCU 功能，二者缺一不可，否則會導致整個設計項目延遲甚至失敗。MCU 是系統的核心，是 Wi-Fi MCU 中最關鍵的部分，因此需要在專案伊始對其效能進行檢查，否則可能在後期發生需要更換元件的情況，通常需要重新設計所有軟體及配置並修改電路。

ADC 不容忽視

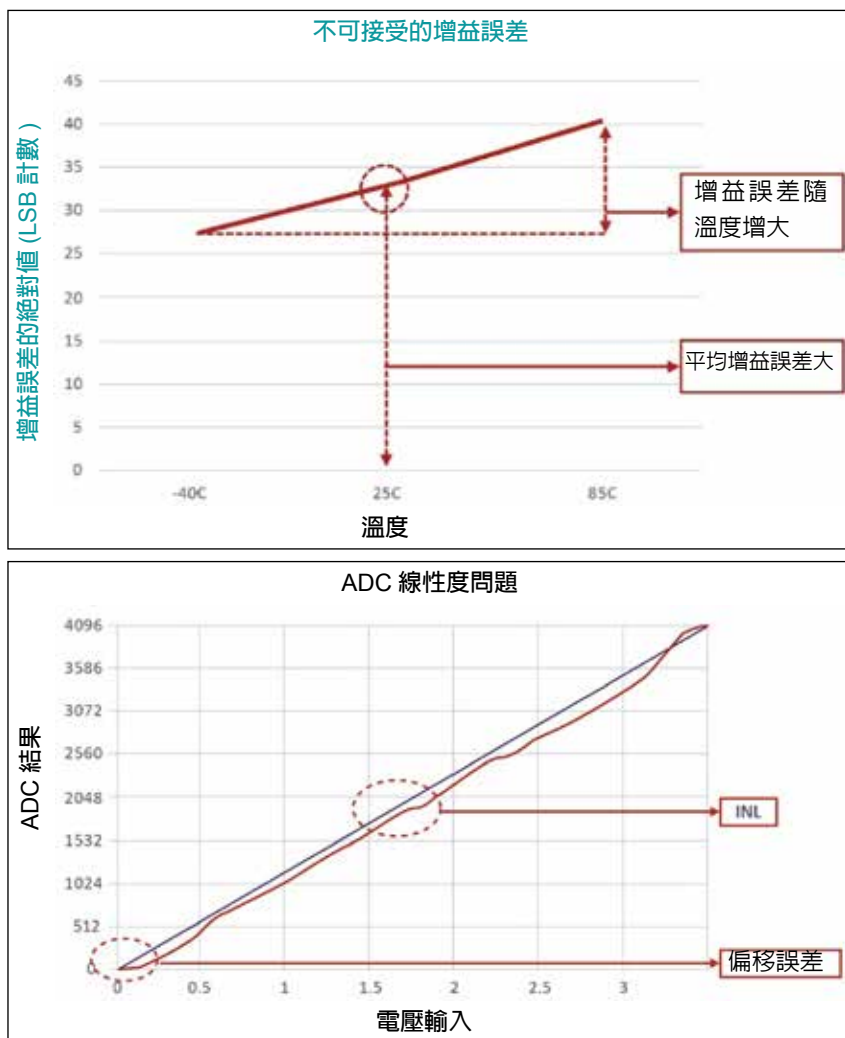
指定 Wi-Fi MCU 時，類比至

數位轉換 (ADC) 是最易忽視的功能之一，儘管它是訊號鏈中類比輸入之後的第一個處理元件。這意味著它的效能將影響整個系統，因此

務必掌握有關類比至數位轉換器的關鍵指標以及 Wi-Fi MCU 製造商為達成指標所應採用的方式。

設計人員關注的首要規範之

圖 1: 低階 ADC 的精確度和線性度差，易受環境和溫度影響



一是 ADC 的位元數。這會讓人感到困惑，因為，事實上，實際位元數將低於（甚至遠低於）資料手冊裡的規範。ADC 可用於執行轉換的有效位元數 (ENOB) 更為重要，ENOB 始終小於資料手冊規範，但與資料手冊規範越接近越好，因為在不同 ADC 之間這一位元數有著很大的差異。可用於執行轉換的位元數越少，SoC 的輸入訊號的精確度就越低。

此外，與所有電子元件一樣，ADC 會為訊號“貢獻”一些對其功能產生負面影響的因素，包括量化和時序誤差以及偏移、增益和線性度的變化。ADC 還有一個眾所周知的缺點：易受諸多工業物聯網運行環境中常見的大溫度波動影響（見圖 1）。Wi-Fi MCU 製造商可以規避這種情況，因此務必聯繫每個候選 Wi-Fi MCU 的製造商以確定其 ENOB、效能隨溫度變化情況、線性度和精確度。如果無法提供這些資訊，則應拋棄不用。

周邊支援

所有 Wi-Fi MCU 至少都支援少量介面標準，因此很容易認為它們能達到要求。而當工程師試圖在其他設計中使用相同的 Wi-Fi MCU 時，他們常常會為自己的草率後悔不已。這種情況在建立或修改工業物聯網系統時越來越常見，因為大多數生產設施均採用由不同製造商在不同時間製造的各種機器和控制器。

隨著系統完善的完善，可能會增加更多的介面，有時可能需要支

援觸控偵測和 LCD 等功能。如果 SoC 有備用 GPIO，則可以在幾乎不共用接腳的情況下控制更多繼電器、開關和其他元件。為此，元件支援的介面應包括乙太網 MAC、USB、CAN、CAN-FD、SPI、I²C、SQI、UART 和 JTAG（可能還包括觸控發送和顯示支援），以確保能夠在現在和可預見未來功能的擴充需求以適應所有情況。

安全始於內部

安全性對於每個物聯網應用都至關重要，但工業環境具有任務關鍵性特徵，一旦有威脅進入工業物聯網的網路，就會在整個設施乃至整個公司擴散。第一級所需安全性位於 MCU 的整合加密引擎中，在這裡，將循序執行或並存執行加密和身份驗證。密碼應包括 AES 加密（金鑰大小最高 256 位元）、DES 和 TDES，身份驗證應包括 SHA-1 和 SHA-256 以及 MD-5。

由於每個雲端服務提供者都有自己的認證和金鑰，為其開通元件是一個複雜的過程，需掌握大量與加密相關的知識，是設計人員針對雲端服務開通產品時最具挑戰性的任務之一。幸運的是，包括 Microchip Technology 在內的一些製造商簡化了這一過程，節省了大量的時間和金錢。這種方法能夠大幅縮短時間，減少混亂；可以將設計過程縮短數周或更長時間，同時憑藉行之有效的可驗證方法確保滿足所有安全和開通要求。

務必注意，大多數 Wi-Fi

MCU 將憑證儲存在快閃記憶體中，其中的資料可存取且容易受到軟體和物理攻擊。如果將此類資訊儲存在硬體設計的安全元件中，則無法透過任何外部軟體讀取其中的資料，因而可以達到最高的安全性。例如，WIFI32 等 Microchip Wi-Fi MCU（圖 2）在公司的 Trust&GO 平臺中採用這種方法安全地開通其 MCU，以連接到 AWS IoT、Google Cloud、Microsoft Azure 和協力廠商 TLS 網路。

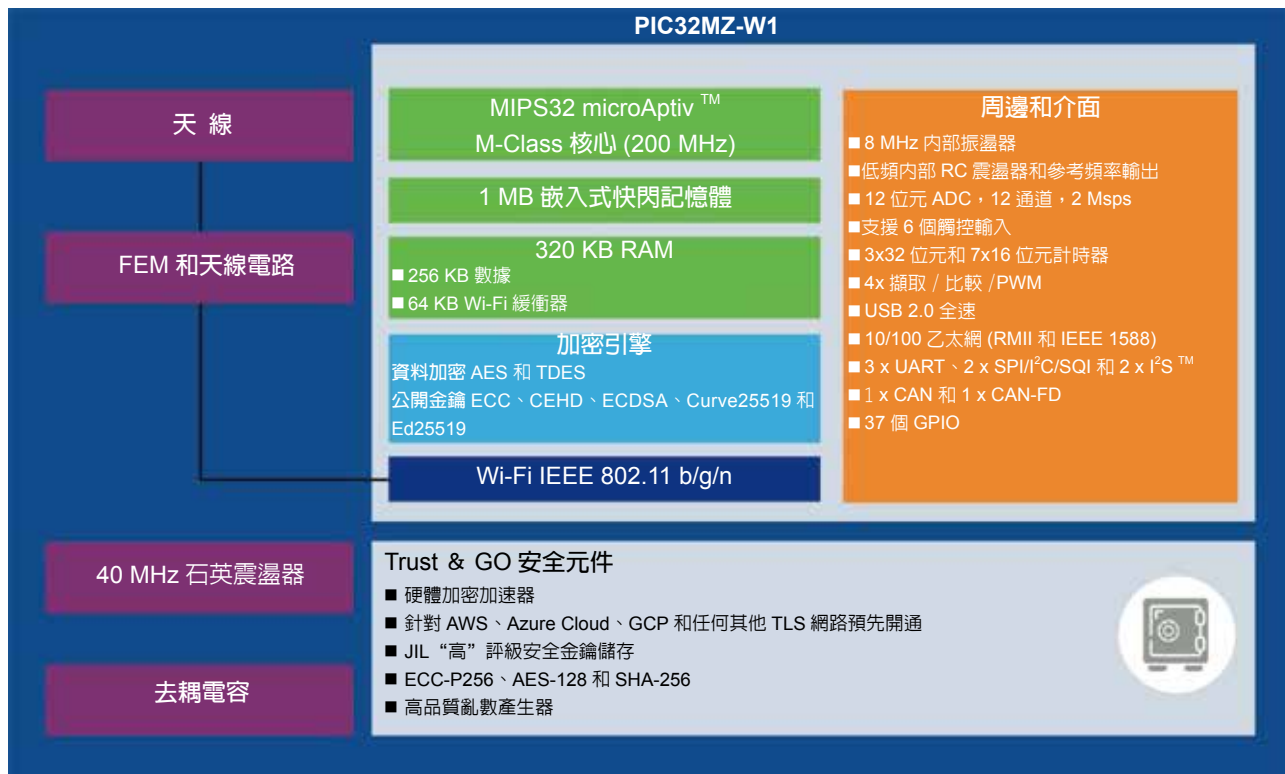
預開通、預配置或自訂的安全元件在製造時即會儲存於元件的硬體安全模組 (HSM) 內生成的憑證，防止憑證在生產期間和之後公開。Trust&Go 平臺只需一款成本低廉的 Microchip 開發套件，設計人員可使用隨附設計套件中的教程和範例程式創建所需的清單檔。一旦安全元件的 C 程式碼在應用程式中運行，就可以從設計轉入生產。

所需安全性的另一種形式是 Wi-Fi 聯盟認證的最新 Wi-Fi 安全。最新版本 WPA3 基於上一代 WPA2 構建，但增加了一些功能，可簡化 Wi-Fi 安全、實現更穩健的身份驗證、提供更高的加密強度並保持網路彈性。所有新元件均須通過 WPA3 認證才能使用 Wi-Fi 聯盟標誌，因此應對每個 Wi-Fi 晶片和 Wi-Fi MCU 進行認證，以實現最高安全性。不過，仍需進行核實以確保候選 Wi-Fi MCU 已通過 WPA3 認證。

確保互通性

如果射頻不匹配、軟體和其

圖 2: WFI32 Wi-Fi 模組將憑證儲存在硬體中加以隔離，使其幾乎不會遭受駭客攻擊



他一些因素，Wi-Fi MCU 始終有可能無法與市場上的部分基地台通信。無法連接到常用的基地台將損及公司聲譽。儘管我們無法保證 Wi-Fi MCU 能與全球每個基地台 (AP) 搭配使用，但可確保 Wi-Fi MCU 通過了與市場上最常用 AP 的互通性測試，盡可能減少問題。

此資訊通常可從製造商網站獲取，但若網站未提供相關資訊，可致電製造商獲取資訊，如果仍未能獲取資訊，請選擇其他供應商。

必須要有協助

最後但同樣重要的是需要設計支援。如果沒有一個全面的整合

式開發環境 (IDE) 平臺，設計人員只能將一些不確定是否有用、簡單或可靠的 Web 資源拼湊在一起。例如，少數 Wi-Fi MCU 製造商只提供了有關產品的基本詳情和原型設計說明後就此止步且不再提供將其從當前階段轉入生產階段所需的資訊，如此將造成設計人員無法完

圖 3: 從原型設計階段到成品，此類整合式開發環境均能為設計人員提供除錯工具和其他工具來降低風險



成最後階段所需的認證並使其無法量產。

真正有用的是，製造商應提供一個全面的 IDE(圖 3)，其中包括 Wi-Fi MCU 執行的每一個類比和數位功能以及要在特定應用中實現所需要的外部元件。應提供一種方法將設計變更對整體效能的影響視覺化，還應具備評估設計的影響視圖，還應具備評估設計的影響視圖。一些基本工具可免費使用，另一些工具則

以適中的成本提供，包括設計用於製造商的 Wi-Fi MCU 系列的評估板。

總結

物聯網的發展趨勢是將更多的處理能力轉向網路邊緣，而不是只集中於基於雲端的資料中心。為此，需要在最少的空間和元件中整合盡可能多的功能。Wi-Fi MCU 是眾多 SoC 中的一種，它將多個功

能整合在一個元件中，而不是分佈於功能特定的離散元件，從而實現上述目標。

如果 Wi-Fi MCU 製造商可提供足夠的資源，則將這些元件整合到嵌入式 IoT 子系統中可能相對簡單。這些資源包括高度安全性(通過一種簡單的開通方法來滿足雲端服務提供者的需求)和全面的 IDE(引導設計人員從原型設計階段轉向生產階段)。CTA

Microchip 推出業界首款 NVMe 和 24G SAS 三模 RAID 和 HBA 儲存介面卡

設計儲存平臺的雲端服務提供者和伺服器 OEM 廠商必須為下一代資料中心提供卓越的效能、靈活性和安全性。Microchip 宣佈推出 Adaptec 智慧儲存 PCIe 第四代 NVMe 三模 SmartRAID 3200 RAID 介面卡，以及 Adaptec SmartHBA 2200 和 Adaptec HBA 1200 主機匯流排介面卡。這些介面卡實現了下一代 NVMe 和 24G SAS 連接和可管理性，具有市場領先的效能，同時提供了下一代資料中心基礎設施所需新等級的安全要求。

Microchip 智慧儲存介面卡提供 8 至 32 個埠的 NVMe 4.0 和 / 或 24G SAS 硬碟支援，並提供 x8 和 x16 PCIe Gen 4 CPU 介面選項，與前幾代產品相比，效能提升達 4 倍。先進的功能，如動態通道複用 (DCM) SAS 鏈路聚合技術，提供大於 99% 的擴展器連接鏈路效率，大幅提升了高密度儲存解決方案的效能。

Microchip 智慧儲存介面卡採用了市場領先的智慧儲存協定堆疊和綜合管理工具。這款最新一代介面卡增加了對通用背板管理 (UBM) 的 SFF-TA-1005 業界標準和用於智慧背板管理的 Intel 虛擬接腳埠 (VPP) 的支援，以及基於分散式管理任務 (Distributed Management Task Force) 標準的平臺級資料模型 (PLDM)/Redfish 設備啟用 (RDE)，簡化透過 MCTP/BMC 實施的頻外 (out-of-band) 管理工作。

儲存基礎設施需要介面卡級別和供應鏈的安全能力。Microchip 新一代介面卡包括業界最廣泛的安全儲存選項，支援自加密驅動器 (SED) 和基於 maxCrypto 控制器的加密 (CBE)。這些新功能擴展了加密邊界，不僅僅是 SED 設備，現在還可以保護儲存在快取記憶體中的資料。Microchip 的可信平臺技術提供了所需的供應鏈安全，並符合開放計算安全專案計畫。

Microchip 的 Adaptec SmartRAID 3200 RAID 介面卡、Adaptec SmartHBA 2200 和 Adaptec HBA 1200 主機匯流排介面卡共用通用的智慧儲存部署工具，例如用於本地管理的 Adaptec maxView 儲存管理器和 ARCCONF 管理工具，用於透過 BMC 和 Chiplink 診斷工具進行遠端系統管理的 MCTP 和基於 DMTF 標準的平臺級資料模型 (PLDM)/RDE(Redfish Device Enablement)。

Adaptec SmartRAID 3200、SmartHBA 2200 和 HBA 1200 板級介面卡，提供多達 32 個 SAS/SATA/NVMe 內部連接埠和 x8 或 x16 PCIe 第 4 代主機介面，現已量產發佈。

