指定支持 Wi-Fi®的 MCU 时的注意事项

Microchip Technology
无线解决方案产品部
资深市场营销工程师
Alex Li

工业物联网的发展趋势是在一个 SoC 而非多个离散器件中执行更多功能，以精简物料清单、降低设计风险、减少占用空间。Wi-Fi® MCU 即是一个典型，它将 Wi-Fi 连接与处理器及所需 GPIO 集成在一起，以满足多种应用的需求。在指定其中一个器件时，需要考虑多个因素，并需审慎进行选择，因此务必对这些器件有所了解。

当今市场上存在低成本的 Wi-Fi 连接方案，但通常会以外设数量和整体性能为代价。这意味着选择最佳 Wi-Fi MCU 充满挑战和风险，因为 Wi-Fi MCU 必须兼具稳健的 Wi-Fi 连接和高性能 MCU 功能，二者缺一不可，否则会导致整个设计项目延迟甚至失败。MCU 是系统的核心，是 Wi-Fi MCU 中最关键的部分，因此需要在项目伊始对其性能进行检查，否则可能在后期发生需要更换器件的情况，通常需要重新设计所有软件及配置配套电路。

ADC 不容忽视

指定 Wi-Fi MCU 时，模数转换是最易忽视的功能之一，尽管它是信号链中模拟输入之后的第一个处理元件。这意味着它的性能将影响整个系统，因此务必掌握有关模数转换器（ADC）的关键指标以及 Wi-Fi MCU 制造商为达成指标所应采用的方式。

设计人员关注的首要规范之一是 ADC 的位数。这会让人感到困惑，因为，事实上，实际位数将少于（甚至远低于）数据手册规范。ADC 可用于执行转换的*有效*位数（ENOB）更为重要，ENOB 始终小于数据手册规范，但与数据手册规范越接近越好，因为在不同 ADC 之间这一位数有着很大的差异。可用于执行转换的位数越少，SoC 的输入信号的精度就越低。

此外，与所有电子器件一样，ADC 会为信号“贡献”一些对其功能产生负面影响的因素，包括量化和时序误差以及失调、增益和线性度的变化。ADC 还有一个众所周知的缺点：易受诸多工业物联网运行环境中常见的大温度波动影响（见图 1）。Wi-Fi MCU 制造商可以规避这种情况，因此务必联系每个候选 Wi-Fi MCU 的制造商以确定其 ENOB、性能随温度变化情况、线性度和精度。如果无法提供这些信息，则弃用。

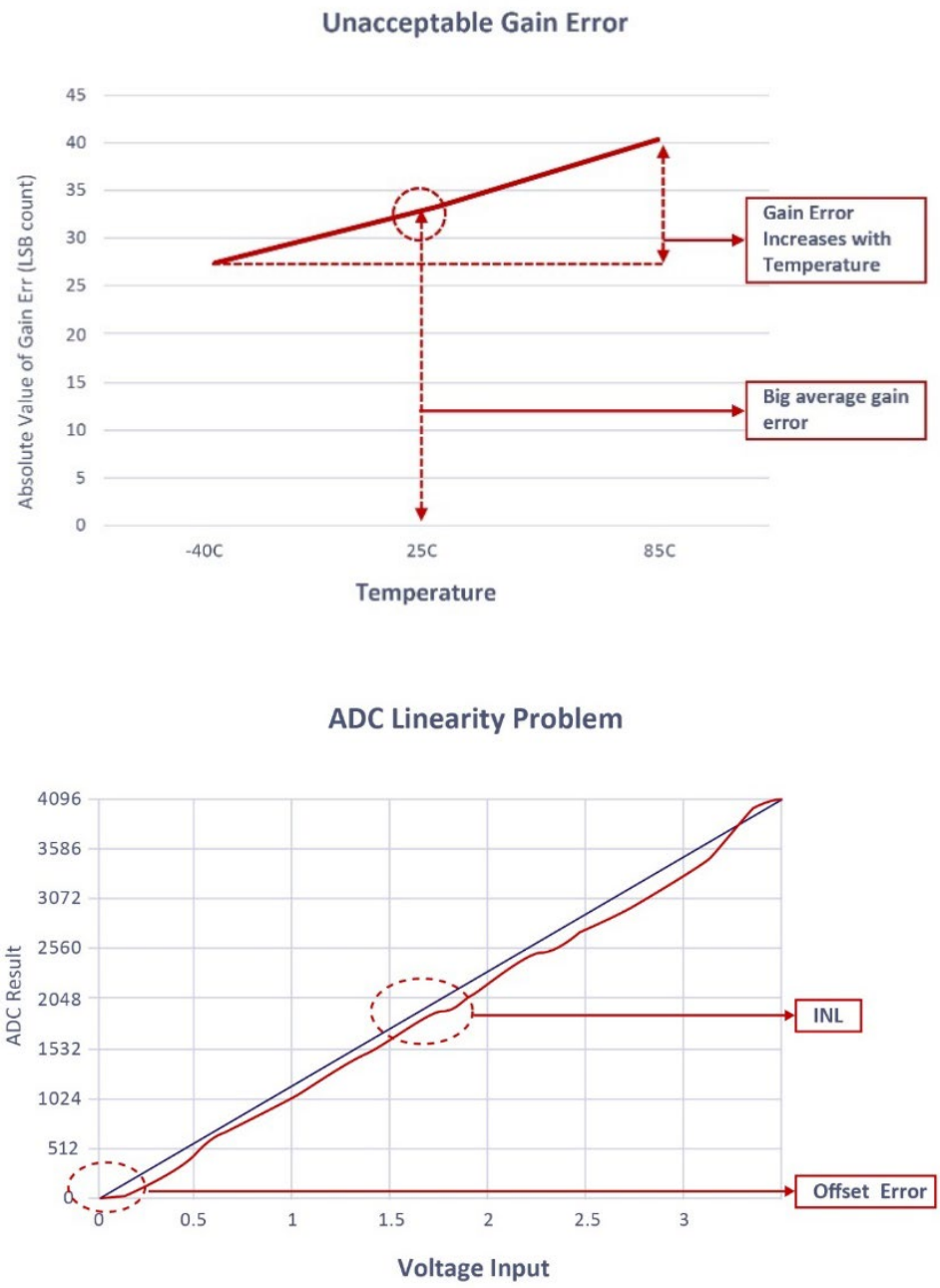

图 1.低档 ADC 的精度和线性度差，易受环境和温度影响

外设支持

所有 Wi-Fi MCU 至少都支持少量接口标准，因此很容易认为它们能达到要求。而当工程师试图在其他设计中使用相同的 Wi-Fi MCU 时，他们常常会为自己的草率后悔不

已。这种情况在建立或修改工业物联网系统时越来越常见，因为大多数生产设施均采用由不同制造商在不同时间制造的各种机器和控制器。

随着系统的完善，可能会增加更多的接口，有时可能需要支持触摸检测和 LCD 等功能。如果 SoC 有备用 GPIO，则可以在几乎不共用引脚的情况下控制更多继电器、开关和其他元件。为此，器件支持的接口应包括以太网 MAC、USB、CAN、CAN-FD、SPI、I^2C、SQI、UART 和 JTAG（可能还包括触摸发送和显示支持），以确保能够在现在和可预见的未来适应几乎所有情况。

安全始于内部

安全性对于每个物联网应用都至关重要，但工业环境具有任务关键性特征，一旦有威胁进入工业物联网的网络，就会在整个设施乃至整个公司扩散。第一级所需安全性位于 MCU 的集成加密引擎中，在这里，将顺序执行或并行执行加密和身份验证。密码应包括 AES 加密（密钥大小最高 256 位）、DES 和 TDES，身份验证应包括 SHA-1 和 SHA-256 以及 MD-5。

由于每个云服务提供商都有自己的认证和密钥，为其置备器件是一个复杂的过程，需掌握大量与加密相关的知识，是设计人员针对云服务置备产品时最具挑战性的任务之一。幸运的是，包括 Microchip Technology 在内的一些制造商简化了这一过程，从而节省了大量的时间和金钱。这种方法能够极大地缩短时间，减少混乱；可以将设计过程缩短数周或更长时间，同时凭借行之有效的可验证方法确保满足所有安全和置备要求。

务必注意，大多数 Wi-Fi MCU 将凭证存储在闪存中，其中的数据可访问且容易受到软件和物理攻击。如果将此类信息存储在硬编码的安全元件中，则无法通过任何外部软件读取其中的数据，因而可以达到最高的安全性。例如，WFI32 等 Microchip Wi-Fi MCU（**图 2**）在公司的 Trust&GO 平台中采用这种方法安全地置备其 MCU，以连接到 AWS IoT、Google Cloud、Microsoft® Azure 和第三方 TLS 网络。

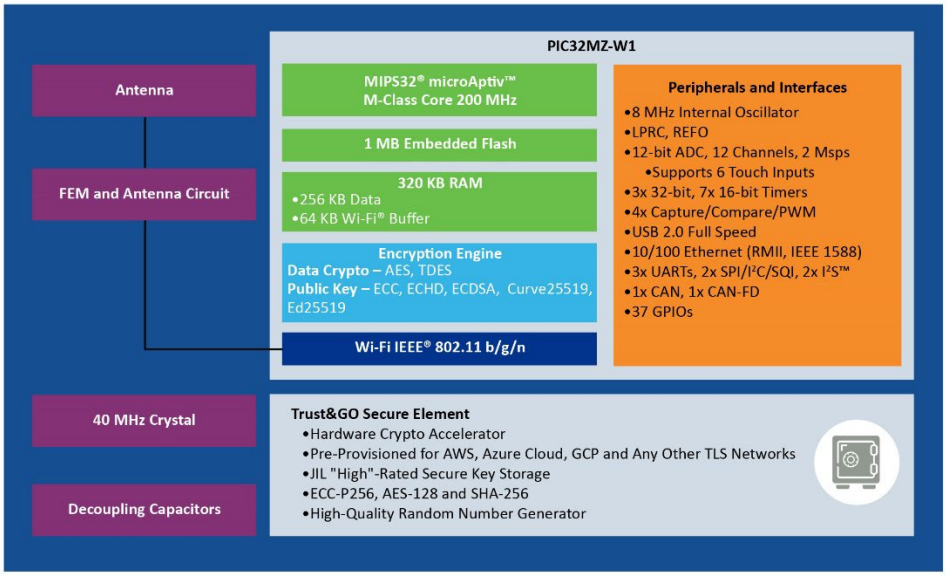

图 2.WFI32 Wi-Fi®模块将凭证存储在硬件中加以隔离，使其几乎不会遭受黑客攻击

预置备、预配置或自定义的安全元件在制造时即会存储于器件的硬件安全模块（HSM）内生成的凭证，防止凭证在生产期间和之后公开。Trust&Go 平台只需一款成本低廉的 Microchip 开发工具包，设计人员可使用随附设计套件中的教程和代码示例创建所需的清单文件。一旦安全元件的 C 代码在应用程序中运行，就可以从设计转入生产。

所需安全性的另一种形式是 Wi-Fi 联盟认证的最新 Wi-Fi 安全。最新版本的 WPA3 基于上一代 WPA2 构建，但增加了一些功能，可简化 Wi-Fi 安全、实现更稳健的身份验证、提供更高的加密强度并保持网络弹性。所有新器件均须通过 WPA3 认证才能使用 Wi-Fi 联盟标志，因此应对每个 Wi-Fi 芯片和 Wi-Fi MCU 进行认证，以实现最高安全性。不过，仍需进行核实以确保候选 Wi-Fi MCU 已通过 WPA3 认证。

确保互操作性

由于射频不匹配、软件和其他一些因素，Wi-Fi MCU 始终有可能无法与市场上的部分接入点通信。无法连接到常用的接入点有损公司声誉。尽管我们无法保证 Wi-Fi MCU 能与全球每个接入点（AP）搭配使用，但可确保 Wi-Fi MCU 通过了与市场上最常用 AP 的互操作性测试，从而能最大程度地减少问题。此信息通常可从制造商网站获取，但若网站未提供相关信息，可致电制造商获取信息，如果仍未能获取信息，请选择其他供应商。

需要得到帮助

最后但同样重要的是需要设计支持。如果没有一个全面的集成开发环境（IDE）平台，设计人员只能将一些不确定是否有用、简单或可靠的 Web 资源拼凑在一起。例如，少数 Wi-Fi MCU 制造商提供了有关产品的基本详情和原型设计说明，但就此止步，不提供将其从当前阶段转入生产阶段所需的信息。

真正有用的是，制造商应提供一个全面的 IDE（**图 3**），其中包括 Wi-Fi MCU 执行的每一个模拟和数字功能以及要在特定应用中实现所需要的全部外部元件。应提供一种方法将设计变更对整体性能的影响可视化，还应具备评估设计的 RF 性能和合规性的能力。一些基本工具可免费使用，另一些工具则以适中的成本提供，包括设计用于制造商的 Wi-Fi MCU 系列的评估板。

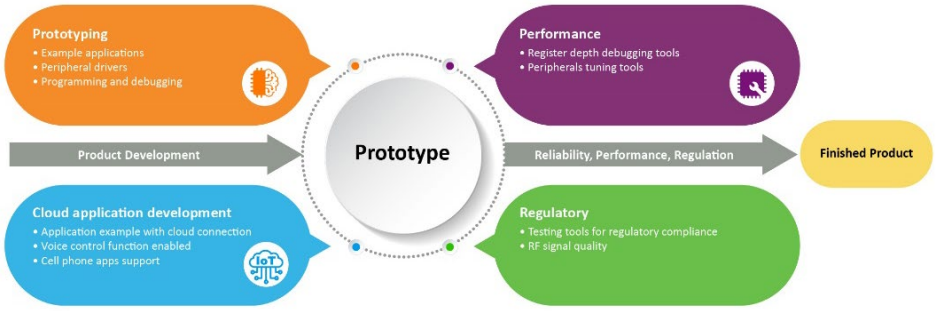

图 3.从原型设计阶段到成品，此类集成开发环境均能为设计人员提供调试工具和其他工具来降低风险

总结

物联网的发展趋势是将更多的处理能力转向网络边缘，而不是只集中于基于云的数据中心。为此，需要在最少的空间和元件中集成尽可能多的功能。Wi-Fi MCU 是众多 SoC 中的一种，它将多个功能集成在一个器件中，而不是分布于功能特定的离散元件，从而实现上述目标。

如果 Wi-Fi MCU 制造商可提供足够的资源，则将这些器件集成到嵌入式 IoT 子系统中可能相对简单。这些资源包括高度安全性（通过一种简单的置备方法来满足云服务提供商的需求）和全面的 IDE（引导设计人员从原型设计阶段转向生产阶段）。