如何调整现有设计
使之应用于物联网（IoT）

作者：Microchip Technology Inc.
业务拓展经理（EMEA）
Arild Rodland

对于许多人来说，当前联网家电数量的激增让人回想起 20 世纪 90 年代越来越多的个人计算机连入互联网的情形。当时，关于这项技术仅仅是一个噱头，还是确实会对社会产生持久影响，诸如此类的争论此起彼伏。如今，联网 PC 和手机已被认为是必不可少的设备，许多人预见到联网家电在全世界普及将成为必然趋势。

能够从全世界任何地方开启咖啡机似乎并不是改变生活的技术，但是咖啡机仅仅是家庭物联网革命的起点。物联网将成为在电器领域取得创新发展和寻求商机的基础。机器学习和人工智能技术的不断进步只会加速这一发展进程。从电器和传感器收集原始数据的能力将开启一个全新的世界，丰富的用例和机遇将接踵而至。

一些设计人员不确定是否要参与物联网革命，因为他们担心构建带有物联网连接功能的嵌入式设计会是一项艰巨的任务。而现实情况是，这些需求很容易实现。支持物联网的产品通常仅包含三个元素：处理器或单片机（“智能”元素）、网络控制器（“连接”元素）以及确保与云安全通信的方法（“安全”元素）。

由于大多数设计人员已经投入了大量时间和精力来打造出色的产品，因此重复使用大多数现有设计工作可带来极大的优势。通常，仅需将连接元素和安全元素添加到现有设计中即可实现物联网连接。无需从头开始设计解决方案，而是可以通过快速转换现有设计来连接到物联网。可以通过采用软件编程领域公认的技术高效完成这项任务，从而简化和加速开发过程。

分解挑战，逐一击破

嵌入式设计人员着手使现有产品能在物联网中运行的任务时，可以向软件编程人员学习一些技巧。面对复杂编程挑战的编程人员一直以来都采用自上而下的设计方法或模块化编程。这种方法涉及将较大的问题分解为较小的、更易于管理的子问题，而这些子问题又可以分解为更小的待处理任务。这是一种强大且经过验证的方法，能够解决单一代码难以处理的挑战性问题。那么，如何将这种方法使用到嵌入式硬件系统中呢？

事实证明，嵌入式系统工程师可以通过对其系统开发进行模块化处理来获得同样的好处。除了面临纯粹的编程挑战之外，嵌入式系统通常还需要符合相应标准并经过严格的认证流程。认证后更改软件或硬件可能需要重新认证产品。仅出于这个原因，将需要认证的部分拆分为多个子系统会带来巨大的优势。这样，一个子系统中的缺陷将不会影响其他子系统的性能。

例如，许多设计人员希望为新一代现有产品添加安全的互联网连接，以改善用户体验及方便添加各种功能，包括远程诊断、监视功能、自动履行服务和统计数据收集，从而为未来的产品增强做好计划。这种支持物联网的产品需要以下三个主要功能：1)原始应用；2)与互联网的连接；3)一种保护应用的方法。如图 1 所示，这种支持物联网的应用本质上是添加了安全功能和连接功能的原始应用。

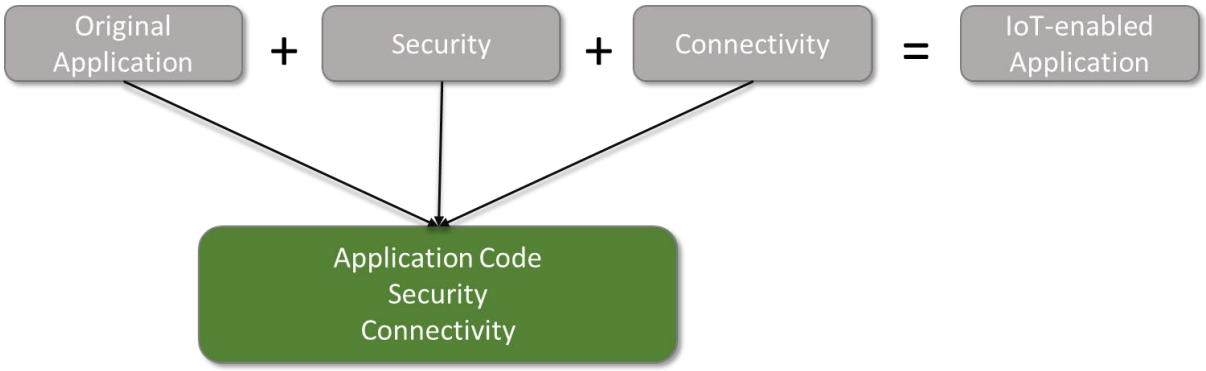
Original Application	原始应用
Security	安全
Connectivity	连接
IoT-enabled Application	支持物联网的应用

图 1：支持物联网的应用包括原始应用、安全功能和连接功能

从实现的角度来看，这种设计挑战可分为三个子任务：原始应用程序代码可重复使用，仅添加了安全功能和连接功能。

不过，对于工程师而言，从头开始添加安全功能和互联网连接功能都很复杂。此外，将新功能集成到现有应用程序中可能会干扰现有解决方案，从而降低组合应用程序的质量。开发人员通常会编写针对当前应用程序进行了高度优化的代码。因此，很难保证在添加时序关键连接功能和计算任务繁重的安全功能的同时，又保证更新后的产品达到相同的性能水平标准。

图 2 说明了这种组合方法。所有功能都作为单个解决方案实现，这增加了编写和调试应用程序的复杂性。一部分代码中的缺陷可能会影响其他关键功能的时序和性能，这可能会使简单的缺陷造成负面影响，进而导致需要进行重新认证。



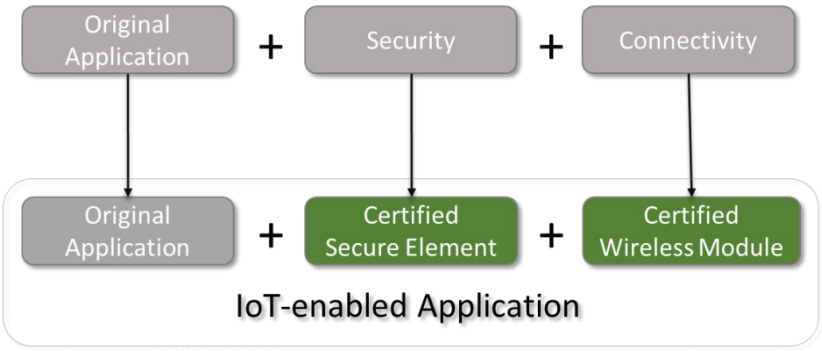
Original Application	原始应用程序
Security	安全
Connectivity	连接
IoT-enabled Application	支持物联网的应用程序
Application Code Security Connectivity	应用程序代码安全连接

图 2：在此集成解决方案中，所有代码和功能都集成在单个器件中，这会增加代码复杂性并延长代码开发时间

采用模块化方法将使设计人员能够保持其现有代码库和 IP 不变，仅根据需要添加连接和安全功能。

使用这种方法，可以将安全和连接功能实现为单独的软件和硬件任务，从而节省大量时间，并减少给定产品所需的工程师数量。该方法还可更方便地重复使用代码和系统，从而提供了更大

的灵活性。例如，设计人员可能希望同时提供同一产品的 Wi-Fi®和低功耗蓝牙（BLE）两种型号。在这种情况下，模块化方法可快速、方便地实现物联网设计的创新。



Original Application	原始应用程序
Security	安全
Connectivity	连接
IoT-enabled Application	支持物联网的应用程序
Certified Secure Element	经认证的安全元件
Certified Wireless Module	经认证的无线模块

图 3：借助模块化解决方案，设计人员可以重复使用现有应用程序，并将安全功能和连接功能隔离为与主应用程序无关的更小、更易于管理的任务

模块化方法的优点是，在向产品添加物联网连接时，不会丢失任何专注于优化和调整现有系统的工作。设计人员可以轻松添加所需的功能，而不会影响系统的其他部分。

为了简化过程，可以选择经过认证的模块实现安全功能和无线通信。这将极大缩短认证时间以及新产品上市所需的时间。Microchip 的 ATECC608A 器件就是一种经过认证的安全元件。此器件可处理与密钥和证书的验证以及安全存储相关的所有任务，无需编写任何代码即可提供安全的解决方案。同样，经过认证的无线模块可执行安全连接到无线网络所需的所有操作。

此外，使用经过认证的模块实现安全功能和无线功能时，不需要设计人员是安全或通信领域的专家。这些模块包含所有必需的代码段，通常由通过 UART、SPI 或 I^2C 等串行接口发送的简单命令控制。

为了进一步简化设计并缩短上市时间，诸如 Microchip AVR-IoT WG 开发板之类的开发板包含了这些模块，以实现安全且易于部署的物联网连接。利用这些工具，工程师只需花费 30 秒并通过几次点击便可将现有产品连接到 Google Cloud IoT Core，然后开始传输数据。

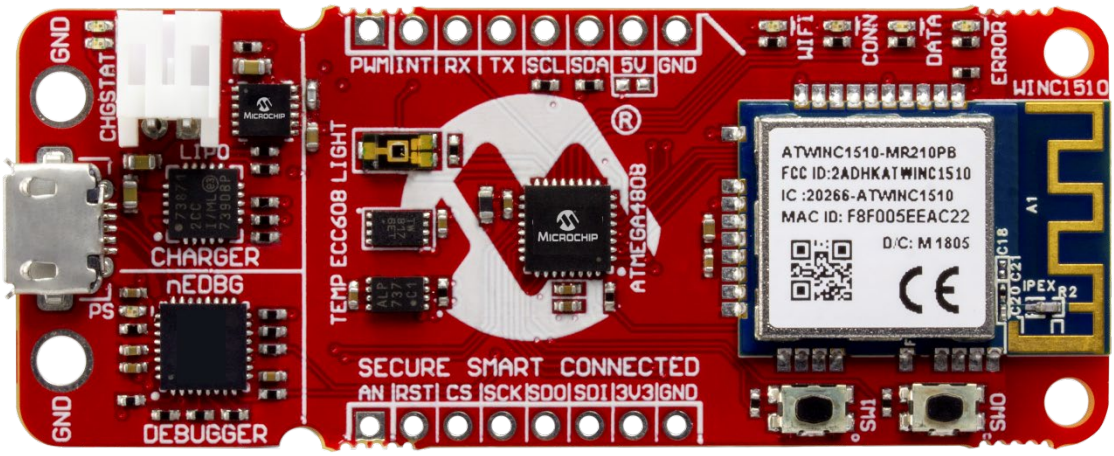


图 4：AVR-IoT WG 开发板结合了 AVR® 单片机、安全元件 IC 和经过认证的 Wi-Fi 网络控制器，可帮助设计人员在几分钟内完成联网设备的原型设计

如果能够将家电和消费产品连接到云，无论是为人工智能和机器学习应用提供大数据，还是仅提供一种执行安全远程固件更新的更安全方法，其潜在的价值都是巨大的。通过分解挑战和使用经过认证的模块来实现安全和通信功能，设计人员可以方便、快捷地调整当前设计来利用这些机会。