把安全性视为蓝牙低功耗赋能的无线微控制器的核心设计因素

作者：安森美(onsemi)产品经理 Ben Widsten

工业应用对无线联接有明确的需求。高度集成的方案将射频无线电与软件定义的数字控制相结合，形成一个无线微控制器（MCU），可满足这种需求。虽然市场上的无线MCU数量在不断增加，但设备制造商却越来越挑剔。他们需要射频提供的联接性，并敏锐地意识到每个层面的安全需求。

即使在最近，安全性也并不总是"作为标准"集成到方案中，这意味着许多目前正在使用的和仍被选用于新设计的无线MCU，可能无法提供与即将上市的最新方案同等的安全水平。半导体制造商和IP供应商一直在学习更多的安全知识，通过合作分享经验和发现潜在的攻击载体。

与新的网络威胁的不断斗争意味着今天对任何平台的构思需要考虑如何为明天提供保护。这需要一个强固的基础，支持安全的固件无线更新（FOTA）。添加一个全集成的射频无线电可帮助提供安全性，但它也代表了黑客的一个明显的攻击媒介。

集成的优势

许多物联网(IoT)端点依靠无线联接来提供真正的远程功能。这些终端越来越多地在家庭、办公室、工厂和其他工业领域等智能环境中运作。低功率无线联接使用节点之间的短跳(short hops)来提供广域覆盖。在这方面，蓝牙低功耗（Bluetooth LE）技术得益于低功耗，其吸引力近年来已大为增加。蓝牙低功耗也是PAN/LAN联接中使用的最固有的安全协议之一。

采用蓝牙低功耗，其低功耗特性得以进一步改善，从而提供更大的联接范围和带宽，但仍考虑最小化系统功耗需求。因此，在考虑终端使用哪种技术时，蓝牙低功耗处于有利地位，特别是如果该终端是电池供电的。在应对IoT的发展需求方面，其他无线PAN协议没有更大的发展，而蓝牙低功耗实现了这一点并降低功耗。蓝牙的普遍性也是一个因素。蓝牙作为智能手机的一项基本技术，使得边缘节点的配置变得更加容易和随时可用。

蓝牙低功耗的所有优点现在都可以集成到高功能无线MCU中，有效地为互联应用提供了一个单芯片方案。当获软件支持时，这些器件可以加速和简化开发。这也突显了对同样全面的安全功能的需求，这些功能基于协议本身的能力而构建，以提供保护，免受在线威胁。

无线MCU中的系统级安全

由于安全如此重要，需要在裸机层面就考虑进去。这代表安全功能将成为处理器本身的一部分，并提供更多基于硬件的安全功能，让黑客不能攻击。这包括使用加密方法进行认证和授权，以及安全创建、共享和存储密钥以实现加密。

当以这种方式实施时，就有可能增强蓝牙低功耗协议已提供的安全功能，例如增加含信任根的安全启动。在Arm®生态系统中，这可通过选择实施Arm TrustZone®和CryptoCell-312安全IP来实现。这为基于Armv8-M指令集的Arm Cortex®实施增加了安全功能。CryptoCell被设计用来提供一些重要的功能，包括真正的随机数生成（TRNG）、代码加密和数据验证。它还支持回滚保护和生命周期管理，这些都被认为是其他IoT设备的弱点。这提供了一个认证的执行环境，并使用密码学以及软件更新验证。

Arm的TrustZone设计用于支持整个芯片设计的物理隔离区以提供硬件安全性，从而在软件和应用层面实现执行隔离。这些技术共同提高了整个方案的安全水平。

这些功能结合蓝牙低功耗时，甚至可以被配置为通过使用蓝牙低功耗的定位功能来提高在线安全性。在工业IoT中，绘图和定位正变得更整合，以提供资产跟踪和室内导航等附加服务。能够安全地验证试图加入私有网络的本地设备，是这些功能将如何互操作的一个例子。

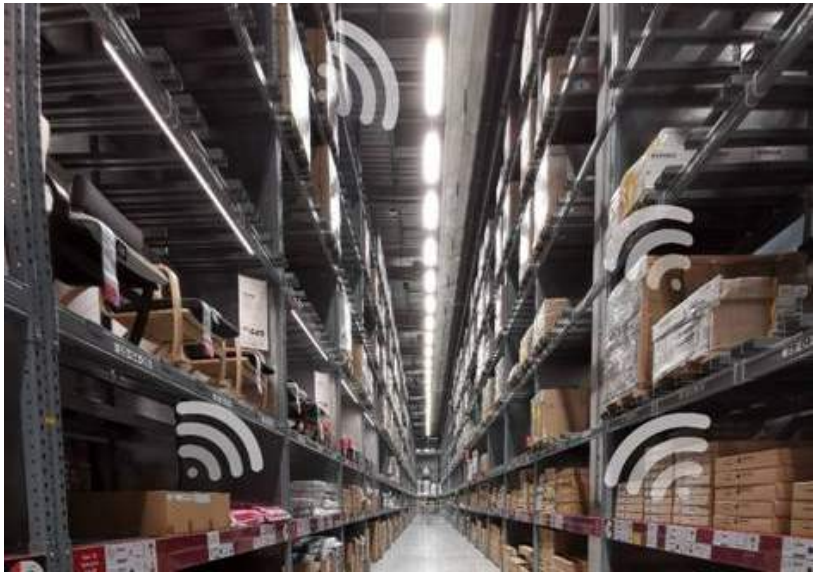

图1：蓝牙现在正被用于室内导航、资产追踪和标记

安森美(onsemi)的RSL15是这种新一代蓝牙5.2无线MCU的一个很好的例子。它代表了安森美无线联接方案组合的延续，基于其在蓝牙低功耗和Wi-Fi的专长而构建，形成了RSL系列的下一步发展。RSL15与RSL10一样，是业界功耗最低的基于闪存的蓝牙低功耗方案。RSL15改进了这一领先业界的无线电，并与含Arm TrustZone CryptoCell-312 IP的Arm Cortex-M33子系统集成在一起，同时增加了一些专门针对工业边缘节点的其他功能。

这些功能包括采用高分辨率的RSSI（接收信号强度指示）、到达角（AoD）和出发角（AoD）形式的增强型定位技术。它具有长距离、高速（2 Mbit/s）的PHY，支持多达10个同时联接。

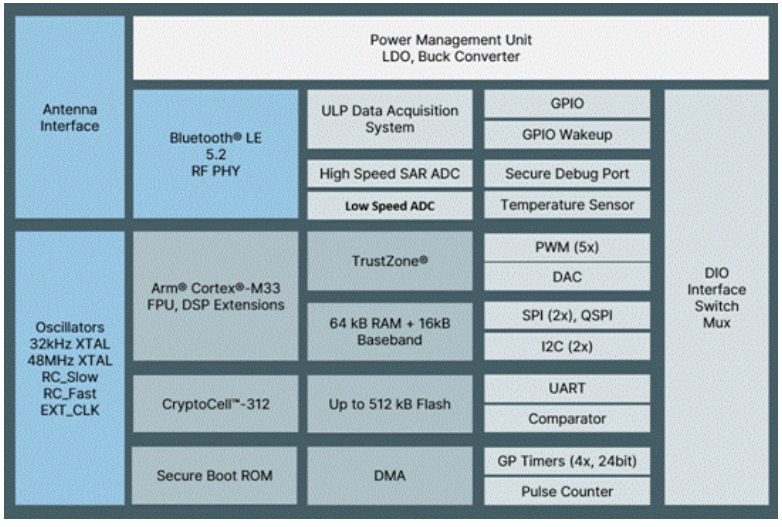

图2：RSL15的高级框图

RLS15将联接性和安全性结合起来，为互联工业应用提供理想的平台。包括PWM、PCM、I2C、SPI、GPIO、UART和RTC在内的外设支持进一步加强了这一点。直接支持RSL15用于超低功耗应用中的一个额外功能是智能感知(Smart Sense)电源模式。这允许一些模拟和数字外设保持工作并获取数据，同时器件的其他部分处于更深的睡眠模式以省电。例如，片上ADC和FIFO可被配置为激励和采样外部传感器，只有在满足预定条件时才唤醒处理器内核。

更容易的安全联接

在硬件层面的整合只是方案的一部分。要获得这些先进功能，需要一个同样全面的软件开发环境。安森美开发的基于Eclipse的IDE以及其他支持Arm Cortex-M33处理器的商业IDE都支持RSL15。作为一个基于Arm的方案，软件方面的许多繁重工作是通过生态系统和使用CMSIS包提供的。

在内部，RSL15使用闪存，这意味着一切都可以安全地无线更新。这包括在设备部署后的操作系统、蓝牙协议栈和客户的应用程序。固件在闪存中通过基于证书的机制，使用私人-公共密钥方案进行认证。

经由蓝牙低功耗安全地联接工业IoT(IIoT)

蓝牙低功耗在工业应用中越来越受欢迎，但同时带来对更高安全性的需求。RSL15具有先进的安全功能和领先的蓝牙低功耗无线电，它将可编程方案的灵活性与业界一流的加密和认证的保证结合起来。结合广泛的软件支持、SDK和开发硬件，安森美已准备好协助制造商开发安全的互联方案。