白皮书

物联网通信模块的设计需求

Naoyuki Tsubaki，物联网产品营销部门，瑞萨电子株式会社

2019 年 7 月

摘要

随着物联网的快速发展，以往没有连接到网络的许多设备也逐渐需要集成通信模块功能。反过来，安全威胁的数量和危害性也处于上升态势。因此，微控制器必须满足一系列要求，包括减小占用空间、降低功耗、增强安全性和及时提供空中下载(OTA)固件更新功能。

引言

互联网技术和各种传感器技术的快速进步推动了物联网的发展，催生出覆盖广泛用途的大量设备。根据市场预测公司发布的数据，预计到 2022 年，物联网设备的市场规模有望增长至一万亿美元。边缘设备集成了面向不同标准的通信模块以及特定的传感器模块（取决于物联网设备的应用和用途），尺寸不断缩小，而且将实现更多功能。因此，这些设备中的微控制器必须满足市场的需求，不仅包括高性能、低功耗等现有要求，还包括更紧凑的封装尺寸和更小的占用空间。

此外，应用开发还需要添加增值功能来提供物联网支持，并且开发程序代码来处理各种通信接口的协议堆栈。这会增加控制复杂度和代码尺寸，意味着微控制器不仅需要性能强大的 CPU，还需要充足的大容量闪存 ROM 和 RAM。从硬件设计人员的角度来看，产品系列变得更加多样化，为了降低开发成本，需要使用专门优化的平台化设计，尽可能多地采用通用电路板开发，实现引脚布局和外形的兼容性。因此高规格、小封装的微控制器是理想的选择。

顾名思义，物联网设备使用了互联网连接，越来越多的人意识到，必须确保物联网设备本身（即边缘设备）的安全性。近年来，以连接到互联网的物联网设备作为网关的网络攻击日益猖獗，另外还出现了利用安全漏洞来劫持设备或利用设备进行监听的事件。这就使得实施适当安全措施成为一个重要问题。如果没有适当的安全措施，设备就会始终面临黑客攻击和劫持等各种风险。为了解决此类问题，必须在充当端点的边缘设备上引入安全措施。这也凸显了整体生命周期管理的重要性，包括在初始制造和运输过程中确保安全的程序写入，以及在进入市场之后，需要安全补丁来修复程序代码出现的问题。常规的方法是为传统控制器添加专用的安全设备，并且咨询安全领域的技术专家后进行系统设计。但对边缘设备来说，由于成本限制，需要更短的开发周期(TAT)，这些实现方法非常困难。因此，我们希望将安全功能集成到微控制器中。

本白皮书阐述了将要安装在物联网边缘设备中的产品应满足的要求。

小占用空间和高性能

随着紧凑型模块的发展，负责功能控制的中央微控制器必须采用占用空间很小的封装。例如，市场上各种通信模块产品系列的微控制器占用的空间通常为10 x 10 mm，但急需5 x 5 mm甚至更小的封装。除了减少封装的占用空间，还需要更大的ROM容量来支持各种应用，以及足够的RAM来处理协议栈。这些产品系列应该能够允许用户根据应用规模来选择合适的存储器容量。在传统的微控制器中，存储器容量和小封装体积需要权衡，难以兼顾。因此，市场上当前的小封装控制器主要是1 MB ROM/256 KB RAM产品。

通过业界领先的 40nmFlash 制程技术，使得我们能够扩展 RX651 产品系列，添加 4.5 x 4.5 mm 封装、2 MB 内部闪存 ROM 和 640 KB RAM 的新产品。与目前已经量产 RX651 系列中最小的 7.0 x 7.0 mm 产品相比，它的占用空间减小了 60%，这让我们可以更灵活地满足市场需求。我们的产品阵容强大，覆盖从 512 KB 到 2 MB 的内部闪存 ROM、从 256 KB 至 640 KB 的 RAM。采用小型封装的 64 引脚产品实现了所有存储器配置之间的引脚兼容性，这有助于客户使用通用的元器件和电路板设计，基于平台来创建产品系列。

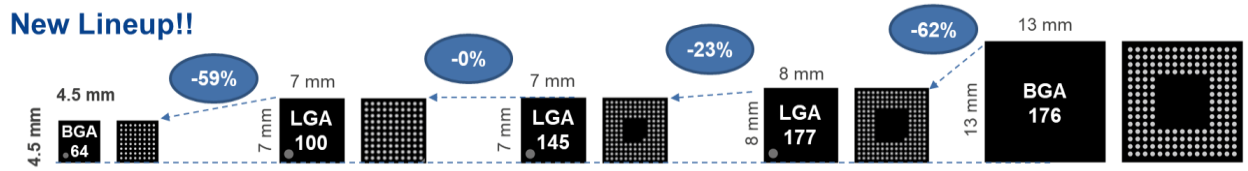

图 1：RX651 64 引脚 BGA 采用小尺寸封装

嵌入式系统中的信任根

开发嵌入式系统时，要在硬件和软件中实现安全功能，需要掌握这些方面技能的资深开发技术人员，其高额成本会成为另一道障碍。此外，让最终用户认可安全性的价值也不容易。如果某些应用中的安全功能明显非常重要，例如在金融交易和机密信息处理中，那么市场会将强大安全性视为增值内容，通常会投入大量开发资源和成本。在这些市场中，使用专用芯片来实现强大安全性一直是通行做法。

近年来，物联网的发展促使越来越多的制造商考虑实施安全功能，甚至延伸至以往不联网的设备。但是，由于缺乏安全方面的经验，设备制造商通常也更熟悉传统的微控制器，利用通用微控制器实现强大安全功能成为了一种合理的做法。这也成为了边缘设备开发的要求。

另外，物联网设备连接到网络时，云端或服务器有可能无法确保安全性，或者充当数据传输和接收中继点的接入点无法确保安全性。因此，作为端点的物联网边缘设备必须拥有集成的安全功能。为了实现这个目标，边缘设备应该带有信任根元件，让设备自身能够确保安全运行。

RX651 微控制器在硬件中实施信任根，提供 Trusted Secure IP(TSIP)功能来保护密钥数据，防止密钥泄露并且提供存储器保护功能，防止已授权的程序被篡改。

RX651 1.5 MB 和 2 MB 闪存的产品，集成了 Trusted Secure IP(TSIP)专用硬件 IP，用于管理密钥，防止对密钥的非法访问，并可通过索引信息来隐藏这些密钥，将它们安全地存储在内部 ROM 中。

此外，所有 RX651 产品中的存储器保护功能允许为内部闪存启用区域保护。这样可以确保将代码存储在无法从外部改写的专用存储器区域中。由于检测恶意代码的安全代码可以通过这种方式得到保护，因而实现了全面安全性。

采用 TSIP 的 RX651 系列产品不需要依赖专用安全芯片。利用通用微控制器自身的 TSIP 硬件功能和特性，建立强大的安全性。

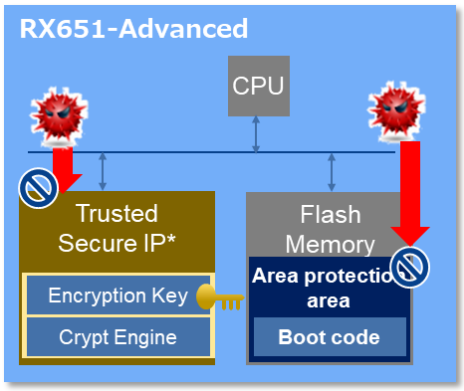

图 2：通过 Trusted Secure IP 和区域保护实现的信任根

RX651 的 Trusted Secure IP 不仅支持 AES 和 3DES 等常用密钥加密方法，还支持 SSL/TLS 通信所需的 RSA 非对称加密。可基于硬件实现连接到不同云服务所需的加密通信，这样可以实现高吞吐量，而不会增加 CPU 负载。

简单的固件更新

通过网络进行固件更新的功能可以视为物联网设备的一个至关重要的特点，它让用户能够在产品上世后继续为产品添加新功能，修复应用错误，增强产品的安全性。由于网络攻击方法不断演进，用户必须为现有产品打补丁。使用传统微控制器，一般要将新固件下载到专用备份存储器区域，并执行专用的更新程序，来执行固件更新。除了要求控制器提供单独的备份存储器之外，这种方法还必须在下载或系统更新时停止系统原来的工作。作为面向物联网应用的处理器，我们希望在内置存储器中部署备份区域，并且实现后台下载。

RX651 的 2 MB 和 1.5 MB 闪存版本提供了 Dual Bank 功能，支持后台运行(BGO)。因此，我们只需利用内部闪存即可实现固件更新，而无需停止系统工作。Dual Bank 功能可将内部闪存分为两个独立的存储区域，一个区域用于执行程序，另一个区域用于下载固件。利用 BGO 功能，可在执行程序代码的同时，通过通信接口接收新固件并将其写入固件下载区域。当后台写入进程完成后，将设置执行区域切换寄存器，执行复位，执行区和下载区就会互换，开始运行新的固件。引导程序内可以包括检查固件是否损坏的步骤，如有必要，还可以轻松地恢复到旧版固件。

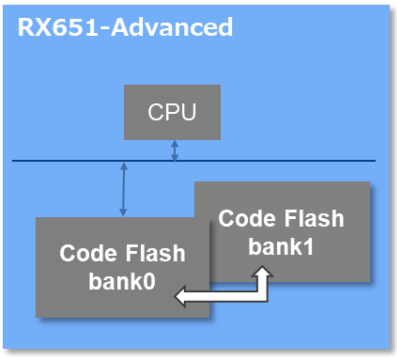

图 3：Dual Bank flash 功能

结论

RX651 的 64 引脚封装产品，将适用于物联网通信模块的多种特性集成在单个芯片中，例如小封装、高存储器容量、安全性、固件更新，提供最高达到 2 MB ROM 到 640 KB RAM 的多个可选版本，以适应各种规模的应用。在不增加额外成本的前提下，这些特性使得该产品系列成为适用于物联网设备的理想微控制器。