白皮书

如何解决嵌入式物联网设计的 6 大安全挑战

2019 年 8 月

摘要

嵌入式物联网设计的安全保障任务不仅充满挑战，而且十分耗时，即便对于资深开发人员亦不例外。探索六种常见的安全挑战，了解瑞萨电子怎样提供基于平台的安全解决方案，从软硬件领域的最新技术发展中获益，并提供深入而全面的多层级防御保障。

物联网常见的安全挑战

预计到 2020 年将会部署 310 亿台物联网(IoT)设备，其中许多设备的安全控制都比较有限，可能会成为黑客的攻击目标。为什么这么多的嵌入式系统都存在设计漏洞？很大程度上是因为开发人员在嵌入式应用和设备安全领域面临着多种挑战和复杂的问题。他们必须密切关注日益变化的威胁环境，并满足不断发展的安全标准。同时，复杂的应用可能也需要满足多种标准，而它们可能会令设备的兼容性和灵活性受限。在很多开发场景下，安全功能的级别越高，相应的成本和功耗可能也会越高，从而可能对终端设备的市场销路造成不利影响。

在本白皮书中，我们确定了嵌入式系统开发人员最常面临的六大安全挑战并提出了见解和解决方案，以帮助简化安全设计工作流程，加快向市场推出安全的设备、服务和系统。

本白皮书所研究的嵌入式系统开发人员面临的六大安全挑战如下：

1. 2019 年了，如何保障我的产品设备安全？
2. 如何保障我的产品安全，以免它们被非授权复制品替代？
3. 如何比较简单地管理安全问题？
4. 如何保护我的设备来抵御多种安全威胁？
5. 我不是安全专家，但我需要安全的产品。我需要了解什么信息？
6. 如何从供应商处获得更多安全相关的标准化和支持，从而将自己的资源运用到产品的差异化设计部分？

挑战 1：2019 年如何保障我的产品设备安全？

几年前，应用开发人员完全无需担忧产品的安全问题，因为设备和应用不像现在这样连接到网络。如今，即便是灯泡、婴儿监控设备和处方药容器等最基础的产品，都需要连接互联网或云。而安全往往会被人忽视，或事后才会亡羊补牢。

2019 年，保障物联网应用不受网络威胁攻击，保护数据和产品功能成为开发人员主要关注的问题，而且必须在软硬件层面上，从设计之初就植入设备当中。基于平台的安全解决方案利用软硬件领域最新的安全技术实施深入而全面的保护，从而提供多层安全防御。

在硬件方面，有效的安全方案需包括：

- 安全密钥管理，旨在确保密钥在明文状态下不可访问。设备应能够安全生成和存储密钥（包括私钥），以实现真正安全的设备唯一标识和配置。
- 硬件加速加密、哈希运算和真随机数生成，旨在加速设备上的加密运算。这种硬件支持可节约处理时间和功耗。
- 提供安全的存储器访问，保护 RAM 和闪存的特定区域，防止未经授权的访问。独立的存储域可将敏感代码和数据与非安全的代码和数据隔离。与此同时，一次性写入保护存储器可防止代码和数据被篡改或重新编程。
- 提供调试和编程访问保护，从而降低黑客使用调试器和编程接口作为攻击切入点的风险。

软件方面应包括：

- 集成并优化的商用级软件，提供经过验证的应用框架和标准 API。
- 通过驱动程序 API，为硬件安全功能提供易用的接口。
- 包含诸多 API 的加密库，提供宏观安全功能、信任根等各种安全功能，并具备识别可信源与可信代码的能力。
- 原生支持常见的通信协议和传输协议，例如安全超文本传输协议(HTTPS)、传输层安全协议(TLS)和其他特定的云协议。

十余年来，瑞萨电子一直处于嵌入式系统安全领先地位，能够充分了解并解决当今互联产品日益强化的安全需求。瑞萨电子提供基于平台的嵌入式安全解决方案，它具有多层次开发基础架构，可为各种嵌入式产品带来深入的安全保护。

例如，Renesas Synergy™平台是一个全覆盖的优质开发平台，其中包括量产级软件和一系列可扩展的引脚兼容的 MCU，并预先经过集成和测试，能够提供多层级安全保障。Synergy 平台可确保在安全可靠的技术基础上构建物联网应用。

Synergy 平台通过安全加密引擎(SCE)模块提供多种密钥生成选项。SCE 可生成基于硬件的，唯一并加密的设备标识，并利用安全存储保护单元(SMPU)和闪存访问窗口(FAW)将其安全地存储在芯片内部闪存中。此外，您还可以利用 Synergy MCU 提供的存储保护功能来存储安全启动代码、证书、密钥以及其他任何敏

感数据。而且，即使使用非安全的存储器，SEC 也能提供安全的密钥存储，以防敏感信息泄露。通过对密钥进行 MCU 硬件相关的唯一密钥封装，可确保密钥隔离，它会通过 MCU 的唯一识别码对每个 MCU 上的密钥进行加密，使得每个 MCU 的 SCE 模块内部只能使用自己这颗 MCU 加密过的密钥。

安全加密引擎

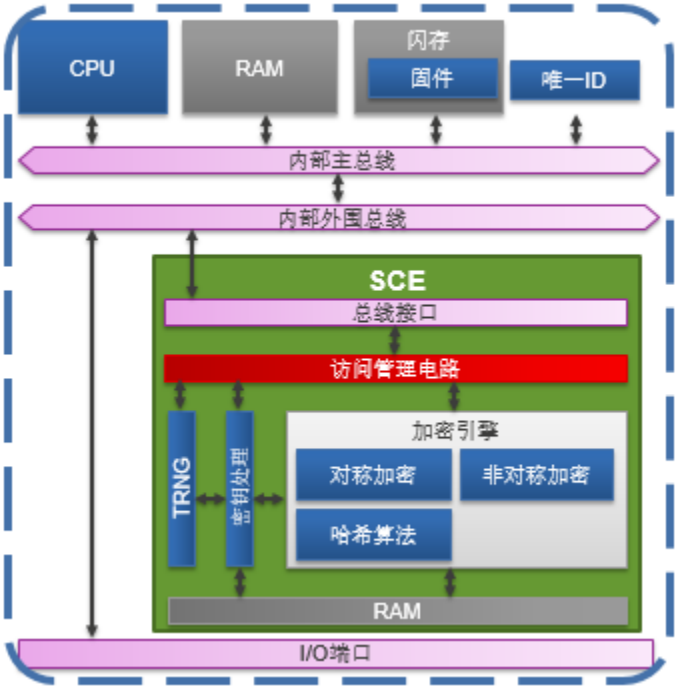

图 1：安全加密引擎 - MCU 内的独立子系统（来源：瑞萨电子株式会社）

此外，开发人员还需要确保通过开发平台能够使最终产品安全轻松地连接到云。随着物联网应用越来越复杂，越来越重视安全性，它们需要具备更强的数据处理能力。由于这些系统越来越依靠云计算来提供物联网数据所需的超级计算和存储基础架构，安全的云连接成为不可或缺的条件。Synergy MCU 通过内置 MQTT 和 TLS 模块为云连接提供支持，而 Synergy 云连接应用提供了内置的安全云连接，可连接到 Amazon Web Services (AWS)、Google Cloud 和 Microsoft Azure 等领先的云环境。

挑战 2：如何保障我的产品安全，以免它们被非授权复制品替代？

不想您的产品被仿制品替代？那么，您得确保竞争对手无法轻松克隆您的设备。为此，您需要确保所销售的产品当中包含某些只有贵公司才能提供的专有功能。

如今，全球供应链都需要努力增强安全性，以确保制造和生产过程中产品的完整性和真实性。

一种办法是通过实施安全制造流程，降低知识产权泄露的风险并保持生产工艺的完整性。Synergy 安全引导管理程序可提供安全的固件闪存编程解决方案，使开发人员能够安全可靠地向制造工厂里的 Synergy MCU 闪存中，远程写入授权固件。这样可防止固件被盗版、篡改或安装到克隆硬件中。

此外，Synergy 安全引导管理程序还能提供强大的信任根，支持唯一标识、硬件密钥保护、安全引导程序、安全闪存升级模块，并提供与 MCU 硬件对接的加密 API 。信任根可以通过安全连接，预先加载到那些专门用来制造和配置处理单元的量产编程系统当中。经过配置的芯片可安全存储数据，并严格控制数据的使用方式。

瑞萨电子 Synergy 安全引导管理器

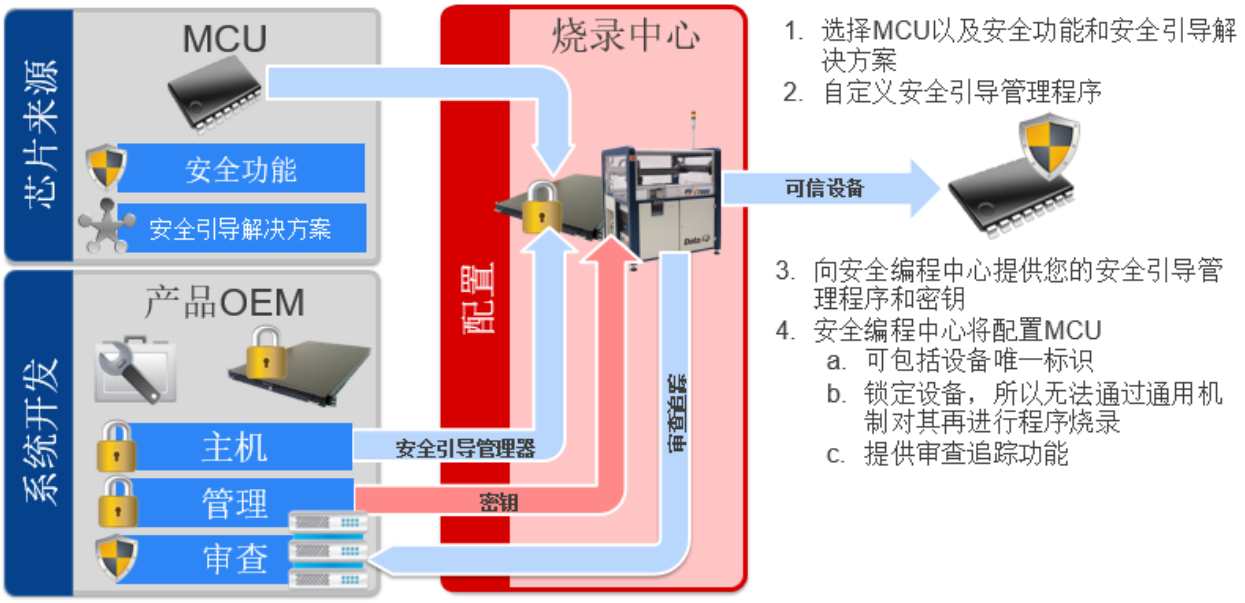

图 2：瑞萨电子 Synergy 安全引导管理程序提供安全的固件闪存编程解决方案（来源：瑞萨电子株式会社）

一旦产品进入市场，安全引导管理程序便可以通过片上信任根，将授权固件安全地更新到 Synergy MCU 的闪存当中：首先对固件进行验证和解密，然后再进行闪存编程，一切均通过安全的云端基础架构进行安全配置，使瑞萨电子的云连接解决方案更加可靠，更值得信赖。

当然，您也可以选择瑞萨电子的合作伙伴来协助您，他们提供安全配置和编程解决方案及服务，致力于以合理的成本保障制造安全。

挑战 3：如何比较简单地管理安全问题？

为嵌入式系统设计深入的分层安全方案充满挑战且十分耗时，而缩短学习曲线的一种办法就是确保开发平台中已内置最新的安全技术和协议。使用 Synergy 平台，开发人员不必学习各种新的相关协议及其他安全保护措施，即可构建安全应用。

Synergy Software Package (SSP)简化了安全互联嵌入式系统开发常用的复杂功能。使用闪存和 SRAM 读写保护，SSP 可保护开发人员用来创建和存储部分代码的存储器区域。这样，开发人员即可创建自定义存储器区域，用来存储临时密钥、私钥及其他敏感数据。

Synergy 平台支持公钥基础架构(PKI)，这是一种通过数字证书提供身份验证的加密方法，也支持预共享密钥(PSK)，这是通信双方在建立数字连接时指定相同密钥进行授权身份验证的加密模型。PSK 提供的加密形式较为简单，可为少量用户访问控制这类应用情景提供适当级别的保护。PKI 实施和管理起来较为复杂，但它属于非对称加密，可验证用户，生成和分发证书，还能维护、管理和撤销证书。无论使用公钥还是私钥，PKI 通常被视为更安全的加密模型，常用于大型加密系统的身份验证。

Synergy 平台提供优化的商用级软件及标准 API，简化了与硬件安全和加密功能的接口方式。应用框架帮助简化了应用代码和底层驱动程序之间原本复杂的无线驱动程序与统一接口的集成问题。这种抽象层级降低了复杂性，并使集成网络协议栈，或根据应用需求断开或加入驱动程序这样的工作变得更加简单。

挑战 4：如何保护我的设备来抵御多种安全威胁？

如今，网络威胁环境充满了许多不利因素和风险。毫无准备和保护的产品上，漏洞和攻击点无处不在。为了帮助设备抵御多种安全威胁，我们需要通过基于硬件生成密钥的方式保护设备标识。该标识可以安全存储在内部闪存中，用来建立互信，在添加到设计和配置到目标应用后还能提供保密功能。

建立强大而安全的设备标识，可使每台物联网设备都能被单独识别并进行身份验证，成为为唯一设备。这样即可针对各个设备设立具体的保护方案，并能对它们与其他安全设备和服务的通信进行加密。强有力的设备标识通过物联网分层安全保护方案来抵御多种安全威胁，它们提供以下功能：

- **信任。**一旦连接到网络，该设备必须通过身份验证才能和其他设备、服务和用户之间建立信任，由此可安全地交换加密数据和信息。信任始于设备正确通过身份验证，从而确保它是合法设备，不是仿造品。

- **隐私。**在物联网内获取和共享的数据信息通常包括敏感数据、个人或财务数据，必须予以保密并保障安全才能满足法规要求。安全设备标识为保障物联网设备和系统连接共享数据时的信息保密奠定了基石。

- **完整性。**确保网络内共享的数据不被篡改是分层安全方案的重要组成部分。数据完整性是一项常被忽视的安全要求，但互联设备和系统依赖于所传输信息的真实性（信任）、保密性（隐私）和完整性。

按系列统计的瑞萨电子 Synergy MCU SCE 硬件安全功能

	功能		密钥封装	NIST CAVP	S7	S5	S3	S1
标识和密钥交换（非对称）	RSA	密钥生成、签名/验证[1]	Y	Y[5]	1024/2048/4096	1024/2048/4096		
	ECC[4]	密钥生成、ECDSA、ECDH[2]	Y	WIP	NIST P192/P224/P256/P384	NIST P192/P224/P256/P384		
	DSA	签名/验证			L：2048/1024，N：256/226/160	L：2048/1024，N：256/226/160		
加密（对称）	AES	ECB、CBC、CTR	Y	Y	128/192/256	128/192/256	128/256	128/256
		GCM		Y	128/192/256	128/192/256	128/256	
		XTS、CCM			128/256	128/256	128/256	
	3DES	ECB			192	192		
		CBC			192	192		
		CTR			192	192		
数据完整性	哈希算法	GHASH		Y	Y	Y	Y	
		SHA1/224/256		Y	Y	Y		
	TRNG	带DRBG-AES-128的硬件熵		Y	Y	Y	Y	Y
	唯一ID				Y	Y	Y	Y
数据保护	MPU	Arm、Bus Master、Bus Slave			Y	Y	Y	Y
	MPU	安全性				Y	Y	Y[3]
	FAW	编程/擦除保护			Y	Y	Y	Y
	SCE	加密模块			SCE7	SCE7	SCE5	
	SCE	密钥安装和密钥封装			Y	Y	Y	

[1] 仅限4096位验证、加密
[2] 通过标量乘法
[3] 不适用于S124
[4] 对于低级别驱动程序，需要配备SSP v1.5.0
[5] 对于低级别驱动程序，需要配备SSP v1.6.0

图 3：Synergy 平台推出的瑞萨电子 Synergy MCU（来源：瑞萨电子株式会社）

数据的安全也是抵御多种安全威胁的重中之重。静态数据是指设备或网络之间没有经常传输的数据，通常驻留在 SRAM 或非易失性存储器中。为了保护静态数据，Synergy MCU 提供了多种数据访问控制，包括读取保护、写入保护、读写保护和一次性写入保护。控制对存储数据的访问，可以减小攻击面，提高系统安全性。

此外，现场部署的 Synergy MCU 还支持远程更新，从而能够抵御最新的网络威胁。

挑战 5：我不是安全专家，但我需要安全的产品。我需要了解什么信息？

要为基于嵌入式设备的产品提供全面而深入的安全保护，需要采用高度集成的优化平台，综合运用多种协议和安全保护措施，多方面保障安全。

瑞萨电子 Synergy 平台通过建立完整的开发环境，提供一系列独有的内置硬件和软件安全功能，为开发人员提供了先发优势。这些功能均基于共享的信任根构建，满足嵌入式设备和物联网安全的要求。此外，该平台还拓展了制造安全可扩展制造能力以及保护知识产权的能力。

开发人员还能利用瑞萨电子在线应用项目库，通过逐步说明和指导来构建端到端安全解决方案。

而且，基于 Synergy 平台进行设计可为您提供庞大且可靠的瑞萨电子社区与联盟伙伴生态系统支持。瑞萨电子建立了经过培训和认证的设计服务合作伙伴网络，可为您设计周期的每个阶段提供支持，帮助您实现

设计和业务目标。利用瑞萨电子合作伙伴有助于加快开发进度，并可将深厚的专业知识应用到您的安全解决方案开发流程中。

挑战 6：如何从供应商处获得更多标准化和安全支持，从而将自己的资源运用到与众不同的设计部分？

开始开发前，请务必选择提供高度集成平台的 MCU 解决方案，以便综合运用各种功能，从多方面保障安全。当设计和安全协议变化，产生黑客可渗透的弱点时，恶意代理就可能会利用这些嵌入式设计中的漏洞。如果 MCU 硬件、软件、通信堆栈和驱动程序并非完全标准化，并集成到应用框架中，情况将尤其危险。

全面而完整的集成开发平台以及深入的安全保护可最大程度地简化设计安全保障任务。开发平台包含各种核心软件、应用功能、协议栈和驱动程序，选择一种集成了这些功能的应用框架，开发人员便可摆脱较底层的集成工作，专注于设计可令产品脱颖而出的特性和功能。

此外，确保您的解决方案提供商拥有有效的完整的合作伙伴生态系统。您可以选择将特定安全特性或功能开发任务外包给可靠的专家，这样还可节约时间并增强最终产品的品质。

瑞萨电子 Synergy 平台是一款全面的优质开发平台，其中包括量产级软件、一系列可扩展的引脚兼容的 MCU、应用框架、功能库、HAL 驱动程序以及先进的软件工具和开发套件，可确保在安全可靠的技术基础上构建应用。该平台内置深入的分层安全方案，能够提供唯一识别信息和并对各个设备进行身份验证，确保设备、服务和用户之间安全通信。

通过和瑞萨电子合作，安全性会根植到平台中，使设计人员能够将跟过时间和技能专注于更上层应用的的挑战和创新，从而抓住快速演变的物联网市场机遇并满足消费者需求。鉴于瑞萨电子已对各种功能预先进行集成、测试和验证，所以工程团队可在 API 级别开始应用软件开发，从而节约数月的时间和精力。

此外，开发人员还可以依靠瑞萨电子合作伙伴的专业知识，他们可携手帮助您开发特定的安全特性或功能，为您现有的团队提供支持或为您的开发过程增添宝贵的技能和经验。

结论

瑞萨电子通过提供基于平台的安全解决方案帮助嵌入式系统开发人员解决设计安全挑战，该方案利用软硬件安全领域的最新突破技术提供深入而全面的多层级安全保障。瑞萨电子 Synergy 平台基于共享的信任根而构建，可深度保障物联网设备、服务和网络的安全，从而确保整个产品生命周期的制造安全和扩展性以及知识产权保护。