白皮书

如何通过安全和可扩展的方式来管理数以千计的设备

2019 年 2 月

摘要

在当今的互联世界中，要为物联网 (IoT) 应用提供全面深入的安全保护，在多个方面带来了挑战。Renesas Synergy 平台提供一系列独特的硬件和软件安全功能，结合在一起可以满足保护物联网设备和网络安全的需求，包括能够在远程生产过程中，确保安全和灵活可调的生产以及知识产权的保护。Renesas S5D3 是 Synergy 微控制器 (MCU) 系列的最新成员，它极大增强了 Synergy 平台的功效，提供远超出同类器件其他解决方案的安全保护方案。通用型 S5D3 不仅工作非常高效，其价位也颇具吸引力，因而成为一款非常引人注目的 MCU 产品，可为物联网系统中的端点设备提供先进的可扩展安全管理。

物联网的安全挑战

不久之前，应用开发人员还无需太担忧他们产品的安全保护，因为应用的连接方式与现在有所不同。但现在，即便最基本的物品 — 从电灯到儿童玩具和电器 — 都要通过互联网或物联网中的云环境接入网络。以前我们只需使用密码和防火墙就足以保证安全，而现在安全要求已经大幅提高。保护物联网应用的安全，以防止数据和目标功能遭受网络安全威胁，已经成为开发人员最为关注的主要因素，而不能事后才注意到安全问题，他们需要在硬件和软件层级，将安全功能内置到器件中。

随着安全威胁的破坏力增大，恶意程度加深，安全标准也在不断演进，复杂的应用可能需要满足多种安全标准，这会影响设备兼容性和灵活性。在很多开发场景下，更先进的安全功能也带来了更高的成本，通常还会提高功耗，从而影响最终应用的市场销路。

因此，物联网应用必须解决一系列特定挑战，包括：

- 保护知识产权，在制造过程中防范知识产权盗窃、产品克隆、过量生产等威胁。
- 防御安全漏洞攻击，这些攻击手段可能用于关闭或损坏关键基础设施甚至导致伤害。
- 保护动态和静态数据的完整性，以确保关键信息的隐私和机密性。
- 奠定坚实的安全基础，包括安全引导管理器和信任根。
- 保护端点到有线或无线网络再到云的通信和连接安全。

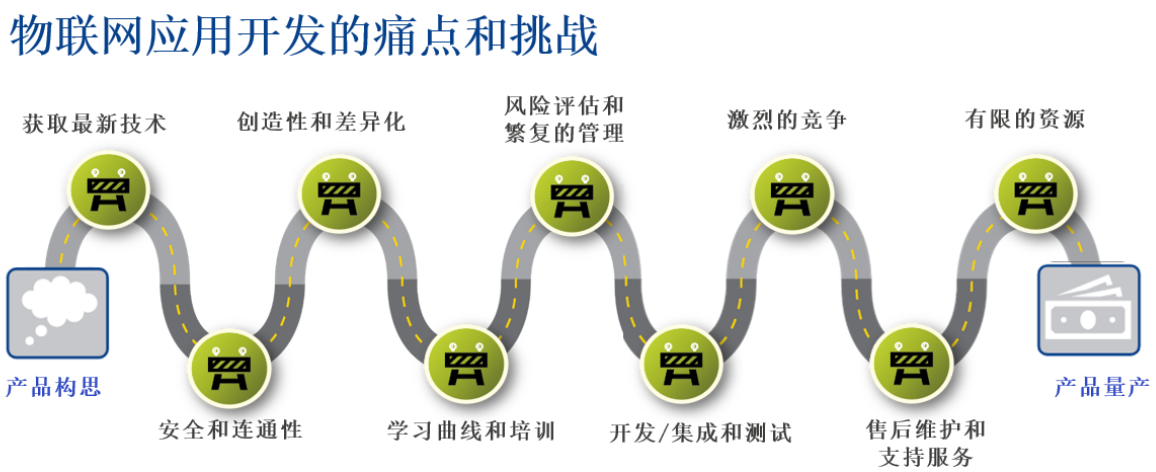


图 1.*物联网应用开发人员必须经历从概念到生产的很长周期，这会影响上市时间，并且增加其他成本*

为了应对这些安全挑战，应用开发人员需要一种基于平台的方法，充分利用最新的硬件和软件技术，实现深入和全面的保护，提供多层次安全保护。

在硬件方面，这个平台包括：

- 提供调试访问保护，避免攻击者将调试接口作为攻击媒介。
- 提供安全和加密引擎，用于加快对称和非对称标准的加密操作，为更快速的 HASH 算法提供硬件支持。
- 生成安全密钥，设备上提供一个安全区域，用于保存这些密钥，确保密钥不会在未加密状态就出现在代码中。每部设备都能够生成和保存自己的密钥，让设备拥有唯一标识，这也是大规模安全配置和部署设备的必备要求。

- 提供安全的存储器访问，保护闪存和 RAM 的指定区域，防止未经授权或意外读写操作。将敏感的代码和数据与不安全的代码和数据隔离，存储在单独的存储域，并采用一次性写入保护存储器防止代码和数据被篡改。

在软件方面，这个平台包括：

- 集成优化的商用级软件，提供经过验证的应用框架和标准 API。
- 与硬件安全和加密功能接口的驱动程序级 API。
- 软件加密算法的功能库，包含更高级别的抽象 API，用于执行微控制器与外部通信设备或网络之间的验证和安全通信，对机密敏感的数据和程序进行加密，以便将其存储在微控制器中。
- 对主要通信协议和传输（例如 TLS、MQTT 和 HTTPS）和云专用协议提供内置支持，让开发人员无需费力地集成底层中间件和网络堆栈，也无需处理这些协议的授权许可和采购成本问题。

嵌入式微控制器软件和硬件平台提供这些集成功能，让物联网开发人员即时受益，这些益处包括：

- 加快开发，因为工程团队能够在 API 级别开始应用软件开发。
- 降低总拥有成本，因为紧密集成的模块提供关键的安全和连接功能，还包括其他外设，能够缩短集成时间，降低物料成本以及专利费和软件费用。
- 降低入门门槛，降低了满足安全和其他各种要求的复杂性。

高度集成的嵌入式微控制器硬件和软件平台对于确保实现物联网设备制造的安全编程至关重要。鉴于全球供应链变得日益复杂，我们现在需要提高安全性，需要付出更多的努力，在制造环境中保持产品的完整性和真实性，确保在生产周期中不受安全威胁。

Renesas Synergy 安全功能

Renesas Synergy 平台是一个经过认证的完整系统解决方案，包括软件、可扩展 MCU 系列和开发工具。借助这个经过验证的全方位平台，工程团队能够在 API 级别开始物联网应用开发，可节省数月的时间和精力。该平台针对 MCU 产品设计进行了优化，为产品创新奠定了坚实的技术基础。

通过集成以下功能，我们将深入分层安全功能内置到 Synergy 平台中。

安全设备标识。通过建立一个强大的设备标识，每个物联网设备都可在连接时被唯一识别并通过验证，确保与其他设备、服务、用户的安全加密通信。强大的设备标识可通过多种方式满足核心物联网安全要求。

- **信任。**当设备连接到网络时，它必须在其他设备、服务和用户之间进行身份验证并建立信任。一旦建立了信任，设备、用户和服务就可以安全通信，交换加密数据和信息。

- **隐私。**随着物联网接入更多的设备，将会生成、收集和共享更多的数据。这些数据可能包括个人信息、敏感信息和财务信息，必须保持私密和安全 – 它们通常处于法规监管之下。设备标识可确保在物联网设备相互连接时进行身份验证和识别。

- **完整性。**设备完整性涵盖物联网生态系统中的设备，以及在其内部传输的数据。设备的完整性首先从证明其身份开始。凭借强大的唯一设备标识，可以确保设备是合法的，从而减少仿冒产品，保护公司品牌。数据完整性是一个容易忽视的安全要求，但互联设备和系统要依赖于所传输信息的真实性和可靠性。

Synergy 平台提供多个密钥生成选项，包括使用平台的安全加密引擎 (SCE) 模块来生成基于硬件的唯一设备标识，进而可以使用安全存储器保护单元 (MPU) 和闪存访问窗口 (FAW)，将该标识安全地存储在设备的内部闪存中。Synergy SCE 模块可以添加到设计中，并针对目标应用进行正确配置。

创建设备标识的第一步是生成密钥。这些密钥可在 Synergy MCU 内部生成，也可在外部的安全工具中生成并注入 Synergy 设备。一旦生成和注入了设备密钥，名为证书颁发机构 (CA) 的企业将颁发数字证书。CA 可能是公共的（位于云中），也可能是私有的（位于本地，通常在安全服务器上托管）。一旦在 Synergy 设备上创建了设备标识并进行了编程，就必须安全地存储该标识，以防被盗或损坏。我们可以使用安全 MPU 和 FAW 功能，在代码闪存和 SRAM 中配置四个安全区域，来实现这个目标。只有“安全代码”才能访问这些区域。我们使用 FAW 寄存器来设置可擦除和编程的代码闪存地址范围。如果地址超出了该范围，我们就说它位于闪存访问窗口之外，一旦编程即无法再修改。我们利用此功能来防止设备标识（密钥和证书）被擦除或重新编程。

这个安全代码区域还包含 API 函数，只有经过授权，才能使用安全数据区域。在 Synergy MCU 上运行的任何非安全代码都不能访问或修改这个部分。由于安全 MPU 设置是在提取重置向量之前读取和应用的，因此它也在执行任何代码之前应用。在离开安全编程中心之前，使用 FAW 功能来锁定 MPU 设置（使用可一次性编程的 FPSR 位），以防止这些设置被修改。

Synergy 器件提供的受保护存储器功能可用于存储安全引导代码和设备证书/密钥，以及对设备标识应用非常重要的其他敏感数据。

保护静态数据安全

随着物联网和云连接的快速发展，数字数据安全性已经成为保护商业机密和个人隐私的首要任务。静态数据是未在设备间或网络间传输的数据。在嵌入式系统中，安全数据可以存储在易失性数据存储器（MCU 的内部 SRAM 或外部 SDRAM）或非易失性数据存储器（例如 MCU 的内部闪存存储、外部 QSPI 存储器和外部 EEPROM 存储器）中。

Synergy MCU 提供数据访问控制、身份验证方案以及 CPU 和总线主控单元对静态安全数据的读/写和一次性写入访问保护。此外，Synergy MCU 还提供安全功能，可禁止通过非安全软件访问对某些安全相关外设进行控制。

数据访问控制。随着我们对设备连接的需求增加，以及嵌入式系统日益复杂，导致更多潜在的攻击面暴露出来。控制对安全数据的访问，可以有效地减小攻击面，从而提高系统安全性。

Renesas Synergy 平台提供以下数据访问控制：

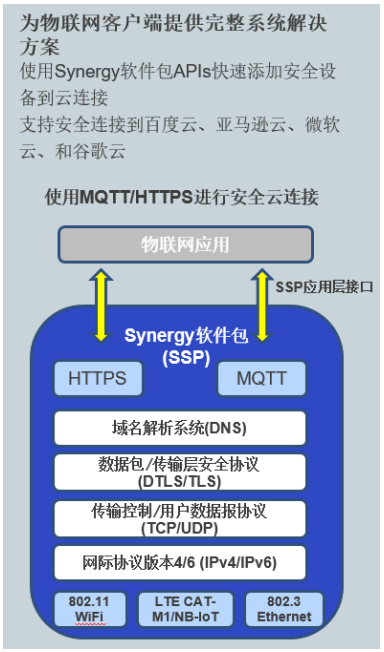
- **读保护。**可以为闪存和 SRAM 中的敏感数据和代码设置读保护属性，确保只有授予读取权限的软件才能访问它们。安全 MPU 还能够建立提供读保护的敏感区域。
- **写保护。**保护敏感数据以防止恶意修改或擦除是非常重要的。可以使用 Synergy 器件中的存储器选项配置设备，为易失性和非易失性数据提供写保护，防止未经授权的修改。
- **读/写保护。**读/写保护可减小恶意软件和 IP 盗窃的攻击面。对于内部闪存数据，Synergy 器件可通过两种方式提供读/写保护：
    - Synergy Security MPU 可以禁用非安全软件对安全 MPU 闪存和 SRAM 区域的读写访问，或者
    - 当安全 MPU 和 FAW 结合使用时，闪存中的敏感数据可以获得读写保护，禁止来自安全和非安全软件的读写操作。
- **一次性写入保护。**在某些应用中，在设备的生命周期内，需要保护静态敏感数据，禁止对其访问或进行更改。例如，安全引导加载程序在产品的生命周期内不得改变。对于数据存储在内部闪存的应用，则可对 FAW 设置进行编程，以提供一次性写入保护。
- **一次性写入和读取保护。**受一次性写入保护的数据可以选择进行读保护。处理敏感数据时，可为受一次性写入保护的数据提供读保护，以确保只有安全软件才能读取数据内容。

安全云连接

物联网采用了一系列技术，将事物和用户中以及事物和用户之间的多种新型通信方式通过智能手段融合在一起。设备利用传感器连接到网络，提供从环境中收集的信息，或者允许其他系统通过致动器执行相应操作。在这个过程中，物联网设备会产生大量数据，而云计算则能够让数据传输到预期目的地。

Synergy 平台为 百度云、亚马逊云服务(AWS)、谷歌云 和 微软云(Azure) 等领先的云环境提供安全的内置连接。Synergy MCU 使用 SSP 的 MQTT 和 TLS 模块提供云连接支持。

MQTT 协议。MQTT 全称是“消息队列遥测传输”。MQTT 是一种轻量级的客户端服务器发布-订阅消息传输协议，具有开放和易用的特点。MQTT 的适用于受限器件，例如低带宽、高延迟或不可靠的网络。这些特征使得 MQTT 非常适合在受限环境下使用，例如机器到机器 (M2M) 和物联网环境中的通信，因为这些通信要求很简短的代码，或者网络带宽非常宝贵。



TLS 协议。传输层安全 (TLS) 协议及其前一代的安全套接字层 (SSL) 协议都是在计算机网络上提供安全通信的加密协议。TLS/SSL 协议在两个通信应用之间提供私密性和可靠性。它具有以下基本特性：

- **加密：**对相互通信的应用之间交换的消息进行加密，以确保连接是私密的。采用 AES 等对称加密机制实现数据加密。
- **验证：**这种机制使用证书来验证对方的身份。
- **完整性：**这种机制可以检测消息是否遭到篡改和伪造，从而确保连接是可靠的。消息验证代码 (MAC)，例如安全哈希算法 (SHA)，可以确保消息完整性。

安全引导管理器

Synergy 安全引导管理器提供支持安全和灵活可调的生产。这是通过安全的固件闪存编程解决方案实现的，它让开发人员能够安全可靠地将授权固件编程到远程制造设施现场的 Synergy MCU 闪存中，同时保护固件，防止它被修改、盗用或安装在克隆硬件上。

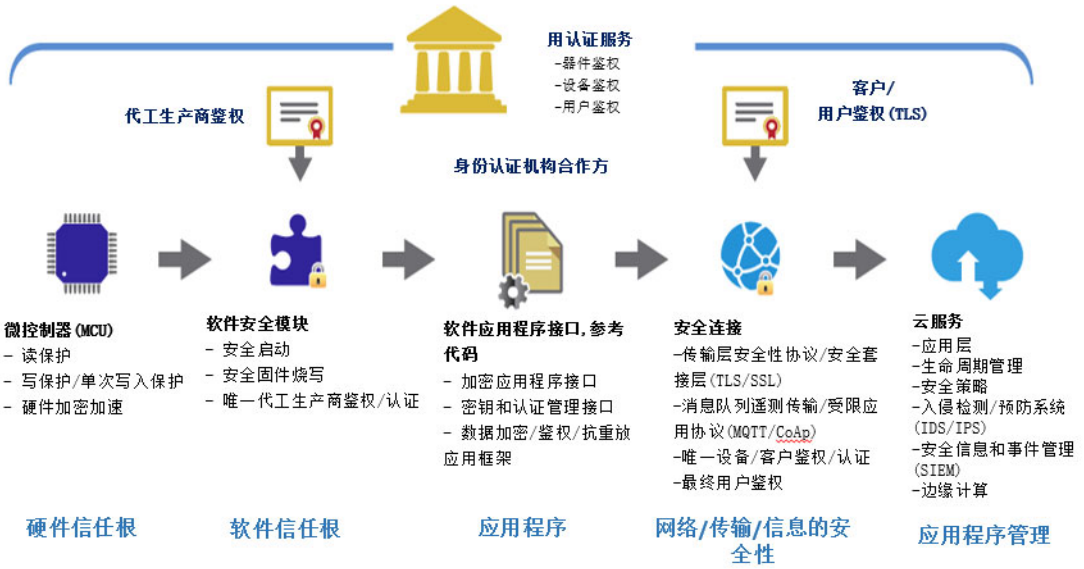


图 2.Renesas 在产品生命周期内提供信任根保护。

Synergy MCU 和 Synergy 安全引导管理器结合使用，通过唯一标识、硬件保护密钥、安全引导加载程序、安全闪存更新模块以及与 MCU 硬件接口的加密 API，提供强大的信任根保护。安全引导管理器包括以下功能：

- 控制（数字签名）固件的工具。
- 下载引导加载程序、证书和密钥。
- 将用户应用固件下载到授权 MCU。

首先，在安全编程中心在每个目标 Synergy MCU 上安装唯一信任根。信任根包括 Renesas Synergy 引导管理器，以及由固件控制工具生成的唯一“信任根”。在后面的步骤中，这个控制工具将对授权固件进行签名和加密，因为安全引导加载程序仅加载已由控制工具签名的固件。信任根通过安全连接预加载到编程器系统，该系统专为大批量制造和配置而设计，可以安全地存储数据，并严格控制数据的使用方式。

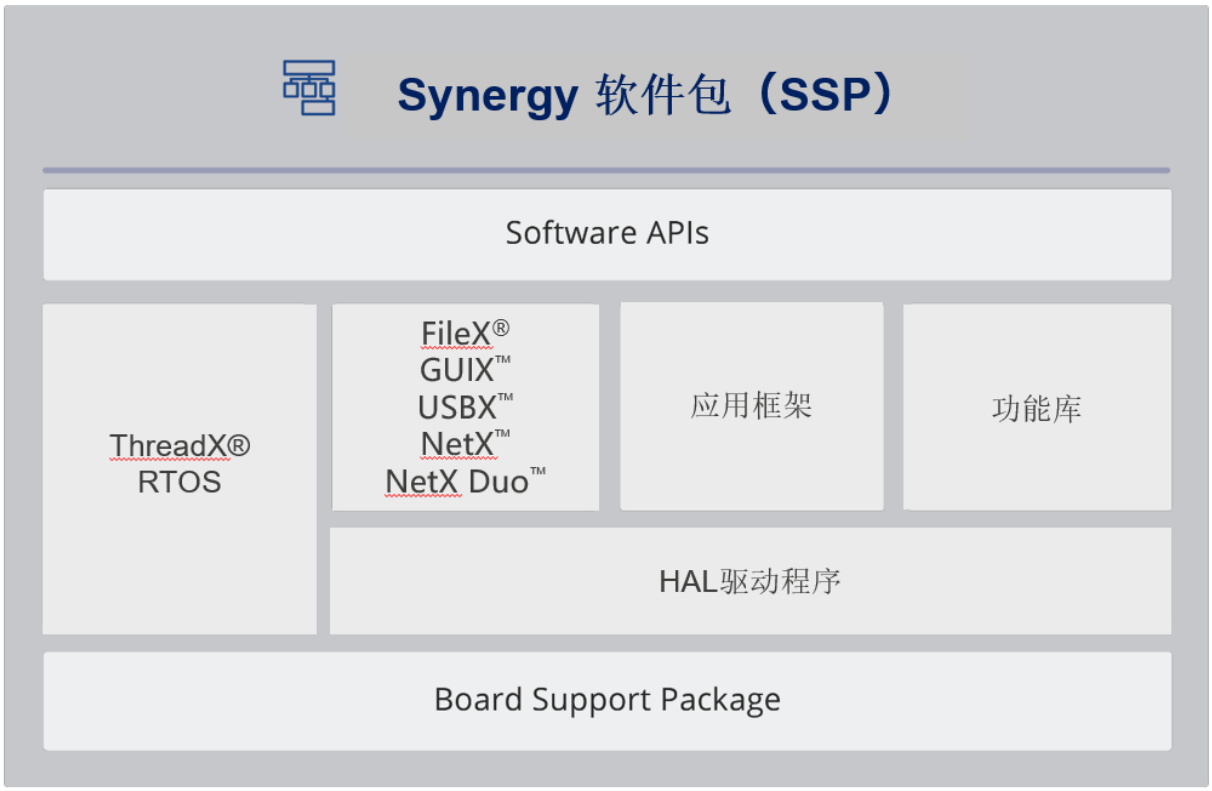
授权 MCU 加载到编程系统，信任根下载到各个 MCU，密钥为每个器件提供安全唯一标识。接下来安装之前使用控制工具进行数字签名并加密的授权固件。编程系统将固件下载到 MCU，先前安装的信任根将对固件进行验证和解密，并将其写入闪存。这个过程结束时，为安全引导加载程序设置的闪存访问窗口将被锁定，不允许修改，从而确保它作为不得改变的信任根，仅引导受信任的固件。

然后将编程的 Synergy MCU 发往 OEM 或合同制造厂，在这些工厂将 MCU 贴装到电路板上，最后将电路板安装到最终产品或应用中。一旦进入现场，授权的固件即可安全更新到 MCU 的闪存中，利用片上的信任根对固件进行验证和解密，然后进行闪存编程 – 所有这些都通过安全云基础设施进行安全的配置。

Synergy 软件包

Synergy 软件包 (SSP) 提供针对 Synergy 平台开发和优化、经过商业认证合格的软件。SSP 包括一系列经过验证的框架和标准 API，将顶级实时操作系统 (RTOS)、中间件套件、多种算法函数库，以及底层驱动程序紧密集成在一起，帮助简化您遇到的复杂功能，同时开发互联嵌入式系统。其分层架构让开发人员能够使用通用 API 来编写应用，或者根据需要直接连接至 MCU 器件的驱动层。

附加的软件组件可为软件提供补充，包括专用功能、中间件包和应用框架。Synergy 平台还包括两个软件开发环境：e² studio 和 IAR Embedded Workbench™ for Renesas Synergy。软件和工具包括在 Synergy 平台中，不收取专利费或软件采购费用。



为了确保做好生产准备，瑞萨电子依据涵盖整个软件开发生命周期的国际标准 ISO/IEC/IEEE 12207 来开发 SSP。SSP 的每个部分都根据这些要求来定制，并根据这些要求进行测试。

Renesas S5D3 微控制器简介

S5D3 MCU群组

Renesas S5D3 是 Synergy 系列微控制器的最新成员，可作为安全可靠、高性价比的物联网系统开发平台。S5D3 MCU 基于高性能 Cortex M4F 内核，针对内部存储器进行了优化，嵌入式闪存与 SRAM 的比率为 2：1，并且实现了外设高度集成。S5D3 基于高效的 40nm 工艺制程构建，Synergy 软件包为其提供全面支持，同时提供强大的设计支持和器件评估环境，包括目标板套件和两个集成开发环境 (IDE)。S5D3 提供了一个通用规格，可为工业和楼宇自动化等领域的物联网应用提供先进的安全和端点管理。

S5D3 属于 S5 MCU 大系列，其设计实现了高性能和高集成度，还提供广泛的连接、图形引擎、多个高精度数据采集模拟接口。S5 系列 MCU 还具有增强的安全和加密功能，为高级加密算法提供硬件加速。S5 系列极具可扩展性和引脚兼容性，还提供硬件套件，以加速产品开发。

S5D3 为 S5 MCU 系列增加了一个新的极具性价比的产品层次。通用型 S5D3 适合需要高性能和强大安全性，但不需要片上图形加速或以太网连接等功能的应用。40nm 工艺制程可提高 CPU 工

作能效，非常适合需要持续收集监控数据的物联网应用。S5D3 针对内存进行了优化，提供 512 KB 代码闪存、8 KB 数据闪存和 256 KB 的 SRAM。它不仅工作非常高效，其价位也颇具吸引力，因而成为一款非常高效的 MCU 产品，可为物联网系统中的端点设备提供先进的可扩展安全管理。S5D3 面向工业和楼宇自动化市场的各种应用，可用于系统和机械控制。它还适用于智能仪表中的网络控制，以及办公自动化解决方案中的系统控制单元。

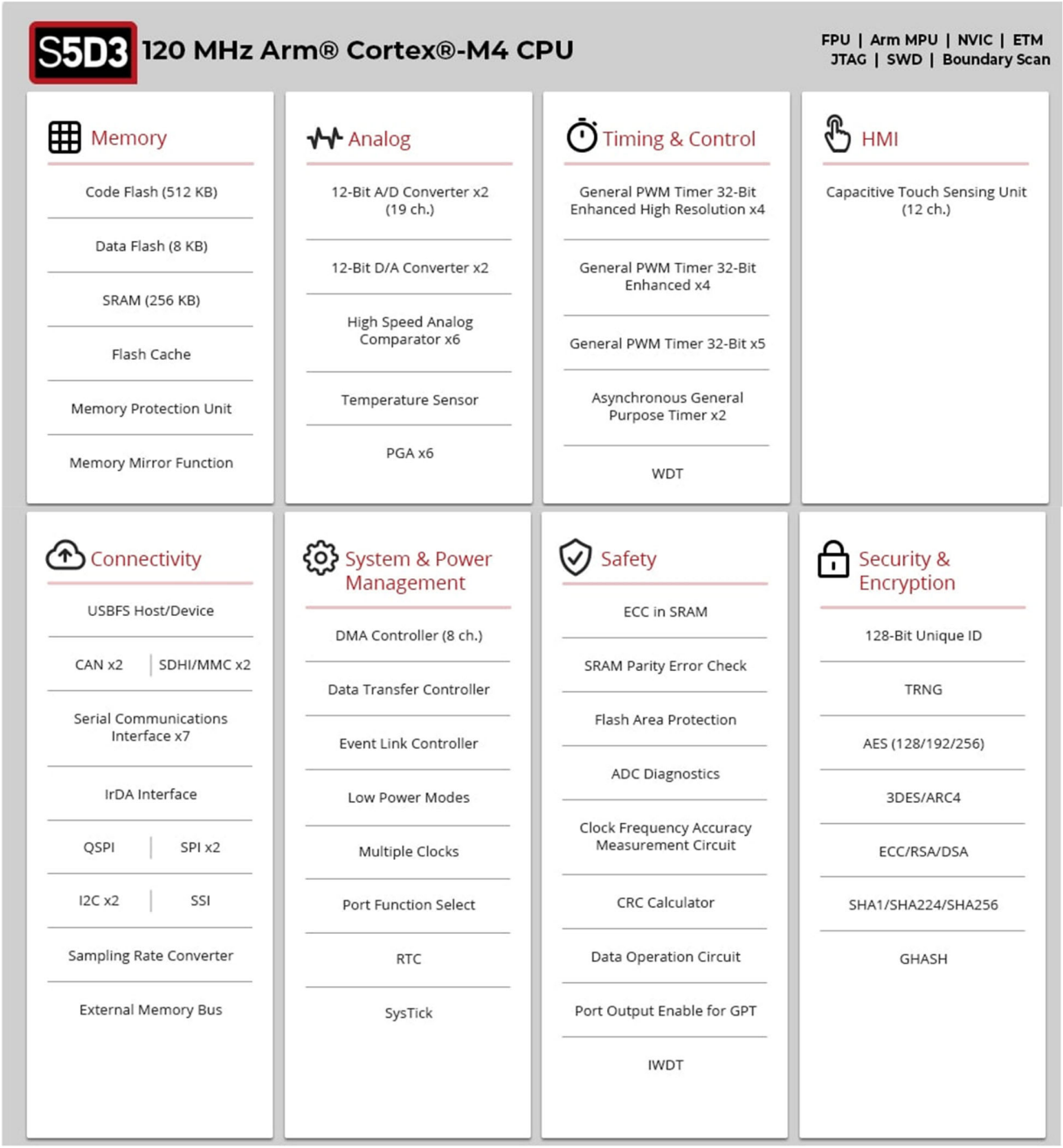


图 3：S5D3 MCU 组系统框图

S5D3 的主要优势

提供集成安全功能，因而无需外部安全功能。S5D3 通过将多种先进功能集成到 MCU 中提供安全信任根。

S5D3 的集成加密引擎，即安全加密引擎 (SCE7)，能够提供远超同类 MCU 中其他解决方案的安全保护功能。SCE7 是 MCU 上的独立子系统，由专用控制逻辑电路管理和保护。封装的密钥可防止敏感信息泄漏：每个 MCU 拥有唯一密钥封装可确保密钥隔离，加密引擎为每个 MCU 提供唯一加密密钥，因而密钥只能在特定 MCU 的加密模块内访问。

SCE7 还内置硬件加速器，包括 ECC、RSA、AES、3DES、SHA 和 TRNG，具有密钥生成功能。安全模块还在片上闪存中提供受写入保护的引导代码和数据（根密钥、配置）。这可以防止代码被更改、复制或反向工程。安全 MPU 会建立安全存储器，使其在硬件级别与非安全存储器隔离，从而让受信任和不受信任的代码和数据实现隔离。

S5D3 内置大容量嵌入式 RAM，因而适合处理各种通信堆栈。在互联的物联网环境中，具有稳定连接的应用至关重要。要管理产生合理数量的有效载荷的通信堆栈，就需要较大的嵌入式 SRAM，以便提升性能和降低 BOM 成本。S5D3 提供的嵌入式闪存和 SRAM 的比率为 2：1（分别为 512 KB 和 256 KB）。

结论

为物联网应用提供全面深入的安全保护需要高度集成的优化平台，多种功能共同发挥作用，在多个方面提供安全性。Renesas Synergy 平台提供一系列独特的硬件和软件安全功能，这些功能建立在共享信任根的基础上，以满足保护物联网设备和网络安全的要求，最终确保安全；灵活可调的生产以及提供知识产权保护。Renesas S5D3 是 Synergy 的 MCU 系列的最新产品，提供强大的分层安全功能，可以在物联网系统中实现端点设备的先进可扩展安全管理。