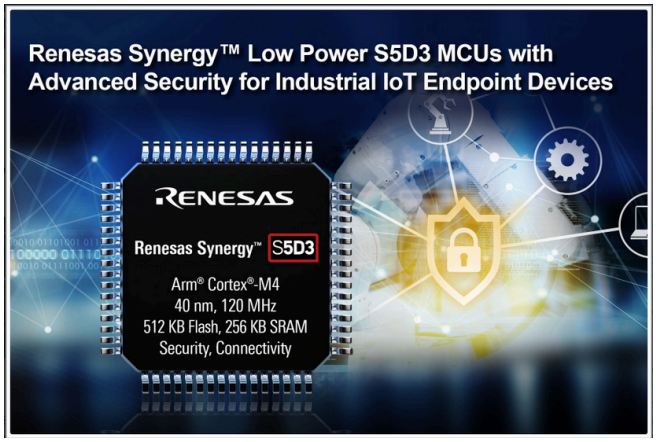
White Paper

How to Manage Thousands of Devices in a Secure, Scalable Way

February 2019

Abstract

Providing comprehensive, in-depth security protection for Internet of Things (IoT) applications in today's connected world brings challenges on multiple levels. The Renesas Synergy Platform provides a unique set of hardware and software security capabilities that combine to meet the requirements of securing IoT devices and networks, including the ability to ensure secure, scalable manufacturing and protection of intellectual property during production at remote locations. The Renesas S5D3 is the latest addition to the Synergy family of microcontrollers (MCUs) that power the Synergy Platform, and provides security protections far above other solutions in this class of device. The general-purpose S5D3 offers highly efficient operation at an attractive price point, making it a very effective MCU to enable advanced scalable security management for endpoint devices in IoT systems.



Security Challenges in the Internet of Things

Not that long ago, application developers didn't have to worry much about securing their products because applications were not connected in the way that they are today. Now, even the most basic items—from light bulbs to children's toys and appliances—are now connected by networks, the Internet or cloud environments in the IoT. Security requirements have advanced greatly from the days of when passwords and firewalls sufficed. Securing IoT applications to protect data and intended functionality from cyber threats is now a primary consideration for developers—not an afterthought—and needs to be built into devices at both the hardware and software levels.

Security standards are constantly evolving, as threats grow more powerful and malicious, and complex applications may require meeting multiple standards, which can inhibit device compatibility and flexibility. In many development scenarios, higher security features also come with higher costs and often higher power consumption, impacting the marketability of the end application.

Thus, applications for the IoT must meet a range of specific challenges, including:

- Protecting intellectual property from such threats as IP theft, product cloning and over-production during manufacturing.
- Defending against exploits that can be used to shut down or damage vital infrastructure or cause injury.

- Protecting data integrity in flight and at rest, to ensure privacy and confidentiality of critical information.
- Creating robust foundations, including a secure boot manager, and a root of trust.
- Securing communications and connections, from end points to wired or wireless networks and to the cloud.

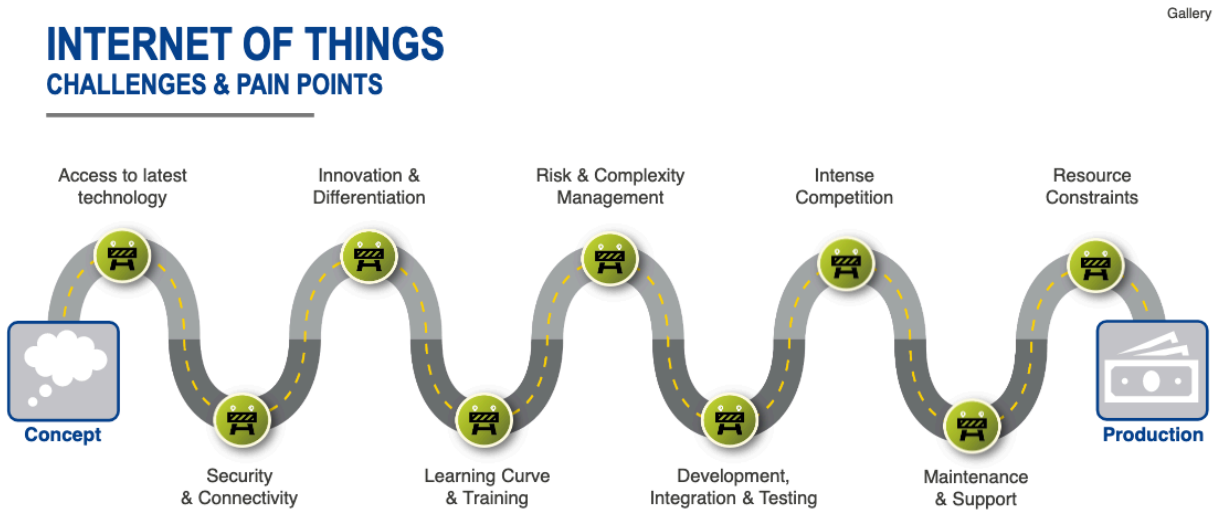


Figure 1. *IoT application developers must follow a long journey from concept to production, impacting time to market and adding other costs*

To meet these security challenges, application developers need a platform-based approach that takes advantage of the latest advances in both hardware and software to implement in-depth, comprehensive protections that offer multiple layers of security.

On the hardware side, this platform includes:

- Protected debugging access, to eliminate debugging interfaces as attack vectors.
- A security and encryption engine, to accelerate encryption operations for both symmetrical and asymmetrical standards, and hardware support for faster HASH algorithms.
- Generation of secured keys, with a security enclave on the device to hold the keys and ensure they aren't exposed to code in their unencrypted state. Each device can generate and hold its own key, enabling the device to have its own unique identity, which is required for the secure provisioning and deployment of devices at scale.
- Secure memory access, which safeguards designated regions of Flash memory and RAM from unauthorized or unintentional read or write attempts. Sensitive code and data should be isolated in a separate memory domain from non-secure code and data, and write-once protected memory safeguards code and data from being changed.

On the software side, this includes:

- Integrated and optimized commercial grade software with proven application frameworks and standard APIs.
- Driver-level APIs that interface with the hardware security and encryption features.

- Functional libraries of software cryptographic algorithms with higher-level abstracted APIs to perform authentication and secure communication between the microcontroller and external communication devices or networks, and to encrypt confidential and sensitive data and program for storage in the microcontroller.

- Built-in support for major communication protocols and transports—such as TLS, MQTT and HTTPS—and cloud-specific protocols, so developers don't need to wrestle with integrating low-level middleware and network stacks, or deal with licensing and costs of these protocols.

An embedded microcontroller software and hardware platform that delivers these integrated functionalities offers immediate benefits to IoT developers, including:

- Accelerated development, as engineering teams can begin application software development at the API level.

- Reduced total cost of ownership, as tightly integrated modules incorporate key security and connectivity features and other peripherals, to reduce integration time, bill of material costs, and royalties and fees for software.

- Lowered barriers to entry, reducing the complexity of meeting security and other evolving requirements.

A highly integrated embedded microcontroller hardware and software platform is also critical for helping ensure more secure programming for manufacturing of IoT devices. Given the increased complexity of global supply chains, extra security and diligence is now needed to ensure that the integrity and authenticity of products are maintained in the manufacturing environment and not compromised during the production cycle.

Renesas Synergy Security Features

The Renesas Synergy Platform is a complete, qualified system solution that includes software, a scalable family of MCUs, and development tools. With this comprehensive, proven platform, engineering teams can begin IoT application development at the API level, saving them months of time and effort. It also ensures that their product innovations rest on a solid, robust technology foundation optimized for MCU-based product designs.

In-depth, layered security is built into the Synergy platform through integration of the following features.

Secure Device Identity. With the establishment of a strong device identity, each IoT device can be uniquely identified and authenticated when it is connected to ensure secure and encrypted communication between other devices, services and users. Strong device identity addresses core IoT security requirements in a number of ways.

- **Trust.** When a device connects to the network, it must authenticate and establish trust between other devices, services and users. Once trust is established, devices, users and services can securely communicate and exchange encrypted data and information.

- **Privacy.** As more IoT devices connect, more data is generated, collected, and shared. This data can include personal, sensitive and financial information that must be kept private and secured – often under regulatory compliance. Device identity can ensure authentication and identification when the IoT devices are connected to one another.

- **Integrity.** Device integrity applies to both the devices and data being transmitted within the IoT ecosystem. The integrity of a device starts with proving it is what it says it is. With a strong unique device identity, devices are ensured as legitimate – reducing counterfeit products and protecting a company's brand. Data integrity is an often-overlooked requirement, but connected devices and systems rely on the authenticity and reliability of the information being transmitted.

The Synergy platform provides multiple key generation options including using the platform's Secure Crypto Engine (SCE) module to generate a unique hardware-based device identity that can be securely stored in the device's

internal flash using security memory protection units (MPUs) and Flash access windows (FAWs). The Synergy SCE modules can be added to designs and configured correctly for target applications.

The first step in creating a device identity is key generation. The keys can be either generated inside the Synergy MCU or they can be generated externally in a secure facility and injected into the Synergy device. Once the device keys are generated or injected, an entity called the Certificate Authority (CA) issues digital certificates. A CA can be either public (located in the Cloud) or private (located on-premises and typically hosted on a secure server). Once the device identity is created and programmed on the Synergy device, it must be securely stored to prevent it from being stolen or corrupted. This is achieved by using the Security MPU and FAW features to configure four secure regions in code Flash and SRAM. These regions can only be accessed by "secure code." The FAW registers are used to set the code Flash address range, which can be erased and programmed. The addresses that are outside this range, referred to as outside the Flash Access Window, cannot be modified once programmed. This feature is used to prevent the device identity (keys and certification) from being erased or reprogrammed.

The secure code region also contains API functions that are only authorized to work on the secure data region. This section cannot be accessed or modified by any un-secure code running on the Synergy MCU. The Security MPU settings are read and applied before the reset vector is fetched, and therefore apply before any code is executed. The Security MPU settings are locked using the FAW feature (using a one-time programmable FPSR bit) before leaving the secure programming center to prevent them from being modified.

Protected memory features offered by Synergy devices can be used for storing the secure boot code and device certificate/keys amongst other sensitive data which are vital for device identity application.

Secure Data at Rest

With the rapid growth of IoT and cloud connectivity, digital data security has become a top priority when protecting trade secrets and personal privacy. Data at Rest is data that is not actively moving from device to device or network to network. In an embedded system, secure data can reside in volatile data storage (an MCU's internal SRAM or external SDRAM) or non-volatile data storage (such as an MCU's internal flash storage, external QSPI storage, and external EEPROM storage.)

Synergy MCUs offer data access controls, authentication schemes, and read/write and write-once access protection from CPU and bus masters for secure Data at Rest designs. In addition, Synergy MCUs provide security functions that disable control of certain security-related peripherals from non-secure software access.

Data Access Control. Increased demands for device connectivity as well as greater complexity in embedded systems result in more potential attack surfaces exposed. Controlled access to the secure data effectively reduces the attack surface, thus increasing system security.

The Renesas Synergy platform provides the following data access controls:

- **Read Protection.** Sensitive data and code residing in flash and SRAM can have read protection properties set to ensure that only software granted with read permission can access them. The Security MPU has the capability to establish sensitive regions with read protection.

- **Write Protection.** It is important to protect sensitive data from being maliciously modified or erased. Volatile and non-volatile data can be write-protected to avoid unauthorized modifications by using the memory-options setting in a Synergy device.

- **Read/Write Protection.** Read/Write protection reduces the attack surface from malware and IP theft. For internal flash data, there are two ways Synergy devices can provide read/write protection:

    - The Synergy Security MPU can disable read and write access to the security MPU flash and SRAM regions from non-secure software, or

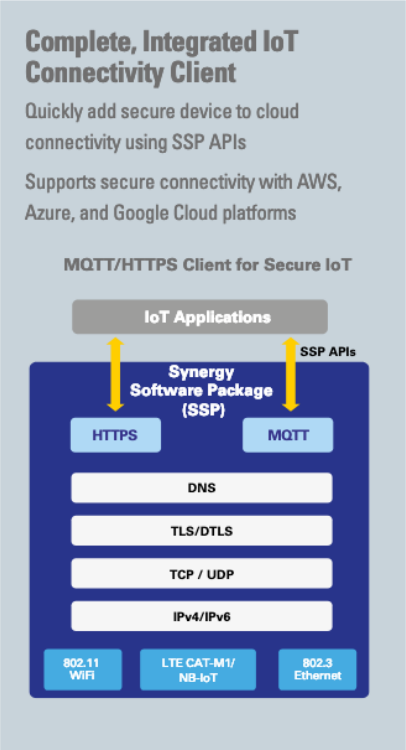
    - When the Security MPU and FAW are used together, the sensitive data in Flash can be read- and write-protected from both secure and non-secure software.

- **Write-Once Protection.** In some use cases, sensitive Data at Rest needs to be protected from access or alteration for the lifetime of the device. For example, a secure boot loader must be immutable for the lifetime of the product. For use cases where the data resides on internal flash, FAW settings can be programmed to provide write-once protection.

- **Write-Once and Read Protection.** Write-once protected data can be optionally read protected. When handling sensitive data, read protection can be provided to the write-once protected flash data to ensure that only secure software can read the contents.

Secure Cloud Connectivity

The IoT comprises a sprawling set of technologies that intelligently link together multiple new forms of communication between and among things and people. Using sensors, devices connect to the network to provide the information they gather from the environment or allow other systems to reach out and act on the world through actuators. In the process, IoT devices generate massive amounts of data, and cloud computing provides a pathway to enable data to travel to its intended destination.



The Synergy platform provides secure, built-in connectivity to leading cloud environments, including Amazon Web Services (AWS), Google Cloud, and Microsoft Azure. Synergy MCUs deliver support for cloud connectivity using the SSP's MQTT and TLS modules.

MQTT Protocol. MQTT stands for Message Queuing Telemetry Transport. MQTT is a Client Server publish-subscribe messaging transport protocol that is an extremely lightweight, open and simple to use. MQTT is designed for constrained devices, as well as low-bandwidth, high-latency or unreliable networks. These characteristics make MQTT ideal for use in situations that include constrained environments, such as communication in Machine to Machine (M2M) and IoT contexts, where a small code footprint is required, and/or network bandwidth is at a premium.

TLS Protocol. Transport Layer Security (TLS) protocol and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide communications security over a computer network. The TLS/SSL protocol provides privacy and reliability between two communicating applications. It has the following basic properties:

- **Encryption:** The messages exchanged between communicating applications are encrypted to ensure that the connection is private. Symmetric cryptography mechanism such as AES is used for data encryption.

- **Authentication:** A mechanism to verify the peer's identity using certificates.

- **Integrity:** A mechanism to detect message tampering and forgery ensures that a connection is reliable. The Message Authentication Code (MAC), such as Secure Hash Algorithm (SHA), ensures message integrity.

Secure Boot Manager

The Synergy Secure Boot Manager provides the functionalities to enable secure and scalable manufacturing. This is achieved via a secure firmware flash programming solution that enables developers to reliably and securely program authorized firmware into the flash memory of Synergy MCUs in remote manufacturing facilities and in the field, while protecting the firmware from being modified, pirated or installed on cloned hardware.

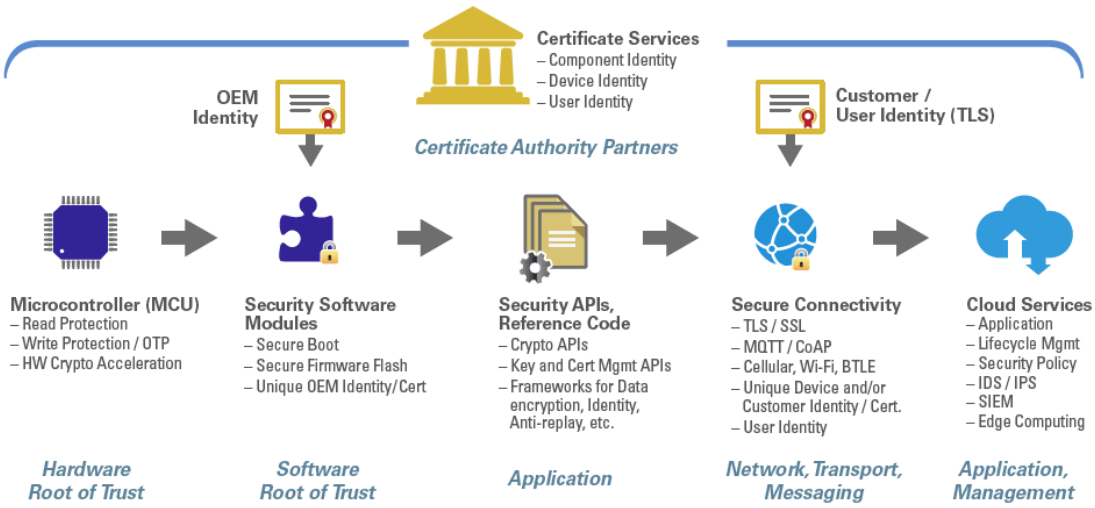


Figure 2. *Renesas provides root-of-trust protection across the product lifecycle.*

The combination of Synergy MCUs and Synergy's Secure Boot Manager delivers a strong root-of-trust through a unique identity, hardware protected keys, a secure boot loader, a secure flash update module, and cryptographic APIs that interface with the MCU hardware. The Secure Boot Manager includes:

- Tools for Mastering (digitally signing) firmware.
- Downloading the Boot Loader, certificates, and keys.
- Flashing the user application firmware onto the authorized MCUs.

The process begins by installing a unique root-of-trust on each destination Synergy MCU in a secure programming center. The root of trust consists of the Renesas Synergy Boot Manager plus a unique "root of trust" generated by a firmware Mastering Tool. In a later step this Mastering Tool will sign and encrypt the authorized firmware, as the Secure Boot Loader will only load firmware that has been signed by the Mastering Tool. The root-of-trust is pre-loaded through a secure connection into a programmer system designed for high volume manufacturing and provisioning of chips, which stores the data securely, and maintains tight control on how the data is used.

Authorized MCUs are loaded onto the programming system, and the root of trust is flashed onto individual MCUs along with keys that give each of the devices a secure, unique identity. The next stage in the chain is installing the authorized firmware that has previously been digitally signed and encrypted using the Mastering Tool. The programming system will flash the firmware to the MCUs and the root-of-trust previously installed will validate, decrypt and write the firmware to flash memory. At the end of the process, the flash access window set to the Secure Boot Loader is locked from being modified – ensuring that it will function as an immutable root-of-trust, booting only trusted firmware.

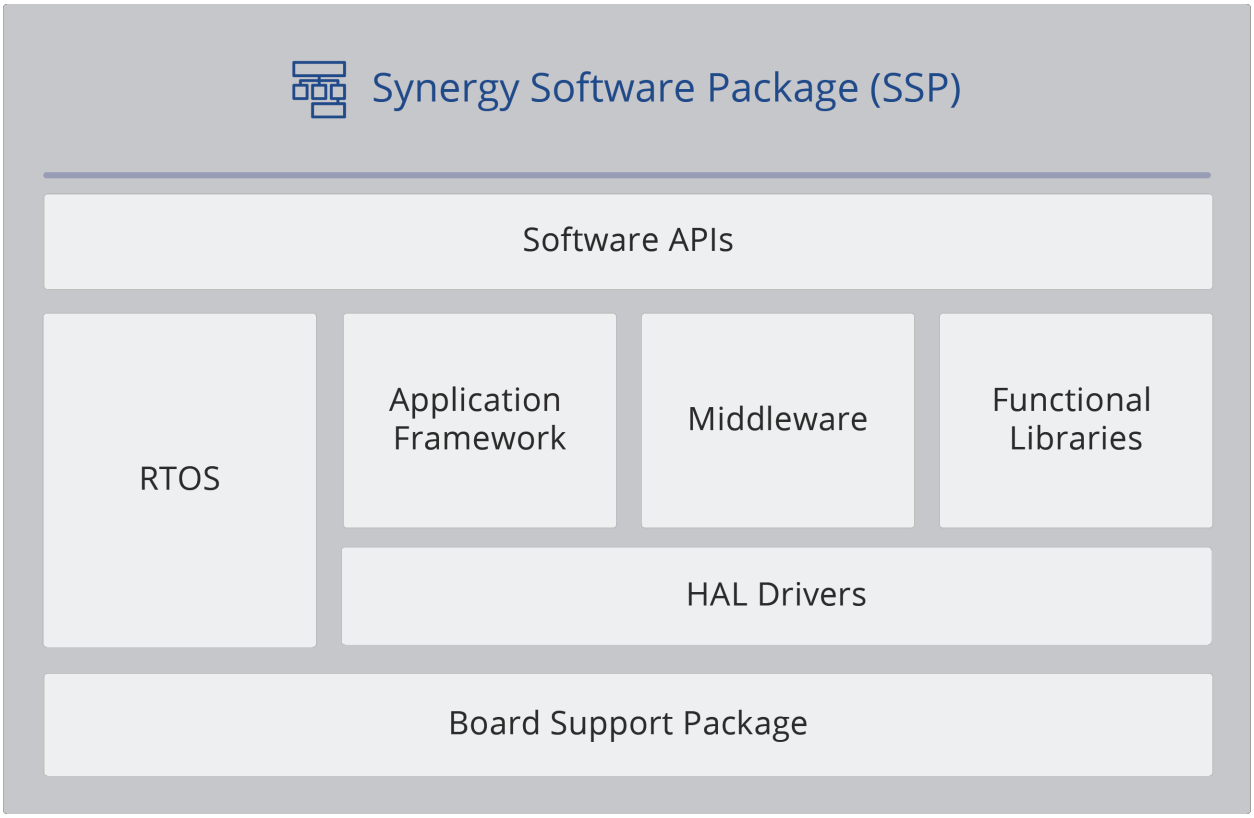
The programmed Synergy MCUs can then be shipped to an OEM or contract manufacturing facility, where the MCUs are mounted onto circuit boards to be installed into the final product or application. Once in the field, authorized firmware can be securely updated to the MCUs' flash memory, with the on-chip root-of-trust being used to validate and decrypt the firmware before flash programming – all securely provisioned via secure cloud infrastructure.

Synergy Software Package

The Synergy Software Package (SSP) provides commercially qualified software developed and optimized for the Synergy platform. The SSP includes a proven series of frameworks and standard APIs that tightly integrate a premium real-time operating system (RTOS), a suite of middleware, a variety of libraries, and low-level drivers to simplify complex functions encountered while developing connected embedded systems. A layered architecture

enables developers to write applications using common APIs or by directly connecting to the MCU device driver level as needed.

Add-on software components complement the software with specialty functions, middleware packages and application frameworks. The Synergy platform also includes two software development environments: e^2 studio and IAR Embedded Workbench™ for Renesas Synergy. Software and tools are included in the Synergy Platform free of fees or royalties.



To ensure production readiness, Renesas developed the SSP according to the international standard ISO/IEC/IEEE 12207 that covers the entire Software Development Life Cycle. Every element of the SSP is defined by and tested to meet these requirements.

Meet the Renesas S5D3 Microcontroller

The Renesas S5D3 is the latest addition to the Synergy family of microcontrollers, and serves as a secure, cost-optimized platform for IoT system development. The S5D3 MCU is based on a high-performance Cortex M4F core and is optimized for memory, with an embedded Flash versus SRAM ratio of 2 to 1, and high peripheral integration. The S5D3 is built on a highly efficient 40nm process, and is fully supported by the Synergy Software Package, with a robust design support and device evaluation environment, including target board kits and two Integrated Development Environments (IDEs). The S5D3 offers a general-purpose specification that provides advanced security and endpoint management for IoT applications in such fields as industrial and building automation.

The S5D3 is part of the larger S5 MCU series, designed for high performance and tight integration, with extensive connectivity, a graphics engine, and multiple high precision data acquisition analog interfaces. The S5 series MCUs also feature enhanced security and safety features, with hardware acceleration for advanced encryption algorithms. The S5 series are highly scalable and pin-compatible and offer hardware kits to accelerate product development.

The S5D3 adds a new, cost-optimized tier to the S5 MCU family. The general-purpose S5D3 is designed for applications that require high performance and robust security but that don't require such features as on-chip graphic acceleration or Ethernet connectivity. The 40nm process allows greater power efficiency for CPU operation, and is a good fit for IoT applications where monitoring data is continually collected. The S5D3 is optimized for memory, with 512 KB of code Flash, 8 KB of data Flash and 256 KB of SRAM. It offers highly efficient operation at a very attractive price point, making it a very effective MCU for advanced scalable security management for endpoint devices in IoT systems. The S5D3 is targeted for applications in the industrial and building automation market, where it can be used for system and mechanical control. It is also suitable as a network control in Smart Meter applications, and as a system control unit in office automation solutions.

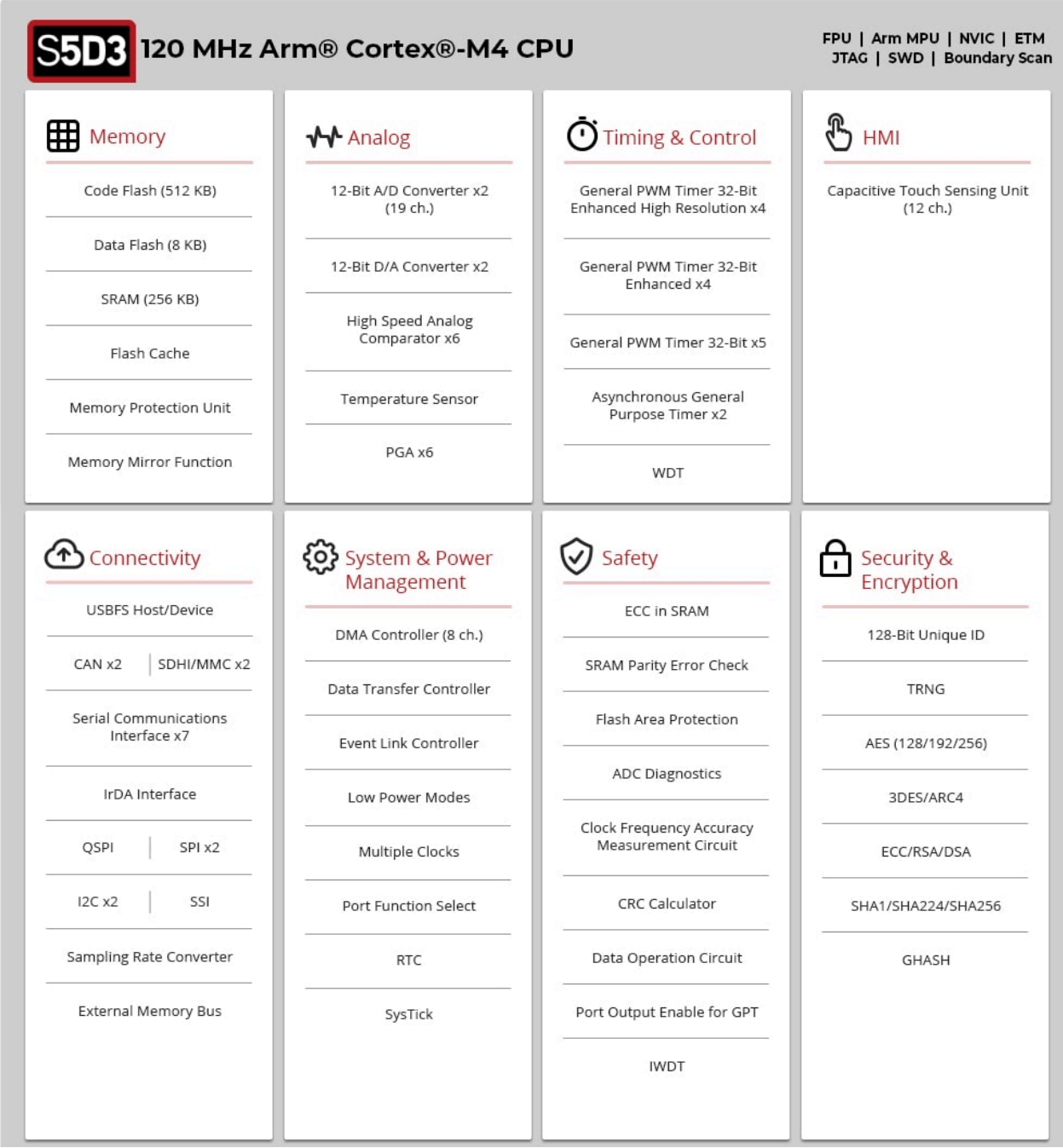


Figure 3: *S5D3 MCU Group Block Diagram*

S5D3 Key Benefits

Integrated security features that eliminate the need for external security functions. The S5D3 offers a security root of trust through the combination of multiple advanced features integrated onto the MCU.

The S5D3's integrated cryptographic engine, the Secure Cryptographic Engine (SCE7), provides security protections far above other solutions in this class of MCU. The SCE7 is an independent subsystem on the MCU, managed and protected by dedicated control logic. Wrapped keys prevent exposure of sensitive information: key isolation is ensured by MCU-unique key wrapping, which encrypts keys uniquely for each MCU so keys are only accessible within the crypto module on a specific MCU.

The SCE7 also has built-in hardware accelerators, including ECC, RSA, AES, 3DES, SHA and TRNG, with key generation capability. The security module also offers write-protected boot code and data (root keys, configuration) with on chip Flash. This protects code against being changed, copied or reverse engineered. The Security MPU establishes secure memory that is isolated from non-secure memory at the hardware level, and enables separation of trusted and untrusted code and data.

Large amounts of embedded RAM already built in, making the S5D3 suitable for handling a variety of communication stacks. An application with robust connectivity is critical in a connected IoT environment. To manage communications stacks that deliver a reasonable amount of payload requires a large embedded SRAM to bring performance up and BOM cost down. The S5D3 offers an unusual embedded Flash versus SRAM ratio of 2 to 1, (512 KB vs. 256 KB).

Conclusion

Delivering comprehensive, in-depth security protection for IoT applications requires a highly integrated, optimized platform of functionalities that work together to provide security multiple levels. The Renesas Synergy Platform provides a unique set of hardware and software security capabilities that build on a shared root of trust to meet the requirements of securing IoT devices and networks, culminating in the ability to ensure secure, scalable manufacturing and protection of intellectual property. The Renesas S5D3 is the latest addition to the Synergy family of MCUs, with robust, layered security features ready to enable advanced scalable security management for endpoint devices in IoT systems.