白皮書

# 如何安全地管理數千個設備並確保其可擴展性

2019 年 2 月

## 摘要

在現今的連網世界中，若要為物聯網 (IoT) 應用提供全面、深入的安全保護，可能會在許多層面遭遇困難。Renesas Synergy 平台提供一套獨特的硬體和軟體安全功能，可以滿足保護物聯網裝置和網路的需求——包括在生產期間以遠端方式確保安全、可靈活調整的生產和智慧財產權保護。瑞薩電子 S5D3 是 Synergy 系列微控制器 (MCU) 的最新成員，不僅使得 Synergy 平台更為強大，其安全防護功能更遠遠高於此類裝置的其他解決方案。通用型 S5D3 以極具吸引力的價格展現優異效能，是一款相當有效率的 MCU，能夠為物聯網系統中的端點裝置實現先進並且可擴展的安全管理。


## 物聯網的安全挑戰

不久之前，應用程式開發人員還不必費心保護自己的產品，因為當時的應用程式並不像現在一樣四處連結。如今，即使是最基本的物品 (如燈泡、兒童玩具、家用電器等)，都可以透過物聯網中的網路、網際網路或雲端環境相互連接。相較於以往只需密碼和防火牆就足以因應的年代，現代的安全需求大幅提升。在現代，保護物聯網應用程式，以防護資料和預期功能不受網路威脅的攻擊，已成為開發人員的主要考量因素，而非留待事後才設法解決，而且還需將安全機制建構於裝置中的硬體和軟體層級。

隨著威脅變得愈來愈強大且危險，安全標準也在不斷發展，複雜的應用可能需要滿足多種標準，而這將不利於裝置的相容性和彈性。在許多開發方案中，愈高的安全性功能也意味著愈高的成本和功耗，從而影響最終應用成品的銷售成績。

因此，物聯網應用程式必須滿足一連串特定挑戰，包括：

- 保護智慧財產免於遭受 IP 竊取、產品仿冒、製造生產過剩等威脅。
- 防範會關閉或損壞重要基礎架構，或甚至能造成人身傷害的攻擊。
- 保護動態和靜態資料的完整性，確保關鍵資訊的隱私和機密性。
- 打造穩健的基礎，包括安全啟動管理器和信任根。
- 保護通訊和連線，從端點到有線或無線網路以及到雲端。

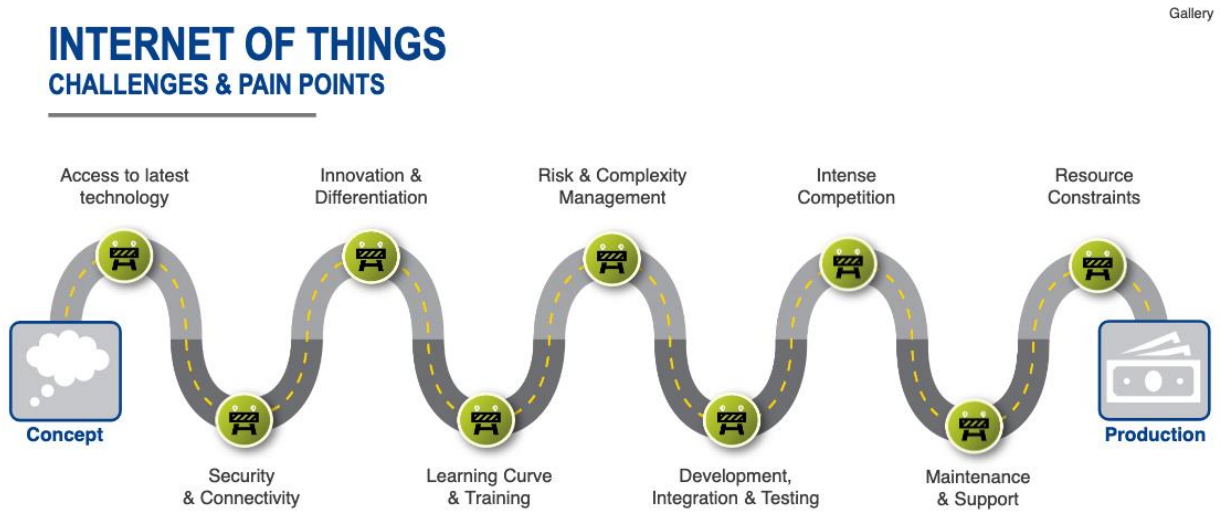



***圖 1.****物聯網應用程式開發人員必須遵循從概念到生產的漫長旅程，這會影響產品開發週期並增加其他成本*

為了因應這些安全挑戰，應用程式開發人員需要一種平台式的方法，運用硬體和軟體的最新發展，以實現可提供多層次安全性的深入全面保護。

在硬體方面，此平台包括：

- 受保護的偵錯存取，避免偵錯介面成為攻擊途徑。
- 用於加速對稱和非對稱標準加密操作的安全加密引擎，，以及實現更快速 HASH 演算法的硬體支援。
- 產生安全金鑰，在裝置上使用安全區域來儲存金鑰，並確保這些金鑰不會在未加密狀態下暴露於程式碼中。每個裝置都可以產生並留存本身的金鑰，因此裝置具有自己的獨特識別。在進行大規模的裝置安全設定和部署時，這是必備的做法。
- 安全的記憶體存取，可以保護快閃記憶體和 RAM 的指定區域，免於遭受未經授權或意外的讀寫嘗試。而敏感程式碼和資料應在一個單獨的記憶體領域中與非安全程式碼和資料隔離，而且單次寫入保護記憶體可以防止程式碼和資料被變更。

在軟體方面，這包括：

- 經整合和最佳化的商業等級軟體，具有成熟的應用程式框架和標準 API。
- 與硬體安全性和加密功能相關的驅動程式層 API。
- 軟體加密演算法的功能庫，具有更進階級別的抽象 API，用於在微控制器和外部通訊裝置或網路之間執行認證和安全通訊，以及在微控制器中加密機密敏感資料和程式加以儲存。
- 內建支援主要通訊的通訊協定和傳輸 (例如 TLS、MQTT 和 HTTPS) 以及雲端的特定通訊協定，因此開發人員無需整合低階中介軟體和網路堆疊，也無需處理這些通訊協定的授權和採購成本。

一套嵌入式微控制器軟體暨硬體平台可提供這些整合的功能，為物聯網開發人員帶來直接的效益，包括：

- 加快開發，因為工程團隊可以在 API 層級開始應用程式軟體開發。
- 降低總體擁有成本，因為緊密整合的模組包含重要的安全性和連線功能以及其他週邊裝置，以減少整合時間、材料成本，以及軟體的授權和費用。
- 降低技術進入門檻，針對滿足安全性和其他不斷變化的需求減少複雜性。

高度整合的嵌入式微控制器硬體暨軟體平台也極為重要，有助於確保將更安全的程式設計用於製造物聯網裝置。有鑑於全球供應鏈的複雜性日益增加，現在必須要取得額外的安全性和做法，以確保在製造環境中維護產品的完整性和真實性，且不會在生產週期中受到影響。

## Renesas Synergy 的安全功能

Renesas Synergy 平台是完整、合格的系統解決方案，包含軟體、可擴展的 MCU 系列和開發工具。工程團隊可以透過這套經過驗證的全面性的平台，在 API 層級開發物聯網應用程式，而省下數個月的時間和心力，並且確保團隊能在針對 MCU 產品設計而最佳化的穩健且強大的技術基礎上，進行產品創新。

Synergy 平台整合下列功能，內建深入的分層安全性。

**安全裝置識別。**物聯網裝置建立強大的裝置識別功能，在連線時進行唯一識別和認證，以確保其他裝置、服務和使用者之間獲得安全的加密通訊。強大的裝置識別功能則以多種方式滿足核心物聯網的安全需求。

- **信任。**裝置連線到網路時，必須在其他裝置、服務和使用者之間進行驗證並建立信任。建立信任後，裝置、使用者和服務就可以安全地進行通訊，並交換加密的資料和資訊。

- **隱私。**隨著愈來愈多物聯網裝置進行連線，所產生、收集和共用的資料也隨之增加。這些資料可能包括個人資訊、敏感資訊和財務資訊，而這些資訊必須保密並受到保護，且通常需符合法規規範。IoT 裝置彼此連線時，裝置識別可以確保認證和識別。

- **完整性。**裝置完整性適用於在物聯網生態系統內傳輸的裝置和資料。裝置的完整性始於展現其所宣稱的功能。藉由強大的獨特裝置識別功能，確保裝置是合法的，減少仿冒產品並維護公司的品牌。許多人忽視資料完整性的需求，但是連線裝置和系統需仰賴傳輸資訊的真實性和可靠性。

Synergy 平台提供多種金鑰產生選項，包括使用平台的安全加密引擎 (SCE) 模組產生唯一的硬體型裝置識別，可使用安全記憶體保護單元 (MPU) 和快閃記憶體存取範圍 (FAW) 安全地儲存在裝置的內部快閃記憶體中。Synergy SCE 模組可以加入至設計中，並針對目標應用程式進行正確的設定。

建立裝置識別的第一步是產生金鑰。金鑰可以在 Synergy MCU 內部產生，也可以在安全設備中從外部產生並放入 Synergy 裝置中。產生或放入裝置金鑰後，稱為憑證授權單位 (CA) 的實體將發行數位憑證。CA 可以是公有的 (位於雲端)，也可以是私有的 (位於本機，通常託管在安全的伺服器上)。在 Synergy 裝置上建立並編寫裝置識別後，就必須安全儲存，以免遭竊或損壞。這可透過 Security MPU 和 FAW 功能在程式碼快閃記憶體和 SRAM 中設定四個安全區域達成。這些區域只能透過「安全程式碼」存取。FAW 暫存器用於設定程式碼快閃記憶體位址範圍，這個範圍可以被清除和編寫。超出此範圍的位址 (也就是快閃記憶體存取範圍外) 在編寫後無法修改。此功能可用於防止裝置識別 (金鑰和認證) 被清除或重新編寫。

安全程式碼區域也包含僅被授權在安全資料區域上運作的 API 函數。Synergy MCU 上執行的任何非安全程式碼都無法存取或修改此部分。在取回重設向量之前會讀取並套用安全 MPU 設定，因此會在執行任何程式碼之前套用。在離開安全程式設計中心之前，使用 FAW 功能 (使用一次性可程式化 FPSR 位元) 鎖定安全 MPU 設定，以防止這些程式碼被修改。

Synergy 裝置提供的受保護記憶體功能可用於儲存安全啟動程式碼和裝置憑證/金鑰，以及對裝置識別應用極為重要的其他敏感資料。

## 安全資料

隨著物聯網和雲端連線的快速發展，確保數位資料安全已成為保護商業機密和個人隱私的首要考量。靜態資料是未主動從裝置移動到裝置，或從網路移動到網路的資料。在嵌入式系統中，安全資料可以留存在暫時性資料儲存 (MCU 的內部 SRAM 或外部 SDRAM) 或非揮發性資料儲存 (例如 MCU 的內部快閃記憶體、外部 QSPI 儲存和外部 EEPROM 儲存) 中。

Synergy MCU 提供資料存取控制、認證機制，以及 CPU 和匯流排主控的讀寫和單次寫入存取保護，以實現安全的靜態資料設計。此外，Synergy MCU 也提供安全功能，停用從非安全軟體存取控制與安全相關的週邊裝置。

**資料存取控制。**對嵌入式系統的裝置連線需求增加以及複雜性提高，導致更多潛在的攻擊面因此暴露。對安全資料的受控存取功能可有效減少攻擊面，藉以提高系統安全性。

Renesas Synergy 平台提供下列資料存取控制：

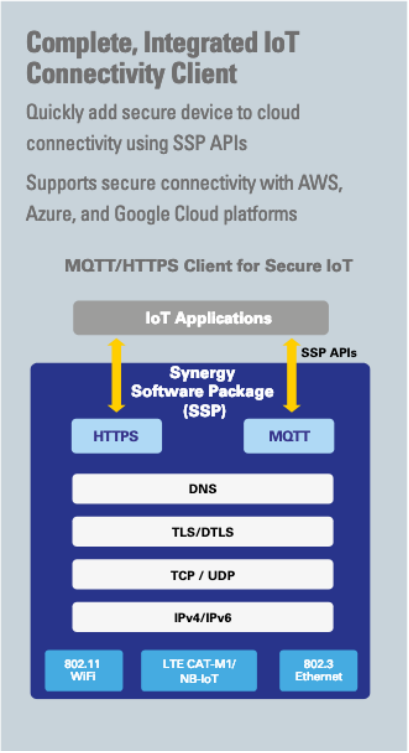
- **讀取保護。**留存在快閃記憶體和 SRAM 中的敏感資料和程式碼可獲得讀取保護屬性，以確保只有具讀取權限的軟體能存取受保護的資料。安全 MPU 能建立具有讀取保護的敏感區域。
- **寫入保護。**保護敏感資料不被惡意修改或清除是相當重要的。透過使用 Synergy 裝置中的記憶體選項設定，可以對暫時性和非暫時性資料進行寫入保護，以避免未經授權的修改。
- **讀寫保護。**讀寫保護可以縮減惡意軟體和 IP 竊取的攻擊面。針對內部快閃記憶體資料，Synergy 裝置可透過兩種方式提供讀寫保護：
    - 對於來自非安全軟體的安全 MPU 快閃記憶體和 SRAM 區域，Synergy Security MPU 可以停用讀寫存取，或者
    - 安全 MPU 和 FAW 一起使用時，快閃記憶體中的敏感資料可以對安全和非安全軟體進行讀寫保護。
- **單次寫入保護。**在特定使用案例中，需要保護敏感的靜態資料，以防止在裝置的生命週期中存取或變更這些靜態資料。例如，安全啟動載入程序必須在產品的生命週期內維持不可變。對於資料留存在內部快閃記憶體上的使用案例，可以對 FAW 設定進行程式編寫以提供單次寫入保護。
- **單次寫入和讀取保護。**可以選擇對單次寫入保護的資料進行讀取保護。處理敏感資料時，可以向單次寫入保護的快閃記憶體資料提供讀取保護，以確保只有安全軟體能讀取內容。

## 安全的雲端連線

物聯網由一套範疇廣泛的技術組合而成，可透過智慧方式將事物和群眾之間的多種新型通訊連結在一起。裝置使用感測器連線到網路，以提供從環境中收集的資訊，或允許其他系統透過執行器進行連線並進行處理。在此過程中，物聯網裝置會產生大量資料，而雲端計算則提供一條途徑，將資料傳輸到預定的目的地。

Synergy 平台為業界頂尖的雲端環境提供安全的內建連線，包括 Amazon Web Services (AWS)、Google Cloud 和 Microsoft Azure。Synergy MCU 使用 SSP 的 MQTT 和 TLS 模組提供對雲端連線的支援。

**MQTT 通訊協定。**MQTT 是指訊息佇列遙測傳輸。MQTT 是一種用戶端伺服器發佈訂閱式訊息傳輸通訊協定，極為輕量、開放，而且易於使用。MQTT 專為受限裝置以及低頻寬、高延遲或不可靠的網路而設計。這些特性使 MQTT 相當適用於需要較小程式碼容量，以及/或者網路頻寬相當寶貴的受限環境，例如機器到機器 (M2M) 和物聯網環境中的通訊等情境。




**TLS 通訊協定。**傳輸層安全性 (TLS) 通訊協定及較早期的安全通訊端層 (SSL)，是透過電腦網路提供通訊安全性的加密通訊協定。TLS/SSL 通訊協定在兩個通訊應用程式之間提供隱私和可靠性，具有下列基本屬性：

- **加密：**在通訊應用程式之間交換的訊息會經過加密，以確保連線的私密性。AES 之類的對稱加密機制則用於資料加密。
- **驗證：**使用憑證以驗證對等裝置識別的機制。
- **完整性：**偵測訊息篡改和偽造的機制，以確保連線可靠。訊息認證碼 (MAC)，例如安全雜湊演算法 (SHA)，確保訊息完整性。

## 安全啟動管理器

Synergy 安全啟動管理器提供各種功能，實現安全並且可靈活調整的生產程序，這是透過安全的韌體快閃記憶體程式設計解決方案所實現的，該解決方案幫助開發人員以可靠、安全的方式，將經授權的韌體編寫到遠端製造設施和現場的 Synergy MCU 快閃記憶體中，同時保護韌體不被修改、盜竊或安裝在仿冒的硬體上。

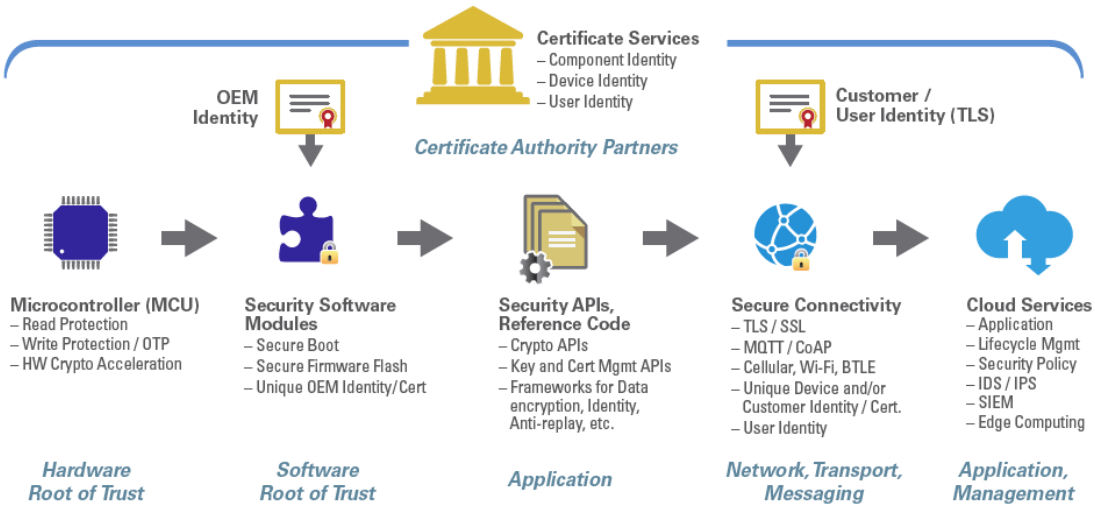



***圖 2.****瑞薩電子在整個產品生命週期中提供信任根保護。*

Synergy MCU 結合 Synergy 的安全啟動管理器，透過獨特識別、受硬體保護的金鑰、安全啟動載入程序、安全快閃記憶體更新模組以及與 MCU 硬體連線的加密 API，提供強大的信任根。安全啟動管理器包括：

- 用於管理 (數位簽章) 韌體的工具。
- 下載啟動載入程序、憑證和金鑰。
- 將使用者應用程式韌體刷新到授權的 MCU 上。

該過程會先在安全程式設計中心的每個目標 Synergy MCU 上安裝唯一的信任根。信任根包括 Renesas Synergy Boot Manager 以及由韌體 Mastering Tool 產生的獨特「信任根」。在後續的步驟中，這個 Mastering Tool 將對授權韌體進行簽署和加密，因為安全啟動載入程序將只會載入已由 Mastering Tool 簽署的韌體。信任根透過安全連線預先載入到程式設計人員系統中，該系統專為大量生產和供應晶片而設計，可以安全儲存資料，並保持對資料使用方式的嚴格控制。

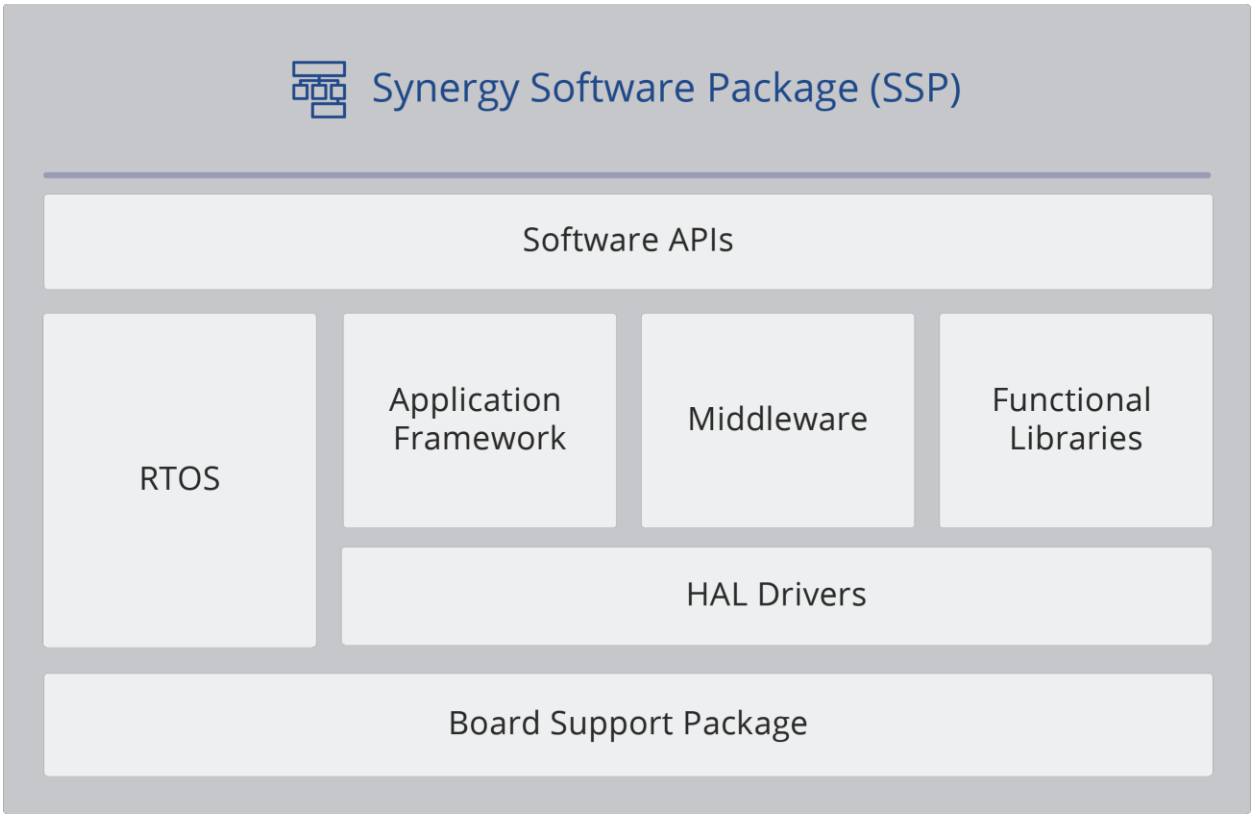
經授權的 MCU 載入到程式設計系統上，信任根刷新到各個 MCU 上，並附有金鑰，為每個裝置提供安全、唯一的識別。過程的下一個階段是安裝先前使用 Mastering Tool 進行數位簽署和加密的授權韌體。程式設計系統將韌體刷新到 MCU，而且先前安裝的信任根將驗證和解密韌體，並將韌體寫入快閃記憶體。在過程結尾時，設定為安全啟動載入程序的快閃記憶體存取範圍將被鎖定而無法修改，確保此為不可變的信任根，僅啟動受信任的韌體。

然後可以將經編寫的 Synergy MCU 運送到 OEM 或簽約製造工廠，將 MCU 裝載到電路板，以便安裝於最終產品或應用程式中。抵達現場後，可將授權韌體安全更新至 MCU 的快閃記憶體中，在進行快閃記憶體程式設計 (flash programming) 之前，使用晶片上的信任根來驗證和解密韌體，這些都透過安全的雲端基礎架構進行安全設定。

## Synergy 軟體套件

Synergy 軟體套件 (SSP) 提供針對 Synergy 平台開發及最佳化的商業級合格軟體。SSP 是經過驗證的框架和標準 API，將頂尖的即時作業系統 (RTOS)、一套中介軟體、多個程式庫，以及低階驅動程序緊密整合在一起，幫助您將遇到的複雜功能簡化，同時開發互聯嵌入式系統。其分層架構可供開發人員使用通用 API 編寫您的應用程式，或根據需要直接連接至 MCU 裝置的驅動程式層。

其附加軟體組件 (Add-on software components) 則透過專業功能、中介軟體套件和應用程式框架來補充軟體。Synergy 平台也包括兩個軟體開發環境：適用於 Renesas Synergy 的 e² studio 和 IAR Embedded Workbench™。軟體和工具包含在 Synergy 平台中，不收取任何費用或授權費。




為了確保做好生產準備，瑞薩電子依據涵蓋整個軟體開發生命週期的國際標準 ISO/IEC/IEEE 12207 來開發 SSP。SSP 的每個部分都受到這些要求限定，並根據這些要求進行測試。

## 認識瑞薩電子 S5D3 微控制器

瑞薩電子 S5D3 是 Synergy 系列微控制器的最新成員，可為物聯網系統開發提供符合成本效益的安全平台。S5D3 MCU 採用高性能 Cortex M4F 核心，針對記憶體進行了最佳化，且其嵌入式快閃記憶體與 SRAM 的比例為 2 比 1，具有極高的週邊整合度極。S5D3 並採用高效率的 40nm 製程，Synergy 軟體套件則全面支援並具有強大的設計支援和裝置評估環境，包括目標板套件和兩個整合開發環境 (IDE)。S5D3 還提供通用的規格，為工業和大樓自動化等領域的物聯網應用程式，帶來更進步的安全性和端點管理。

S5D3 是 S5 系列 MCU 產品的一部分，專為高性能和緊密整合而設計，具有廣泛的連線能力、圖形引擎和多個高精度資料擷取類比介面。S5 系列 MCU 也具有強化的安全性和安全功能，以及用於進階加密演算法的硬體加速。S5 系列擁有高度可擴展性和接腳相容性，並提供硬體套件以加速產品開發。

S5D3 是 S5 系列 MCU 中新增的一個符合成本效益的產品組。通用型 S5D3 專為需要高性能和強大安全性，但不需要晶片內建圖形加速或乙太網路連線等功能的應用程式而設計。40nm 製程可為 CPU 運作提供更高的效率，相當適合持續收集監控資料的物聯網應用程式。S5D3 針對記憶體

進行最佳化，具有 512 KB 的程式碼快閃記憶體、8 KB 的資料快閃記憶體和 256 KB 的 SRAM。可實現高效率運作，是相當有效率的 MCU，能夠為物聯網系統中的端點裝置實現進階可擴展的安全管理。S5D3 適用於工業和大樓自動化市場的應用程式，可用於系統和機械控制。而這也適用於智慧儀表應用程式中的網路控制，以及辦公自動化解決方案中的系統控制單元。

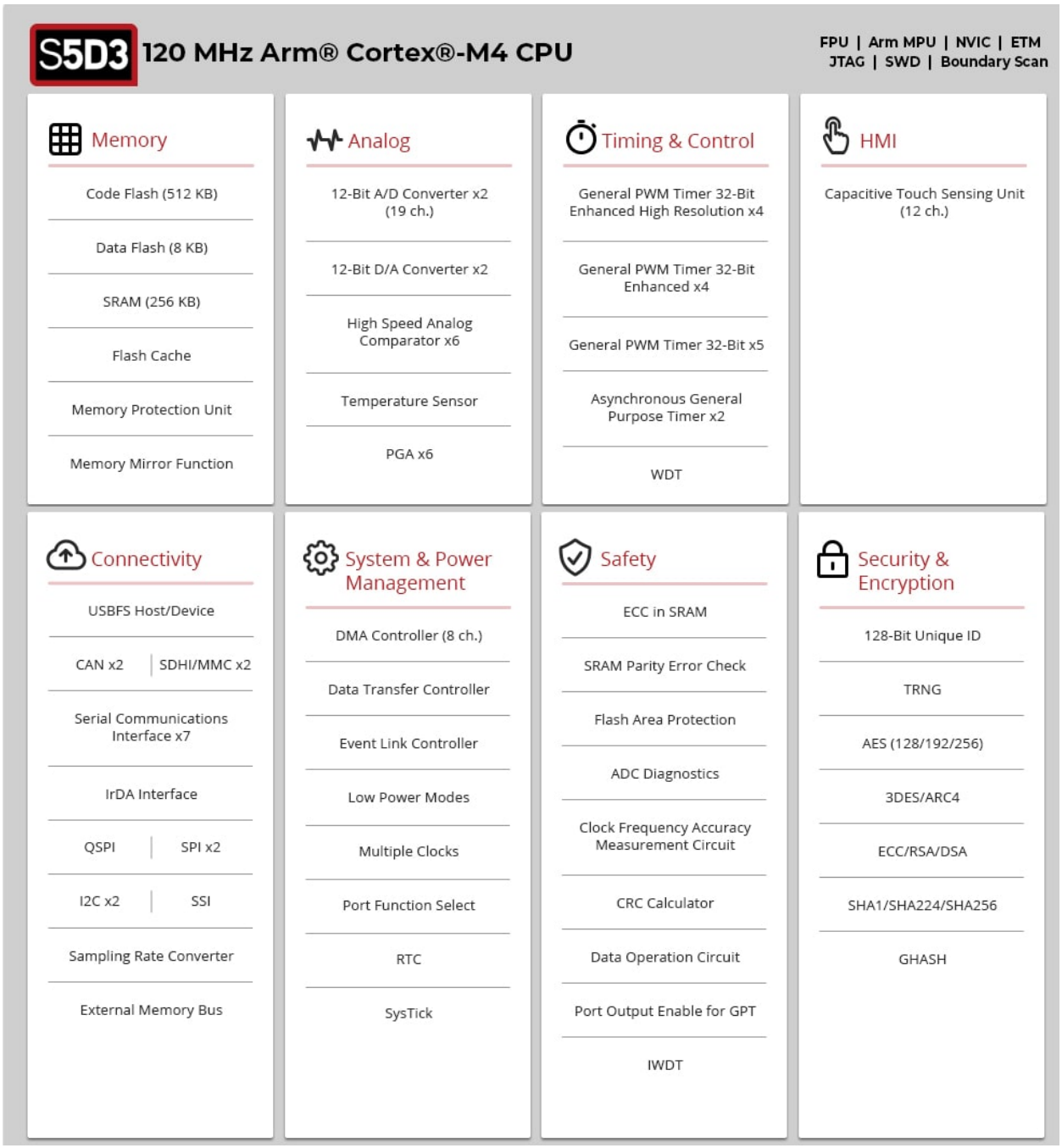



***圖 3**：S5D3 MCU 方塊圖*

## S5D3 的主要優點

**提供整合的安全功能，因而無需外部安全功能。**S5D3 透過在 MCU 上整合的多個進階功能組合提供安全的信任根。

S5D3 的整合式加密引擎「安全加密引擎」(SCE7) 提供的安全保護遠遠高於此類 MCU 中的其他解決方案。SCE7 是 MCU 上的獨立子系統，由專用控制邏輯管理和保護。已包裝的金鑰可防止敏感資訊洩露：透過 MCU 獨有的金鑰包裝確保金鑰隔離，該金鑰包裝為每個 MCU 獨特加密金鑰，因此金鑰只能在特定 MCU 的加密模組記憶體存取。

SCE7 也具有內建硬體加速器，包括 ECC、RSA、AES、3DES、SHA 和 TRNG，具有金鑰產生功能。安全模組也提供晶片內建快閃記憶體的寫入保護引導程式碼和資料 (根金鑰、設定)。這可以保護程式碼不被變更、複製或反向工程處理。安全 MPU 建立與硬體層級的非安全記憶體隔離的安全記憶體，並且將受信任和不受信任的程式碼和資料加以分離。

**內建大容量嵌入式 RAM，因此 S5D3 適合處理各種通訊堆疊。**具有強大連線能力的應用程式在連線的物聯網環境中極為重要。若要管理提供合理負載數量的通訊堆疊，需要使用大型嵌入式 SRAM 來提高性能並降低 BOM 成本。S5D3 為此提供了絕佳的嵌入式快閃記憶體與 SRAM 比例，達到 2 比 1 (512 KB 與 256 KB)。

## 結論

為物聯網應用程式提供全面、深入的安全保護，需要高度整合的最佳化功能平台，這些功能可以協同工作以提供多層次的安全性。Renesas Synergy 平台提供一套獨特的硬體和軟體安全功能，這些功能建立在共用信任根基礎之上，可以滿足保護物聯網裝置和網路的需求，能夠確保安全、可靈活調整的生產以及智慧財產權保護。瑞薩電子 S5D3 是 Synergy MCU 的最新成員，具有強大的分層安全功能，可為物聯網系統中的端點裝置實現優良且可擴展的安全管理。