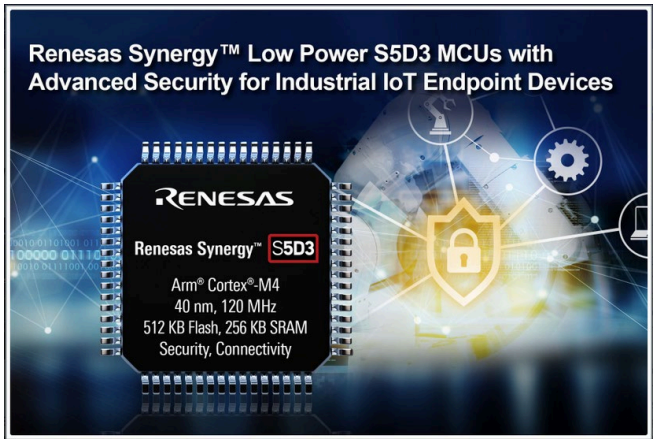
백서

수많은 장치를 안전하고 확장 가능한 방식으로 관리하는 방법

2019 년 2 월

Abstract

네트워크로 모든것이 연결된 오늘날의 사물인터넷(IoT) 환경에서 포괄적이고 심층적인 보안 보호 기능을 제공하기 위해서는 여러 과제에 직면하게 된다. Renesas Synergy Platform 은 원격 생산 과정에서의 안전하고 확장 가능한 제작과 지적 재산권의 보호 기능 등 IoT 장치와 네트워크 보안 요구 사항을 충족시킬 수 있는 고유한 복합 하드웨어 및 소프트웨어 보안 기능을 제공한다. Renesas S5D3 은 시너지 플랫폼을 구동하는 시너지 마이크로 컨트롤러 제품군에 추가된 최신 제품으로, 동일 기종의 다른 솔루션보다 월등히 높은 보안 기능을 제공한다. 범용 S5D3 은 가격대비 뛰어난 효율성을 제공하며 IoT 시스템의 최종 장치에 확장 가능한 첨단 보안 관리 기능을 구현하도록 해준다.



사물인터넷 보안의 과제

애플리케이션이 오늘날처럼 연결되지 않았던 얼마 전까지만 하더라도 개발자들은 제품 보안에 대해 크게 걱정할 필요가 없었다. 하지만 이제는 전구에서 장난감, 가전 제품에 이르기까지 가장 기본적인 제품조차도 IoT 네트워크나 인터넷, 클라우드 환경으로 연결되어 있다. 암호나 방화벽만으로도 충분했던 때와 비교하면 보안에 대한 요구 사항이 현저하게 높아졌다. 이제 개발자들은 사이버 위협으로부터 데이터와 기능을 보호할 수 있도록 IoT 애플리케이션 보안을 먼저 생각해야 하고 하드웨어와 소프트웨어 방식 모두로 보안 장치를 구축해야 한다.

사이버 위협이 고도화되고 악의적으로 이용되는 오늘날 보안 표준은 끊임없이 진화하고 있으며 이에 따라 애플리케이션들은 다수의 표준을 충족시켜야 하기 때문에 장치 호환성이나 유연성이 저하될 수 있다. 많은 개발 사례에서 높은 보안 기능은 비용과 전력 소모의 증가로 이어지며 최종 애플리케이션의 시장성에 영향을 준다.

따라서 IoT 애플리케이션은 다음과 같은 요소를 충족시켜야 한다:

- 지적 재산의 도용, 제품 복제, 제작 단계에서의 과다생산 등으로부터의 지적 재산 보호
- 중요 인프라를 폐쇄 또는 손상시키거나 악용하는 행위로부터 보호
- 중요 정보의 기밀유지와 보안을 위한 데이터의 무결성 보장
- 부트 매니저 보안 등 견고하고 신뢰할 수 있는 기반 조성
- 엔드 포인트와 유무선 네트워크, 클라우드간의 통신 및 연결 보안

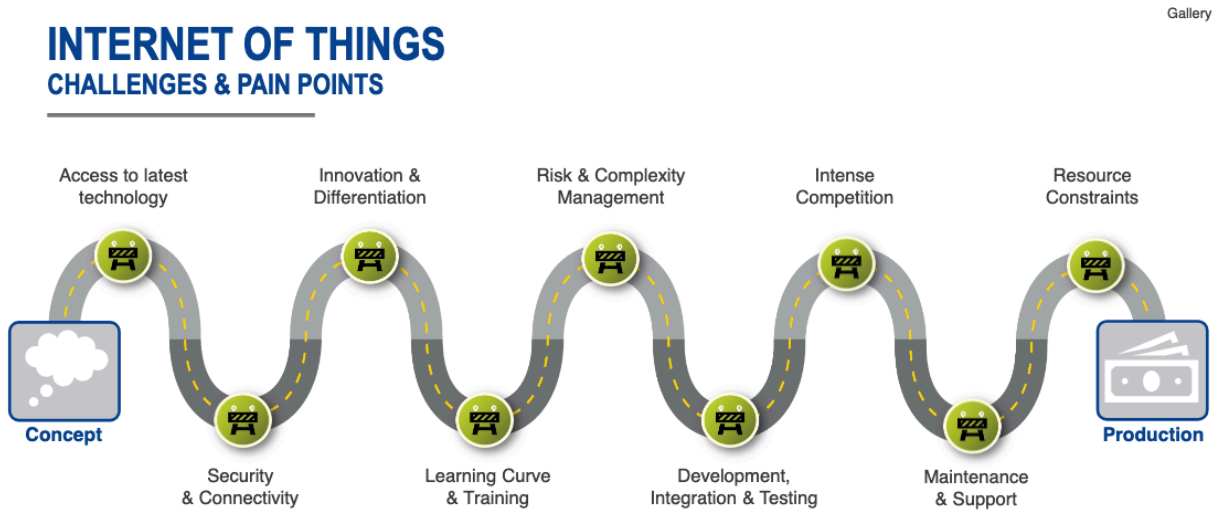


그림 1. *IoT 애플리케이션 개발은 제품 구상에서 생산에 이르는 긴 과정에서 출시 일정과 기타 비용이 추가된다.*

이러한 보안 과제를 충족시키기 위해 애플리케이션 개발자들은 첨단 하드웨어 및 소프트웨어 기술을 활용하여 다중 보안을 제공하고 심층적이고 포괄적인 보호 기능을 구현할 수 있는 플랫폼 기반 접근 방식을 필요로 한다.

하드웨어 측면에서 플랫폼에는 다음과 같은 구성요소가 포함된다:

- 디버깅 인터페이스를 공격 벡터에서 제외시킬 수 있는 안전한 디버깅 액세스
- 대칭 및 비대칭 표준에 대한 신속한 암호화 작업을 위한 보안 및 암호화 엔진, 보다 빠른 HASH 알고리즘을 위한 하드웨어 지원.

- 키를 보유한 보안영역이 있고 암호화되지 않은 상태의 코드 노출을 방지해주는 보안 키 생성. 각 장치는 고유 한 키를 생성 및 보유할 수 있기 때문에 장치들을 안전하게 보호하고 대규모로 배포하는 데 필요한 고유 ID 를 가질 수 있음.

- 의도하지 않거나 무단 읽기 또는 쓰기 시도로부터 플래시 메모리와 RAM 의 지정된 영역을 보호할 수 있는 안전한 메모리 액세스. 민감한 코드와 데이터는 비보안 코드와 데이터로부터 별도의 메모리 도메인으로 격리되어야 하며 바꿔 쓰기가 되지 않는 보호 메모리는 코드와 데이터가 변경되는 것을 방지함.

소프트웨어 측면에서는 다음과 같은 구성요소가 포함된다:

- 검증된 애플리케이션 프레임워크 및 표준 API 를 가진 통합되고 최적화된 상용 소프트웨어

- 하드웨어 보안 및 암호화 기능 인터페이스를 가진 드라이버 수준의 API

- 마이크로 컨트롤러와 외부 통신 장치 또는 네트워크 간의 인증과 보안 통신을 수행하고 기밀 데이터와 마이크로컨트롤러 저장 프로그램을 암호화하기 위한 상위 수준의 API 가 있는 소프트웨어 암호화 알고리즘의 기능 라이브러리

- 개발자가 낮은 수준의 미들웨어와 네트워크 스택을 통합하거나 프로토콜의 라이선스나 비용을 걱정할 필요가 없는 TLS, MQTT, HTTPS 등 주요 통신 프로토콜 및 전송을 위한 내장형 지원과 클라우드 전용 프로토콜

이러한 통합 기능을 제공하는 임베디드 마이크로컨트롤러 소프트웨어와 하드웨어 플랫폼은 IoT 개발자에게 다음과 같은 이점을 제공한다:

- 엔지니어링 팀이 API 수준에서 애플리케이션 소프트웨어 개발을 시작할 수 있어 개발 시간이 단축됨.

- 통합 모듈에 주요 보안 및 연결 기능, 기타 주변 장치가 포함되어 있어 통합 시간 단축, BOM (bill of material), 로열티, 소프트웨어 비용 등 총 소유 비용이 절감됨.

- 진입 장벽을 낮춤으로써 보안 및 기타 요구 사항에 따른 복잡성이 줄어듦.

고도로 통합된 임베디드 마이크로 컨트롤러 하드웨어 및 소프트웨어 플랫폼은 또한 IoT 장치 제조에 있어 보다 안전한 프로그래밍을 보장하는 데 매우 중요하다. 글로벌 공급 체계의 복잡성이 증가함에 따라 제품의 무결성과 신뢰성을 보장하고 생산 과정에서 저하되지 않도록 하기 위해서는 추가 보안과 조치가 필요하다.

Renesas Synergy 의 보안 기능

Renesas Synergy Platform 은 소프트웨어와 확장 가능한 MCU 제품, 개발 툴이 포함된 완전하고 검증된 시스템 솔루션이다. 엔지니어링 팀은 이 포괄적이고 검증된 플랫폼을 통해 API 단계에서 IoT 애플리케이션 개발에 착수할 수 있기 때문에 수개월의 시간과 노력을 절약할 수 있다. 또한 MCU 기반 제품 설계에 최적화된 안정적이고 강력한 기술을 기반으로 제품 혁신이 가능하다.

다음과 같은 기능을 통합시켜 고도화된 다중 보안 기능이 Synergy 플랫폼에 구축된다.

보안 장치 ID. 강력한 장치 ID 가 설정되면 각 IoT 장치를 고유하게 식별 및 인증할 수 있어 장치와 서비스, 사용자 간에 안전하고 암호화된 통신을 보장할 수 있다. 강력한 장치 식별은 여러 방식으로 IoT 보안의 핵심 요구 사항을 충족시킬 수 있다.

- **신뢰성.** 장치가 네트워크에 연결되면 다른 장치와 서비스, 사용자들 간의 인증이 필요하고 신뢰성을 형성해야 한다. 신뢰성이 설정되면 장치와 사용자, 서비스는 암호화된 데이터와 정보를 안전하게 통신 및 교환할 수 있다.

- **프라이버시.** 많은 IoT 장치가 연결될수록 생성되고 수집되며, 공유되는 데이터가 증가하게 된다. 이러한 데이터에는 법규에 의거하여 보안이 필요한 개인정보나 민감한 정보, 금융 정보가 포함될 수 있는데 장치 ID 는 IoT 장치들이 상호 연결될 때 인증 및 식별을 보장할 수 있다.

- **무결성**. 장치의 무결성은 IoT 환경 내에서 전송되는 장치와 데이터에 모두 적용된다. 장치의 무결성은 그것이 무엇인지를 증명하는 것으로 시작합니다. 강력하고 고유한 장치 ID 를 통해 장치의 정당성을 검증함으로써 위조 제품을 줄이고 회사의 브랜드를 보호할 수 있다. 데이터의 무결성은 종종 간과되기도 하는 요구 사항이지만 연결된 장치와 시스템은 전송되는 정보의 신뢰성과 진본성에 의존한다.

Synergy 플랫폼은 SCE(보안 암호화 엔진) 모듈을 사용하여 고유한 하드웨어 기반 장치 ID 를 생성하는 등 여러 가지 키 생성 옵션을 제공하는데 여기서 하드웨어 기반 장치 ID 는 MPU(보안 메모리 보호 장치) 및 FAW(플래시 액세스 창)을 사용하여 장치의 내부 플래시에 안전하게 저장할 수 있다. Synergy SCE 모듈은 대상 애플리케이션에 따라 설계에 추가 및 구성이 가능하다.

장치 ID 를 만들기 위해서는 먼저 키를 생성해야 한다. 키는 Synergy MCU 내부나 생성되거나 외부 보안 시설에서 생성되어 Synergy 장치에 입력될 수도 있다. 장치 키가 생성되거나 입력되면 CA(인증 기관)에서 디지털 인증서를 발급하는데 CA 는 공개(클라우드에 위치) 또는 개인(일반적으로 보안 서버에 호스팅 되는 구내형)으로 구분된다. 장치 ID 가 생성되고 Synergy 장치에 프로그래밍되면 장치 ID 가 도난 또는 손상되지 않도록 안전하게 저장해야 한다. 이를 위해 보안 MPU 와 FAW 기능을 사용하여 코드 플래시와 SRAM 에서 4 개의 보안 영역을 구성한다. 이들 영역은 “보안 코드"를 통해서만 접근이 가능하다. FAW 레지스터는 삭제 및 프로그래밍이 가능한 코드 플래시의 주소 범위를 설정하는 데 사용된다. 이 범위를 벗어난 주소, 즉 플래시 액세스 창의 외부는 일단 프로그래밍되면 수정이 불가하다. 이 기능은 장치 ID(키, 인증)가 삭제되거나 다시 프로그래밍되지 않도록 하는 데 사용된다.

보안 코드 영역에는 보안 데이터 영역에서만 적용되는 API 함수도 포함된다. 이 섹션은 Synergy MCU 에서 실행중인 안전하지 않은 코드로는 액세스나 수정이 불가하다. 보안 MPU 설정 재설정 벡터를 가져오기 전에 읽히고 적용되므로 코드가 실행되기 전에 적용된다. 보안 MPU 설정은 보안 프로그래밍 센터에서 나가기 전에 FAW 기능을 사용하여 수정이 불가능하도록 잠글 수 있다(1 회에 한하여 프로그래밍이 가능한 FPSR 비트 사용).

Synergy 장치에서 제공하는 보호된 메모리 기능은 장치 ID 애플리케이션에 필수적인 기타 민감한 데이터 중에서 보안 부트 코드와 장치 인증서·키를 저장하는 데 사용된다.

보안 저장 데이터

사물인터넷(IoT)과 클라우드 연결의 급격한 증가로 인하여 영업 비밀과 개인 정보 보호에 있어서 디지털 데이터 보안의 중요성이 강조되고 있다. 저장 데이터(Data at Rest)는 장치에서 장치로 또는 네트워크에서 네트워크로 활발하게 이동하지 않는 데이터를 의미한다. 임베디드 시스템에서 보안 데이터는 휘발성 데이터 저장소(MCU 의 내부 SRAM 또는 외부 SDRAM)나 비휘발성 데이터 저장소(MCU 의 내부 플래시 저장소, 외부 QSPI 저장소, 외부 EEPROM 저장소)에 상주할 수 있다.

Synergy MCU 는 저장데이터의 보안 설계를 위해 CPU 와 버스 마스터로부터 데이터 접근 제어, 인증 방식, 읽기·쓰기, 바꿔쓰기가 되지 않는(write-once) 액세스 보호 기능을 제공한다. 또한 비보안 소프트웨어의 접근으로부터 특정 보안 관련 주변 장치를 제어할 수 없게 만드는 보안 기능을 제공하기도 한다.

데이터 접근 제어. 임베디드 시스템의 복잡성과 함께 장치 연결에 대한 요구가 증가함에 따라 더 많은 공격 대상이 노출된다. 보안 데이터에 대한 접근 제어는 공격 대상을 효과적으로 줄여주어 시스템 보안을 향상시켜준다.

Renesas Synergy 플랫폼은 다음과 같은 데이터 접근 제어를 제공한다.

- **읽기 보호(Read Protection)**. 플래시와 SRAM 에 저장된 중요 데이터와 코드는 읽기 권한이 부여된 소프트웨어에 한하여 접근이 가능하도록 읽기 보호(read protection) 속성을 설정할 수 있으며 Security MPU 는 읽기 보호 기능이 적용된 보안 영역을 설정할 수 있는 기능을 가지고 있다.

- **쓰기 보호(Write Protection)**. 중요한 데이터를 악의적으로 수정하거나 삭제하지 않도록 보호하는 것이 중요하다. 휘발성 및 비휘발성 데이터는 무단으로 수정되는 것을 방지하기 위해 Synergy 장치의 메모리 옵션 설정을 통해 쓰기 보호가 가능하다.

- **읽기/쓰기 보호**. 읽기/쓰기 보호는 멀웨어와 IP 도용의 공격 대상을 보호할 수 있으며 내부 플래시 데이터의 경우 Synergy 장치는 다음과 같이 두 가지 방식으로 읽기/쓰기 보호 기능을 제공한다:

    - Synergy Security MPU 는 보안 MPU 플래시와 SRAM 영역에 대한 비보안 소프트웨어의 읽기 및 쓰기 접근을 비활성화 할 수 있다, 또는

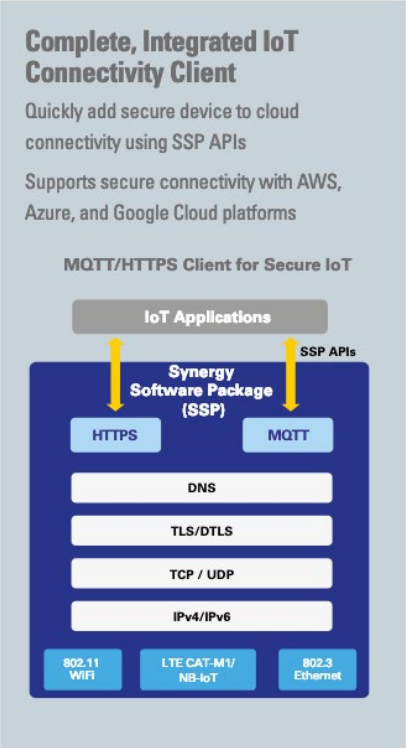
    - 보안 MPU 와 FAW 를 함께 사용하면 플래시에 저장된 민감한 데이터에 대해 보안 소프트웨어와 비보안 소프트웨어 모두에서 읽기/쓰기 보호를 적용할 수 있다.

- **바꿔쓰기 방지(Write-Once Protection)**. 일부의 경우, 민감한 저장데이터는 장치의 수명 주기 동안 접근이나 수정이 되지 않도록 보호하는 것이 필요하다. 예를 들어, 보안 부트 로더는 제품의 수명 주기 동안 수정이 불가능해야 한다. 데이터가 내부 플래시에 저장되어 있는 경우 바꿔쓰기를 방지하도록 FAW 설정을 프로그래밍할 수 있다.

- **바꿔쓰기 방지 및 읽기 보호(Write-Once and Read Protection)**. 바꿔쓰기 방지가 적용된 데이터는 선택적으로 읽기 보호를 적용할 수 있다. 민감한 데이터의 경우 안전한 소프트웨어에 한하여 읽기가 가능하도록 바꿔쓰기가 방지된 플래시 데이터에 읽기 보호를 설정할 수 있다.

안전한 클라우드 연결

IoT(사물인터넷)은 사물과 인간 사이의 여러 새로운 형태의 커뮤니케이션을 지능적으로 연결시켜주는 광범위한 기술로 구성된다. 장치는 센서를 사용하여 네트워크에 연결하여 환경에서 수집한 정보를 제공하거나 액추에이터(actuator)를 통해 다른 시스템이 외부와 연결하여 작동하도록 해준다. 이 과정에서 IoT 장치는 방대한 양의 데이터를 생성하며 클라우드 컴퓨팅은 데이터를 원하는 대상으로 이동시킬 수 있는 통로 역할을 한다.



Synergy 플랫폼은 Amazon Web Services (AWS), Google Cloud, Microsoft Azure 등 주요 클라우드 환경에서 안전하고 통합된 연결을 제공하며 Synergy MCU 는 SSP 의 MQTT 와 TLS 모듈을 사용하여 클라우드 연결을 지원한다.

MQTT 프로토콜. MQTT 는 Message Queuing Telemetry Transport 의 약자로 매우 가볍고 개방적이며 사용하기 쉬운 Client Server publish-subscribe 메시징 전송 프로토콜이다. MQTT 는 제한된 장치뿐만 아니라 낮은 대역폭이나 높은 지연율을 가지고 있거나 신뢰할 수 없는 네트워크를 위해 설계되었다. 이러한 특성 때문에 MQTT 는 코드 크기가 작아야 하거나 네트워크 대역폭이 중요한 M2M(Machine to Machine)과 IoT 환경 등 제한된 환경에 적합하다.

TLS 프로토콜. SSL (Secure Sockets Layer)과 그 후속 프로토콜인 TLS(Transport Layer Security) 프로토콜은 컴퓨터 네트워크에서 통신 보안을 제공하는 암호화 프로토콜이다. TLS/SSL 프로토콜은 통신하는 애플리케이션간에 정보 보호와 안정성을 제공하며 다음과 같은 기본 속성을 가진다:

- **암호화**: 통신하는 애플리케이션들 간에 교환되는 메시지를 암호화하여 정보를 보호하며 AES 와 같은 대칭 암호화 메커니즘이 데이터 암호화에 사용된다.
- **인증:** 인증서를 사용하여 피어(peer)를 식별하는 메커니즘이다.
- **무결성**: 메시지 변조 및 위조를 탐지하는 메커니즘으로 연결의 신뢰성을 보장하며 보안 해시 알고리즘(SHA: Secure Hash Algorithm)과 같은 메시지 인증 코드(MAC: Message Authentication Code)는 메시지의 무결성을 보장한다.

안전한 부트 매니저

Synergy Secure Boot Manager 는 안전하고 확장 가능한 제조를 가능하게 해주는 기능을 제공한다. 이는 개발자가 원격 제조 설비나 현장에 있는 Synergy MCU 의 플래시 메모리에 승인된 펌웨어를 안정적이고 안전하게 프로그래밍 할 수 있도록 해주는 펌웨어 플래시 프로그래밍 솔루션을 통해 가능하며 이는 펌웨어를 수정하거나 불법 복제, 복제된 하드웨어에 설치하는 것을 방지해준다.

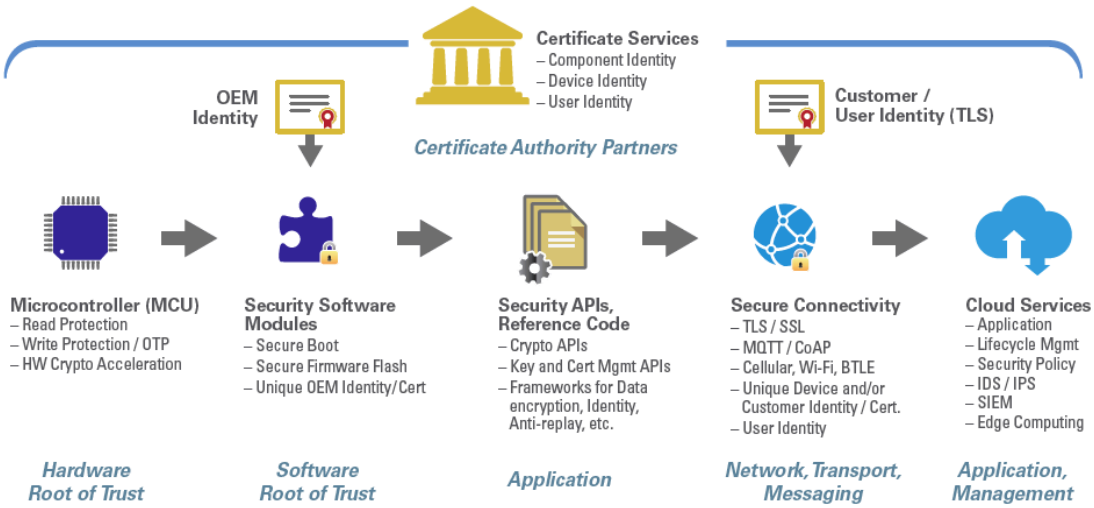


그림 2. *Renesas 는 제품의 전체 수명주기에 걸쳐 root-of-trust 보호 기능을 제공한다.*

Synergy MCU 와 Synergy 의 Secure Boot Manager 는 고유 ID 와 하드웨어 보호 키, 안전한 부트 로더, 안전한 플래시 업데이트 모듈, MCU 하드웨어와 인터페이스가 가능한 암호화 API 를 통해 강력한 root-of-trust 를 제공한다. Secure Boot Manager 에는 다음이 포함된다:

- 펌웨어 마스터링 툴(디지털 서명)
- 부트 로더, 인증서, 키 다운로드
- 인증된 MCU 에 사용자 애플리케이션 펌웨어 플래시

이 프로세스는 보안 프로그래밍 센터의 각 해당 Synergy MCU 에 고유한 root-of-trust 를 설치하는 것으로 시작된다. root of trust 는 Renesas Synergy Boot Manager 와 펌웨어 마스터링 툴에 의해 생성된 고유한 root-of-trust 로 구성된다. 마스터링 툴이 서명한 펌웨어에 한하여 보안 부트 로더에서 로드하기 때문에 이후 과정에서 마스터링 툴은 인증된 펌웨어를 서명하고 암호화한다. root-of-trust 는 데이터를 안전하게 저장하고 사용을 엄격하게 통제하는 칩 대량 생산 및 공급을 위해 설계된 프로그래머 시스템에 보안 연결을 통해 사전 로드된다.

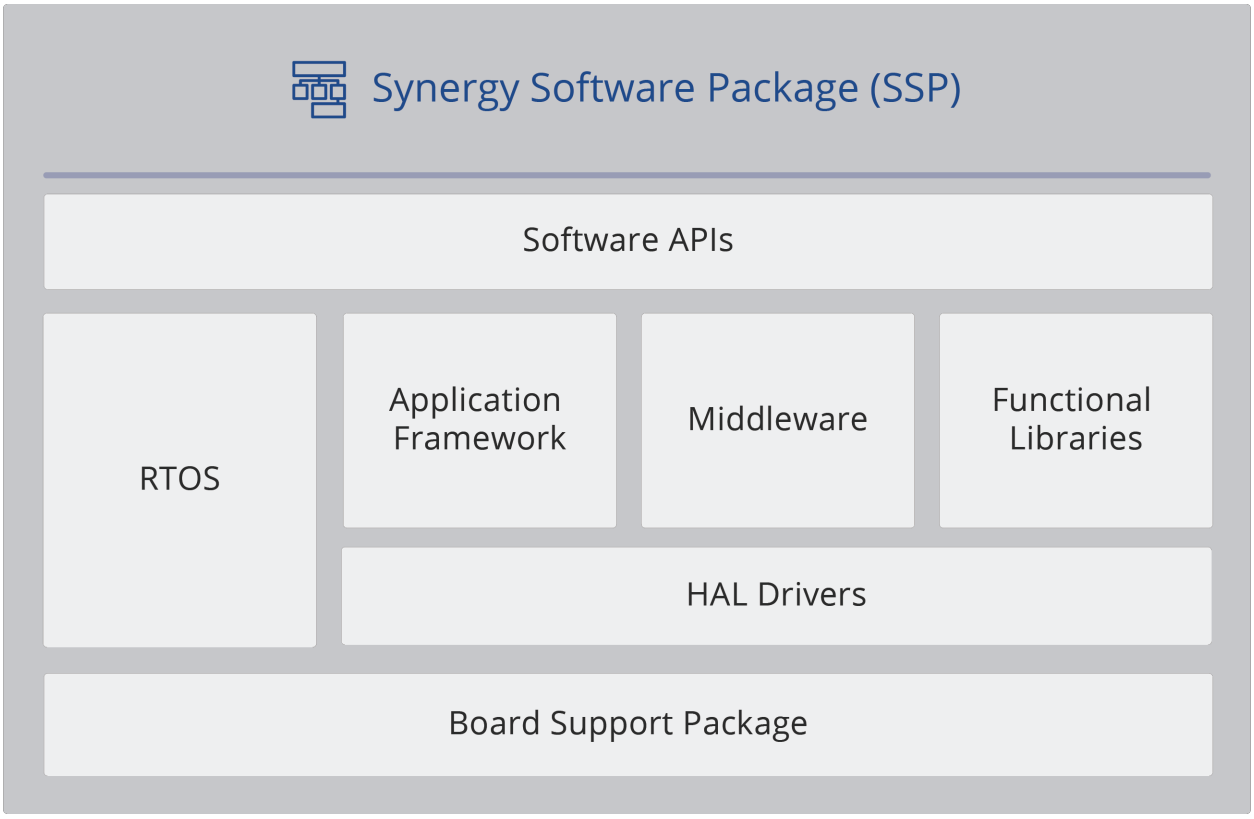
인증된 MCU 는 프로그래밍 시스템에 로드되고 root of trust 는 각 장치에 안전하고 고유한 ID 를 제공하는 키와 함께 각 MCU 에 플래시 된다. 다음 단계에서는 마스터링 툴을 사용하여 이전에 디지털 방식으로 서명되고 암호화된 인증 된 펌웨어를 설치한다. 프로그래밍 시스템은 MCU 에 펌웨어를 플래시하고 기존에 설치된 root-of-trust 는 펌웨어를 검증 및 복호화하고 플래시 메모리에 기록한다. 프로세스 마지막에는 Secure Boot Loader 에 설정된 플래시 액세스 창이 수정되지 않도록 잠기며 신뢰할 수 있는 펌웨어만 부팅하는 변경 불가한 root-of-trust 로 동작한다.

프로그래밍된 Synergy MCU 는 OEM 또는 제조 설비로 운송되며 여기서 최종 제품 또는 애플리케이션에 설치될 회로 기판에 장착된다. 현장에서 인증된 펌웨어를 MCU 의 플래시 메모리로 안전하게 업데이트 할 수 있으며 플래시 프로그래밍 전에 펌웨어의 검증 및 복호화에 사용되는 온칩 root-of-trust 를 사용하여 보안 클라우드 인프라를 통해 안전하게 제공된다.

시너지 소프트웨어 패키지

SSP(Synergy Software Package)는 Synergy 플랫폼용으로 개발 및 최적화된 상용 소프트웨어를 제공한다. SSP 에는 프리미엄 실시간 운영 체제(RTOS)와 미들웨어 제품군, 다양한 라이브러리와 로우 레벨(low-level) 드라이버를 통합하는 검증된 일련의 프레임워크와 표준 API 가 포함되어 있어 연결된 임베디드 시스템 개발 과정에서 발생하는 복잡한 기능들을 단순화시켜준다. 개발자는 계층화된 아키텍처를 활용하여 공통 API 를 사용하거나 필요에 따라 MCU 장치 드라이버에 직접 연결하여 애플리케이션을 생성할 수 있다.

애드온 소프트웨어 컴포넌트는 특수 기능, 미들웨어 패키지, 애플리케이션 프레임워크로 소프트웨어를 보완한다. Synergy 플랫폼에는 또한 소프트웨어 개발 환경인 IAR Embedded Workbench™와 e² studio 가 포함되며 소프트웨어와 툴이 로열티나 비용 없이 무료로 제공된다.



Renesas 는 생산 준비를 지원하기 위해 ISO/IEC/IEEE 12207 국제표준에 따라 소프트웨어의 전체 개발 주기에 사용 가능한 SSP 를 개발하였다. SSP 의 모든 요소들은 이러한 요구 사항을 충족시키도록 정의 및 테스트된다.

Renesas S5D3 마이크로컨트롤러 소개

S5D3 MCU GROUP

Renesas S5D3 은 최신 Synergy 마이크로컨트롤러 제품으로 IoT 시스템 개발을 위한 안전하고 비용에 최적화된 플랫폼이다. S5D3 MCU 는 고성능 Cortex M4F 코어를 기반으로 하며 2:1 의 내장 플래시

대 SRAM 비율을 가지고 있고 주변 장치가 통합되어있어 메모리에 최적화되어 있다. S5D3 은 고효율 40nm 공정을 기반으로 하고 Synergy Software Package 에서 완벽하게 지원하며 타겟 보드 키트와 2 개의 IDE(Integrated Development Environments)를 포함한 강력한 설계 지원과 장치 평가 환경을 제공한다. S5D3 은 산업 및 빌딩 자동화와 같은 분야에서 IoT 애플리케이션을 위한 고급 보안 및 엔드 포인트 관리 기능을 제공하는 범용 사양을 가진다.

S5D3 은 S5 MCU 시리즈의 일부로 광범위한 연결과 그래픽 엔진, 다수의 고정밀 데이터 수집 아날로그 인터페이스를 가지고 있으며 고성능과 긴밀한 통합이 장점이다. S5 시리즈 MCU 는 또한 하드웨어 가속을 통해 강화된 보안 및 안전 기능을 갖추고 있어 고급 암호화 알고리즘을 구현한다. S5 시리즈는 확장 성이 뛰어나고 핀 호환이 가능하며 제품의 개발 속도를 향상시켜주는 하드웨어 키트를 제공한다.

S5D3 은 뛰어난 가성비를 가진 새 S5 MCU 제품으로 범용 S5D3 은 높은 성능과 강력한 보안이 요구되지만 온칩 그래픽 가속이나 이더넷 연결과 같은 기능을 필요로 하지 않는 애플리케이션에 적합하다. 또한 40nm 공정은 CPU 동작에 있어서 높은 전력 효율성을 제공하며 모니터링 데이터가 지속적으로 수집되는 IoT 애플리케이션에 적합하다. S5D3 은 512KB 의 코드 플래시, 8KB 의 데이터 플래시, 256KB 의 SRAM 을 가지고 있어 메모리에 최적화되어 있다. 매우 매력적인 가격과 높은 효율성을 가지고 있어 IoT 시스템에서 엔드 포인트 장치의 확장 가능한 고급 보안 관리에 매우 효과적인 제품으로 산업 및 빌딩 자동화 시장에서 시스템과 기계 제어에 사용할 수 있는 애플리케이션은 물론 Smart Meter 애플리케이션의 네트워크 제어와 사무 자동화 솔루션의 시스템 제어 장치로도 적합하다.

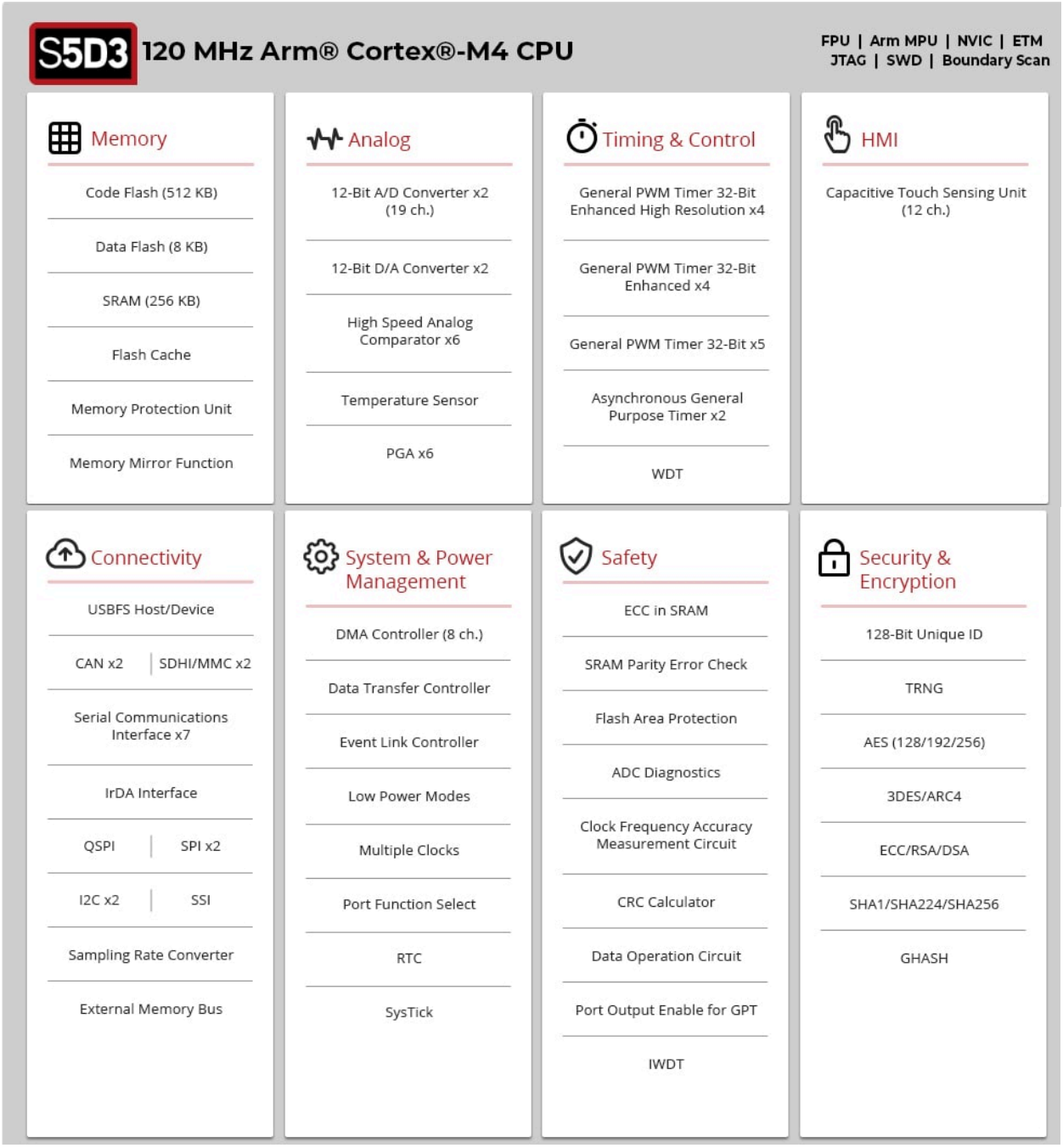


***그림 3:** S5D3 MCU 그룹 블록 다이어그램*

S5D3 의 주요 장점

외부 보안 기능이 필요 없는 통합 보안. S5D3 은 MCU 에 통합된 다수의 고급 기능을 결합시킨 보안 root of trust 를 제공한다.

S5D3 의 통합 암호화 엔진인 SCE7(Secure Cryptographic Engine)은 동일 기종의 MCU 에서 다른 솔루션보다 월등히 우수한 보안 기능을 제공한다. SCE7 은 MCU 의 독립된 하위 시스템으로 전용 제어 로직에 의해 관리 및 보호되며 래핑된 키는

민감한 정보의 노출을 방지해준다. 각 MCU 별로 키를 고유하게 암호화하는 키 랩핑 방식으로 키를 분리시켜 특정 MCU 의 암호화 모듈 내에서만 키에 접근할 수 있다.

SCE7 는 또한 ECC, RSA, AES, 3DES, SHA, TRNG 와 같은 내장 하드웨어 가속기와 키 생성 기능을 가지고 있으며 보안 모듈은 온칩 플래시로 쓰기 보호된 부트 코드와 데이터(루트 키, 구성)를 제공한다. 이를 통해 코드가 변경, 복사 또는 역설계 되지 않도록 보호해준다. Security MPU 는 하드웨어 단계에서 비보안 메모리와 분리된 보안 메모리를 설정하고 신뢰할 수 있는 코드와 데이터를 신뢰할 수 없는 코드와 데이터로부터 분리할 수 있도록 해준다.

대용량 임베디드 RAM 이 내장되어 있어 다양한 통신 스택을 처리하는 데 적합하다. 연결된 IoT 환경에서는 강력한 연결을 가진 애플리케이션이 요구된다. 적합한 양의 페이로드를 제공하는 통신 스택을 관리하려면 성능을 높이고 BOM 비용을 낮추기 위한 대용량 임베디드 SRAM 이 필요하다. S5D3 은 플래시 대 SRAM 의 비율이 2 대 1(512KB 대 256KB)인 것이 특징이다.

결론

IoT 애플리케이션에서 포괄적이고 심층적인 보안 보호 기능을 제공하려면 고도로 통합되고 최적화된 플랫폼에서 기능들이 연동하여 다중 보안을 구현하는 것이 필요하다. Renesas Synergy Platform 은 공유된 root of trust 를 기반으로 IoT 장치와 네트워크의 보안 요구 사항을 충족시키고 고유한 하드웨어 및 소프트웨어 보안 기능을 제공하며 안전하고 확장 가능한 제조 및 지적 재산권을 보호해준다. Renesas S5D3 은 Synergy MCU 계열의 최신 제품으로 강력한 다중 보안 기능을 탑재하여 IoT 시스템의 엔드 포인트 장치의 고급 보안 관리를 구현해준다.