Rapid development of secure IoT products with ARM CoreLink SSE-200 subsystem

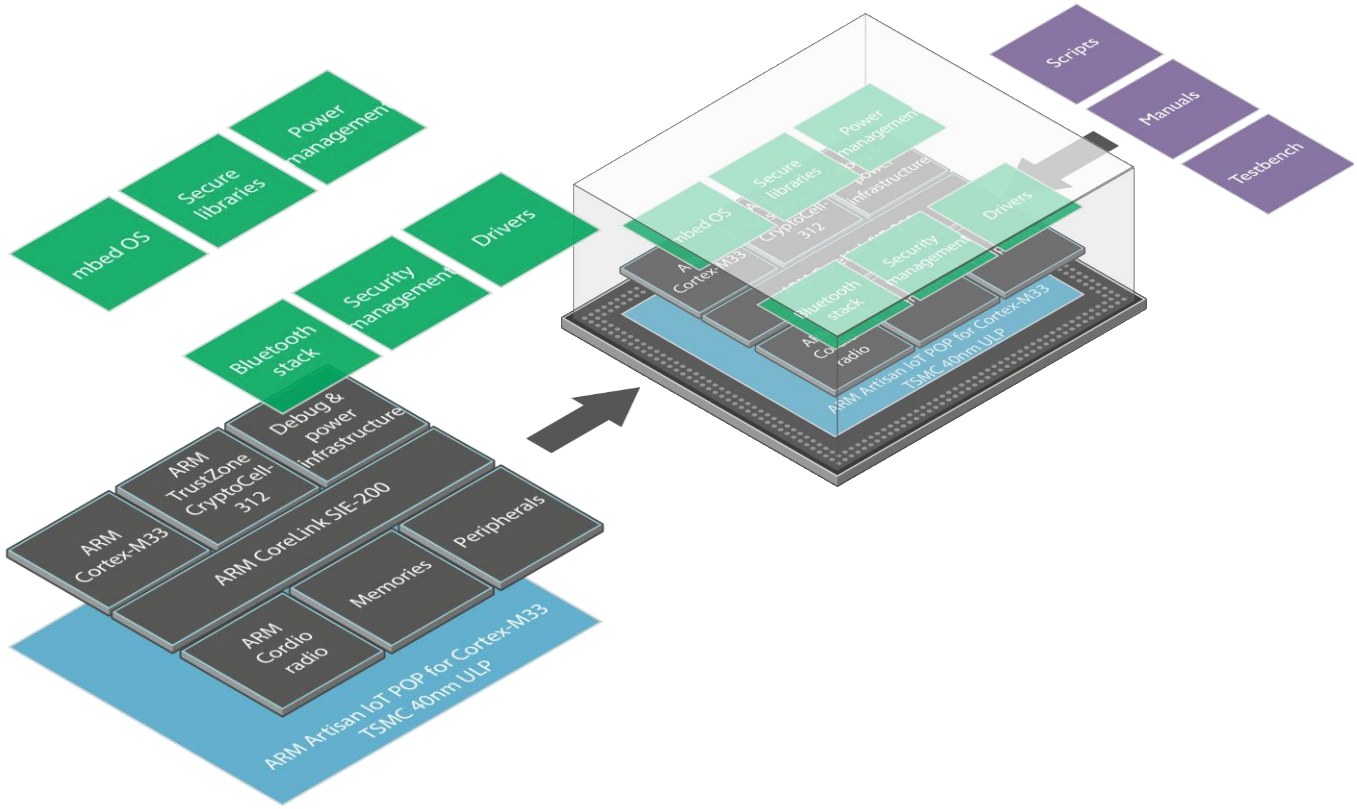
Highlights

- ARM® TrustZone® protection is expanded to the system with a pre-validated, ready to use, power-optimized IoT subsystem
- The ARM CoreLink™ SSE-200 subsystem is a flexible, dual ARM Cortex®-M33 system, running mbed OS and pre-integrated with ARM TrustZone CryptoCell and ARM Cordio® radio IP, embedding ARM's expertise in security and systems' architecture
- ARM accelerates IoT by aligning the ecosystem around this reference implementation, ready to build secure products fast

Accelerating design of secure SoCs for the IoT

Designing secure IoT products is a challenge. Security requires many additional features and capabilities that designers of constrained systems usually struggle to implement. CoreLink SSE-200 integrates ARMv8-M processors, TrustZone CryptoCell security IP and mbed OS to quickly and efficiently implement a secure solution.

Product overview



The CoreLink SSE-200 subsystem is the foundation on which SoC designers will build a new generation of secure IoT products. The design of these products requires expertise, time and a significant integration effort from the deepest hardware levels to the software applications. To address these challenges, ARM has mobilized its best experts to create an integrated solution, to verify it thoroughly and to package it in a way that allows product designers to quickly get a state-of-the-art IoT device.

The CoreLink SSE-200 subsystem is the fastest path to successful ARMv8-M silicon.

It builds on many new components developed by ARM:

- Cortex-M33 processors
- CoreLink SIE-200 System IP components and interconnect
- Power infrastructure
- New instruction caches
- Secure debug infrastructure
- TrustZone CryptoCell (optional)
- Cordio radio (optional) for Bluetooth low-energy and/or 802.15.4 connectivity

CoreLink SSE-200 also integrates software components:

- mbed OS
- Cordio Bluetooth stack
- Secure libraries from the TrustZone CryptoCell
- Various drivers and power management features.

To ensure fast integration of the subsystem in a SoC, a set of scripts and manuals make configuration and implementation easier. Since the CoreLink SSE-200 subsystem is a fully verified IP, there is no need to spend expensive verification time to check its internal behavior, designers can just trust it and concentrate on the integration work.

Complementing the subsystem, a fast model allows software developers to start working right away, and an FPGA platform can be used to prototype the system and further speed-up the development cycle.

The CoreLink SSE-200 subsystem contains many configuration options, making it flexible enough to adapt to very different needs. It also features an advanced and customizable power control infrastructure, with several configurable power domains to enable the low-power needs of the most advanced IoT applications. Its asymmetric dual-core architecture boosts the processing power by a factor of up to 32 when needed, while keeping an ultra-low power consumption during background processing and deep-sleep mode.

Design teams migrating to the new Cortex-M33 processor can take advantage of the CoreLink SSE-200 subsystem, eliminating the need to perform the core subsystem integration work, thus saving 6-to-12 months in their development cycles. This enables design teams to concentrate on integration of value-adding features and architectural innovations for designing the most innovative and secure SoCs for IoT.