CoreLink SIE-200: A secure, low power foundation for IoT nodes

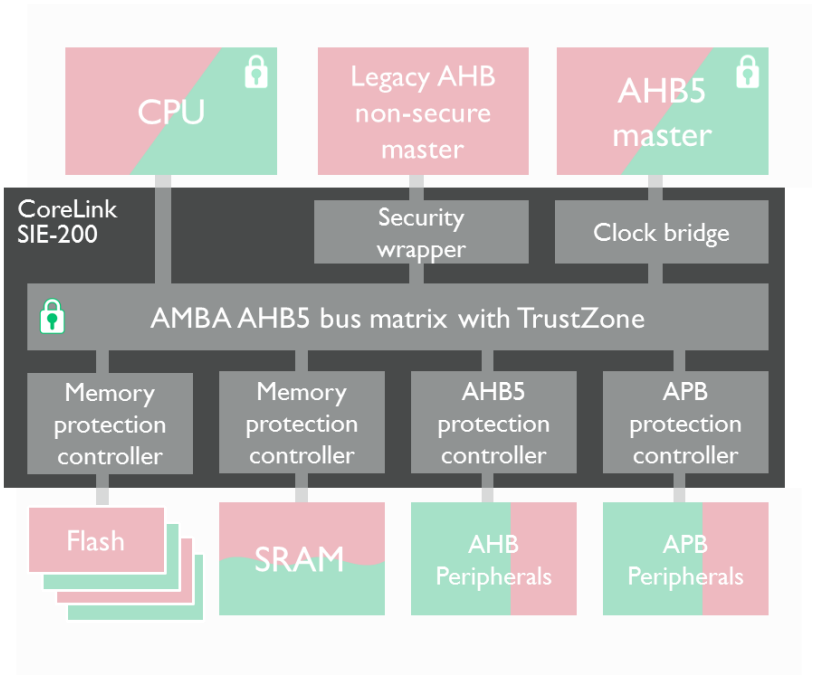
Highlights

- ARM® CoreLink™ SIE-200 extends ARM TrustZone® for ARMv8-M to the rest of the system for the next-generation of secure IoT devices
- Comprehensive mix of backplane IP to efficiently secure memory and peripherals
- Configurable interconnect and TrustZone controllers enable designers to target multiple IoT applications with an optimized ARMv8-M system
- Reduce time-to-market and cost in designing secure systems. CoreLink SIE-200 is pre-verified with ARM v8-M processors, enabling designers to focus on system differentiation and value-add.

Addressing system-level security

In order to maximize the benefits of TrustZone in the ARMv8-M architecture, a holistic approach to system security is a must. Security in IoT is more than just the processor, it requires an approach that protects the entire system and allows secure connectivity all the way from the device to the cloud. The combination of the new ARMv8-M architecture and AMBA® 5 AHB5 protocol provides a new security framework to address system security in microcontrollers. Architects need to quickly adopt to deliver products to catch the fast-moving IoT wave. Furthermore, security is complex and designers need building blocks they can trust to achieve stringent security requirements for their designs.

Product overview



CoreLink SIE-200 provides IP blocks built on top of the AMBA 5 AHB5 interface that extends TrustZone security to the system. The interconnect and TrustZone controllers provide a hardware-enforced isolation between secure and non-secure applications. The interconnect is configurable to support multiple system architectures, enabling designers to tailor each design to suit a specific application.

As CoreLink SIE-200 is based on the AHB5 protocol, it enables per-transaction security signaling through the system. This allows for hardware-assisted security partitioning of the system with efficient use of memory and peripherals across secure and non-secure applications. Advanced power

management features based on the AMBA Low Power Interface enable parts of an MCU to be powered down when not in use, allowing for longer battery life.

Software programmable TrustZone controllers provide hardware enforced partitioning of system resources (memory and peripherals) that can be efficiently and securely shared between secure and non-secure applications.

CoreLink SIE-200 IP provides the lowest-risk route to building ARMv8-M SoCs. The CoreLink SIE-200 IP is co-developed and co-tested with ARMv8-M processors. The architecture of the TrustZone controllers in CoreLink SIE-200 provide compatibility with the ARMv8-M software and tools ecosystem including support from Keil® MDK, ARM Socrates™ IP Tooling, ARM mbed™ OS, and multiple RTOS.

Partner quotes

"Security and trust are of paramount importance for IoT devices," said Mark Cox, Director IoT Platform Group, Analog Devices. "The Cortex-M33 processor puts a TrustZone security foundation into the heart of the processor and CoreLink SIE-200 extends this across the entire SoC. This allows us to strengthen SoC security in the easiest, most energy-efficient way for connected devices."