# AHB Secure Subsystem - ARM Cortex M3

## Overview

The Silvaco Secure AHB Performance Subsystem is a high-performance AHB subsystem that allows for a high level of hardware and software security. It integrates a security-conscious processor, the ARM Cortex-M3, with a security-conscious low power high-performance subsystem. Everything is pre-integrated with the necessary AHB and APB IP cores needed to run a small software kernel or a Real Time Operating System (RTOS). This subsystem is ideal for any deeply embedded system that requires enhanced security and protection from cyber-attacks and intrusions, such as IoT, smart sensors, smart controllers, and mixed signal devices.

Security in the Cortex-M3 is based on the MPU, Handler Mode, and privilege level. There are 8 memory ranges supported by the MPU and, it only regulates one Master component component - the processor - in a multi-Master component system. To prevent additional Master components from violating system integrity, the Secure AHB Subsystem adds the following IP

- Secure AHB Fabric
- SRAM Programmable Memory MPU
- ROM Parameterized Memory MPU

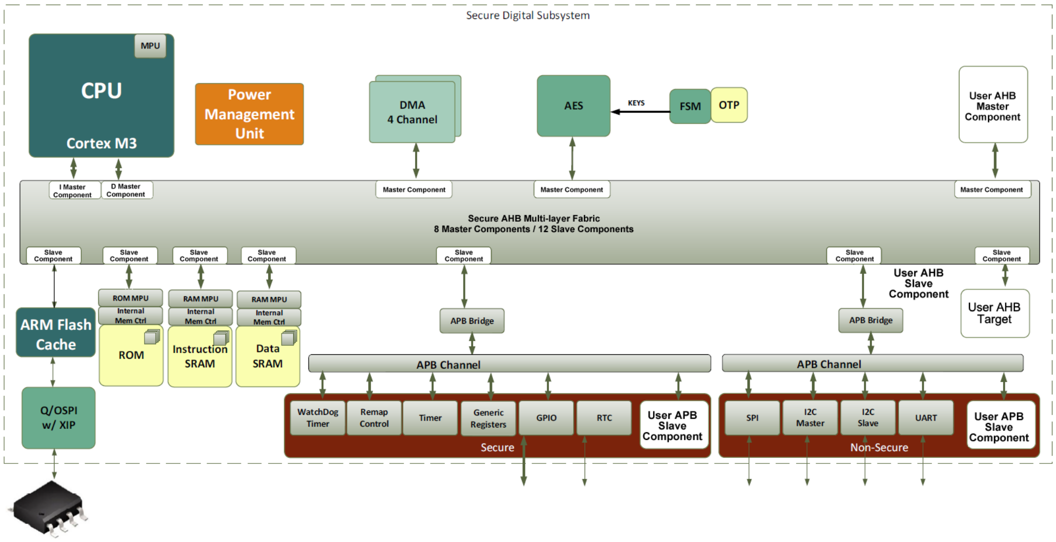
The Secure AHB Fabric connects several AHB Master components (secure or non-secure) to several AHB Slave components (secure or non-secure) in a crossbar switch arrangement. In this system, only the processor can produce secure AHB transactions, and all other AHB Master components are designated as non-secure at all times. AHB Slave components are categorized by the Fabric as either secure or non-secure, depending on the level of protection that is desired. A special case exists for memories, which are designated as non-secure Slave components by the Fabric. Security enforcement for memories is performed instead by the SRAM Programmable Memory MPU and/or the ROM Parameterized Memory MPU. This arrangement provides for greater flexibility for each physical memory - each memory may be divided into secure and non-secure regions - and potentially reduces the number of memory instantiations in the system.

The Secure AHB Fabric & Memory MPUs can be used stand-alone, or in conjunction with the ARM Cortex-M3's Memory Protection Unit (MPU). The Secure Fabric can take care of all coarse memory security partitioning leaving more room in the MPUs for finer tuning.

The subsystem's AES core can be used to establish a Root of Trust, with ROM code authenticating and decrypting a program from serial flash memory. A dedicated state machine can perform a direct load of encryption keys from an OTP memory, so the keys are never available to the processor. After boot-up the AES, OTP, and even the ROM may be powered down if desired. Once the program is decrypted and loaded into memory, a hash signature in the boot header can be used to verify the code in memory before booting it.

Also included in the subsystem are Quad (or Octal) SPI – Serial Flash Controller, AHB Multi-Layer Fabric, Direct Memory Access (DMA) controller, and Power Management (PMU) IP blocks. The subsystem is easily extended to add other user IP cores. The Q/OSPI performance may optionally be accelerated with ARM's Flash Cache IP, which is already pre-integrated into the subsystem.

Secure AHB Performance Subsystem – CM3



## Target Applications

- IoT Edge Devices
- Mixed Signal Digital - MEMS
- Smart Sensors, Smart Metering, Smart Lighting
- Health Monitors
- Surveillance, Home Automation, Smart Thermostats
- Machine/Motor Control, System Health Monitoring

## Processor Options

- ARM Cortex-M3 with low power logic, JTAG, MPU
- Optional Instruction/Data Mux (Von Neuman or Harvard Architecture)
- Optional ARM Flash Cache (order separately from ARM)

## Infrastructure

- CPU
- Secure AHB Bus Matrix / Decode – 8 master component s, 12 slave components
- AHB to APB Bridge (2)
- JTAG

## Standard Peripherals

- 8,16,32-bit Internal SRAM Controller with MPU
- ROM with MPU
- Power Management Unit
- DMA (4 channels)
- AES with optional secure key loader
- Windowed Watchdog Timer
- Timers (2)
- Remap Register
- Real-Time Clock

## Configurable Peripherals

- Secure AHB Fabric Interconnect
- GPIO (width, interrupt capability)
- I2C Master component
- I2C Slave component
- SPI Master component / Slave component
- Quad SPI Master component / Slave component (Octal SPI Controller optional)
- 16550 UART

## Hardware Security Features

- ARM Memory Protection Unit (MPU) & Privilege level
- SRAM & ROM MPUs
- AES H/W Encryption/Decryption
- Keys for AES can be in NV or OTP memory and directly loaded into AES registers (No processor access)
- AHB Fabric is parameterized so each Controller and Target can be designated as secure or non-secure
- If a non-secure AHB Controller attempts to access a secure AHB Target, the access is blocked, bus info is captured, and an interrupt can be generated

## Software

- An RTOS (such as FreeRTOS) may be used
- Secure Flash Loader, Boot Loader
- Examples using AES, Secure Fabric, and MPU
- Interrupt and Fault Handlers
- Use of Main and Process Stacks
- Supervisory Call (SVC) examples
- Example test code for all IP Cores

## Deliverables

- Verilog RTL source code
- Test bench with test suites
- Documentation including User's Guide and Integration Guide
- Technology-independent synthesis constraints
- C software example projects

For more information, please contact us at ip@silvaco.com.

SILVACO

HEADQUARTERS
4701 Patrick Henry Drive, Bldg #23
Santa Clara, CA 95054

| | |
|---|---|
| NORTH AMERICA | sales@silvaco.com |
| BRAZIL | br_sales@silvaco.com |
| EUROPE | eusales@silvaco.com |
| JAPAN | jpsales@silvaco.com |
| KOREA | krsales@silvaco.com |
| TAIWAN | twsales@silvaco.com |
| SINGAPORE | sgsales@silvaco.com |
| CHINA | cn_sales@silvaco.com |

WWW.SILVACO.COM