# ARM® CoreLink™ SSE-200 Subsystem

**Revision: r0p0**

## Technical Overview

**Beta**

ARM®


ARM DTO 0051A (ID022717)

# ARM CoreLink SSE-200 Subsystem
## Technical Overview



### Release Information

The following changes have been made to this book.

**Change history**

| Date | Issue | Confidentiality | Change |
|---|---|---|---|
| 20 December 2016 | A | Non-Confidential | First release for r0p0 Beta |

### Proprietary Notice



ARM Limited. Company 02557590 registered in England.

110 Fulbourn Road, Cambridge, England CB1 9NJ.

LES-PRE-20349

### Confidentiality Status

This document is Non-Confidential. The right to use, copy and disclose this document may be subject to license restrictions in accordance with the terms of the agreement entered into by ARM and the party that ARM delivered this document to.

### Product Status

The information in this document is for a Beta product, that is a product under development.

### Web Address

`http://www.arm.com`

# Contents
# ARM CoreLink SSE-200 Subsystem Technical Overview

# Preface

This preface introduces the *ARM® CoreLink™ SSE-200 Subsystem Technical Overview* (TO). It contains the following sections:

## About this book

This book is for the *ARM® CoreLink™ SSE-200 Subsystem* (SSE-200). It describes the hardware and software for the system.

### Product revision status

The r*n*p*n* identifier indicates the revision status of the product described in this book, where:

**r*n*** Identifies the major revision of the product.

**p*n*** Identifies the minor revision or modification status of the product.

### Intended audience

This book is written for hardware or software engineers who want an overview of the functionality in the CoreLink SSE-200 Subsystem.

### Using this book

This book is organized into the following chapters:

**Chapter 1 *Subsystem Overview***

Read this for a description of the SSE-200 subsystem.

**Chapter 2 *Hardware***

Read this for a description of the SSE-200 hardware.

**Chapter 3 *Software***

Read this for a description of the software available for use with the SSE-200 subsystem.

**Appendix A *Revisions***

Read this for a description of the technical changes between released issues of this book.

The *ARM Glossary* is a list of terms used in ARM documentation, together with definitions for those terms. The *ARM Glossary* does not contain terms that are industry standard unless the ARM meaning differs from the generally accepted meaning.

The *ARM Glossary* is available on the ARM Infocenter at http://infocenter.arm.com/help/topic/com.arm.doc.aeg0014-/index.html.

### Typographical conventions

The typographical conventions are:

***italic*** Highlights important notes, introduces special terminology, denotes internal cross-references, and citations.

**bold** Highlights interface elements, such as menu names. Denotes signal names. Also used for terms in descriptive lists, where appropriate.

`monospace` Denotes text that you can enter at the keyboard, such as commands, file and program names, and source code.

`mono`space Denotes a permitted abbreviation for a command or option. You can enter the underlined text instead of the full command or option name.

| | |
|---|---|
| *monospace italic* | Denotes arguments to monospace text where the argument is to be replaced by a specific value. |
| **monospace bold** | Denotes language keywords when used outside example code. |

## Additional reading

This section lists publications by ARM and by third parties.

See Infocenter, http://infocenter.arm.com for access to ARM documentation.

See www.arm.com/cmsis for embedded software development resources including the *Cortex® Microcontroller Software Interface Standard* (CMSIS).

See ARM mbed™ platform, https://mbed.org/ for information on the mbed tools including mbed OS and online tools.

### ARM publications

This book contains information that is specific to this product. See the following documents for other relevant information:

- *ARM® CoreLink™ SIE-200 System IP for Embedded Technical Reference Manual* (ARM DDI 0571).

The following confidential books are only available to licensees or require registration with ARM:

- *ARM® CoreLink™ SSE-200 Subsystem Technical Reference Manual* (ARM DDI 0574).
- *ARM®v8-M Architecture Reference Manual* (ARM DDI 0553).
- *ARM® Cortex®-M33 Processor Technical Reference Manual* (ARM 100230).
- *ARM® CoreSight™ Components Technical Reference Manual* (ARM DDI 0314).
- *AMBA® Low Power Interface Specification ARM Q-Channel and P-Channel Interfaces* (ARM IHI 0068).
- *ARM® Debug Interface v5 Architecture Specification* (ARM IHI 0031).
- *ARM® Embedded Trace Macrocell Architecture Specification* (ARM IHI 0014).
- *ARM® AMBA® 5 AHB Protocol Specification* (ARM IHI 0033).
- *ARM® AMBA® APB Protocol Specification* (ARM IHI 0024).

## Feedback

ARM welcomes feedback on this product and its documentation.

### Feedback on this product

If you have any comments or suggestions about this product, contact your supplier and give:

- The product name.
- The product revision or version.
- An explanation with as much information as you can provide. Include symptoms and diagnostic procedures if appropriate.

### Feedback on content

If you have comments on content then send an e-mail to `errata@arm.com`. Give:

- the title
- the number, ARM DTO 0051A
- the page numbers to which your comments apply
- a concise explanation of your comments.

ARM also welcomes general suggestions for additions and improvements.

**Note**

ARM tests the PDF only in Adobe Acrobat and Acrobat Reader, and cannot guarantee the quality of the represented document when used with any other PDF reader.

# Chapter 1
# **Subsystem Overview**

This chapter introduces the ARM CoreLink SSE-200 Subsystem. It contains the following sections:

## 1.1 About the SSE-200

The SSE-200 Subsystem provides a starting point for a product in the *Internet of Things* (IoT) and embedded market segments.

The SSE-200 Subsystem drives system architecture and software standardization, and was developed to provide a high-performance computing subsystem that encompasses leading-edge Cortex-M and TrustZone technologies. The solution consists of hardware, software, and software tools to enable the rapid development of IoT System on Chip (SoC) solutions

The SSE-200 provides the following pre-assembled elements to use as the basis of an IoT SoC:

- Two Cortex®-M33 processors.
- Bus matrix for internal and expansion buses.
- System controller.
- CoreSight® Debug and Trace.
- CoreLink™ SIE-200 and CMSDK components.
- SRAM memory.
- Power, clock, and reset control infrastructure.

**Note**

- The SSE-200 is complemented by SW libraries that are integrated with the mbed operating system.
- The provided system components only form part of the finished SoC and ARM expects that the system designers will extend and customize the subsystem for their application requirements.

The following figure shows a block diagram of the SSE-200 elements:

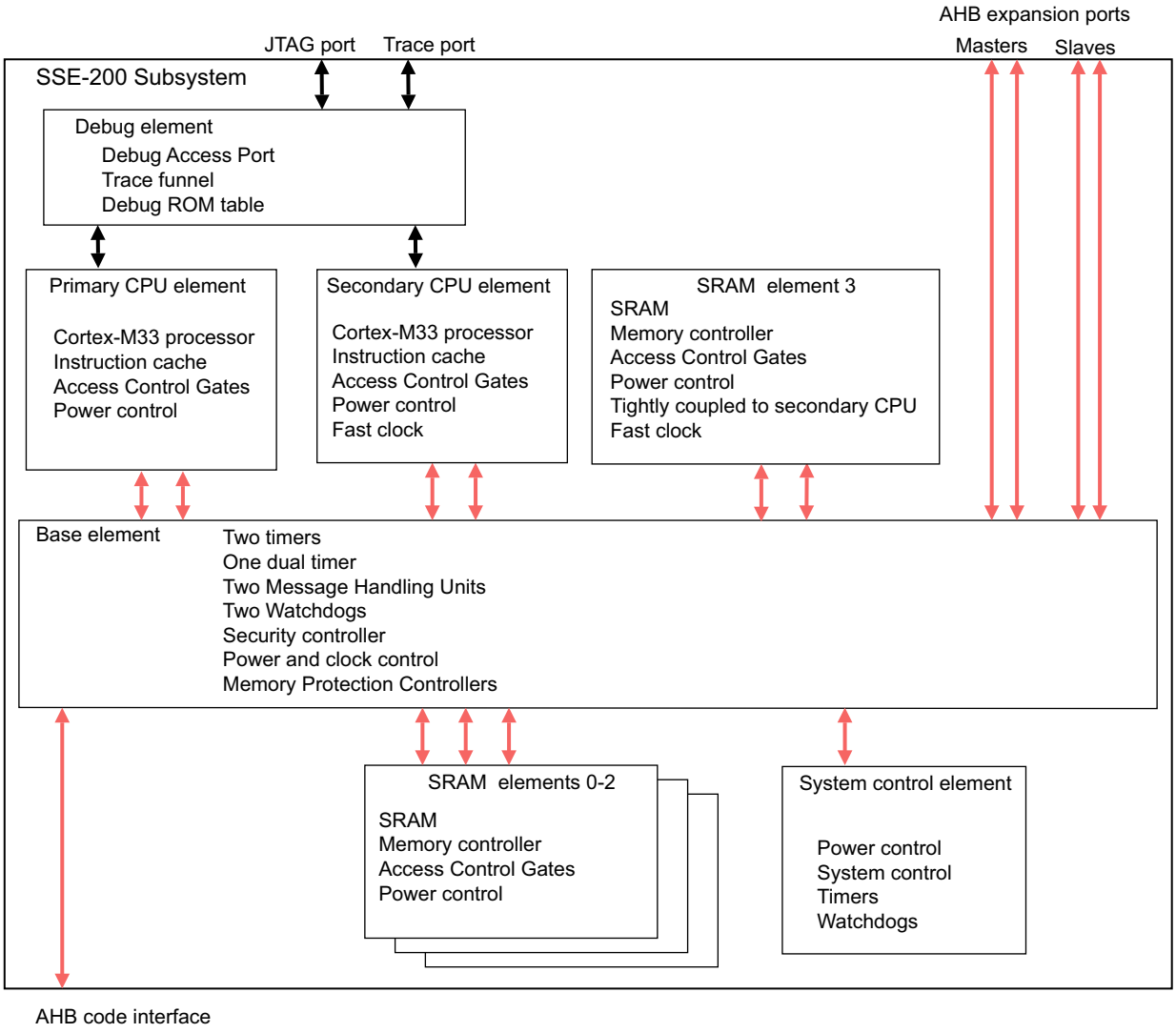


**Figure 1-1 SSE-200 block diagram**

### 1.1.1 About IoT System on Chip implementations

The SSE-200 Subsystem must be extended to create an IoT SoC. A complete system typically contains the following components:

**SSE-200 Subsystem**

The SSE-200 Subsystem consists of two Cortex®-M33 processors and associated bus, debug, controller, and interface logic supplied by ARM.

**Reference system memory and peripherals**

SRAM is part of the SSE-200, but a SoC will require additional memory, control, and peripheral components beyond the minimum subsystem components. Flash memory, for example, is not provided with the SSE-200.

**Communication interface**

The endpoint will have some way of communicating with other nodes or masters in the system. This could be wireless (WiFi, cellular, 802.15.4 ZigBee, or Bluetooth) or a wired connection.

**Sensor or control component**

To be useful as an endpoint, the reference design is typically extended by adding sensors or control logic such as, for example, temperature input or motor speed control output.

**Software development environment**

ARM provides a complete software development environment which includes the mbed operating system, ARM or GCC compilers and debuggers, and firmware.

Any custom peripherals typically require corresponding third-party firmware that can be integrated into the software stack.

Figure 1-2 shows a block diagram of the hardware and software in an IoT system:

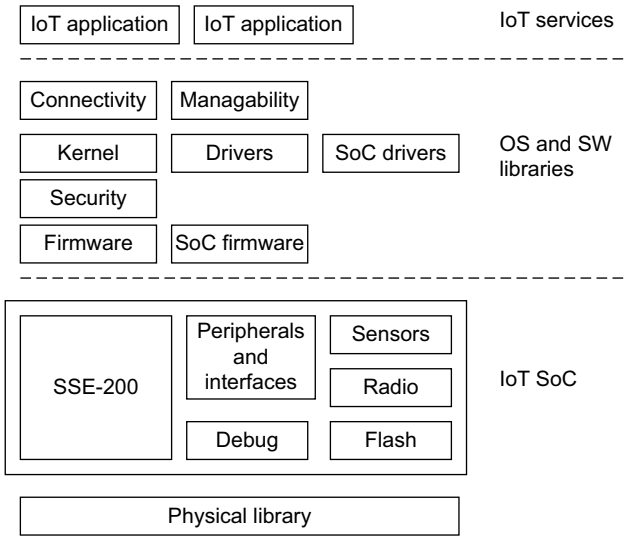


**Figure 1-2 HW and SW solution**

## 1.2 Product deliverables

The CoreLink SSE-200 Subsystem encompasses both hardware and software deliverables.

### 1.2.1 Hardware deliverables

The hardware deliverables include the following:

- SSE-200 Verilog RTL that includes the SSE Subsystem proprietary logic, and elements from the CoreLink SIE-200 System IP for Embedded, the Cortex-M0 System Design Kit, and the CoreLink LPD-500 Low Power Distributor.
- RTL build scripts that automate the process of instantiating a complete subsystem with the licensed options and selected configuration.
- An *Out-of-Box* (OoB) RTL testbench that includes test vectors.
- Static Timing Constraints for the major IP components.
- The *ARM® CoreLink™ SSE-200 Subsystem Technical Reference Manual*.
- The *CoreLink SSE-200 Subsystem Configuration and Integration Manual*. This document assists with the implementation, integration, and interfacing of the SSE-200 into a larger System-on-Chip (SoC).
- Verification reports.

### 1.2.2 Software deliverables

The software deliverables include the following:

- ARM mbed OS. This is an open-source embedded operating system designed for IoT solutions.
- Platform hardware-adaptation layer code required in addition to the open-source code.
- Device drivers and specific libraries.
- Shell scripts to sync, build, and run the software.

### 1.2.3 Documentation

The following documents are supplied with the SSE-200:

**Technical Overview**

The *Technical Overview* (TO) describes the functionality of the SSE-200 Subsystem.

**Technical Reference Manual**

The *Technical Reference Manual* (TRM) describes the functionality and the effects of functional options on the behavior of the processor. It is required at all stages of the design flow. The choices made in the design flow can mean that some behavior described in the TRM is not relevant. If you are programming the processor, additional information must be obtained from:

- The implementer to determine the build configuration of the implementation.
- The integrator to determine the pin configuration of the device that you are using.

### Configuration and Integration Manual

The *Configuration and Integration Manual* (CIM) describes the available build configuration options and related issues in selecting them, and how to implement, connect, optimize, and test a subsystem in a System-on-Chip (SoC) design.

## 1.3 Compliance

The SSE-200 complies with, or includes components that comply with, the following specifications:

- *ARM Architecture*.
- *Debug*.
- *Interrupt controller architecture*.
- *Advanced Microcontroller Bus Architecture*.

This Technical Reference Manual complements the TRMs for included components, architecture reference manuals, architecture specifications, protocol specifications, and relevant external standards. It does not duplicate information from these sources.

### 1.3.1 ARM Architecture

The Cortex®-M33 processor in the SSE-200 implements the ARMv8-M architecture with Thumb-2 technology.

See the *ARM®v8-M Architecture Reference Manual* for more information.

#### Security

The ARM® TrustZone® technology in the ARMv8-M architecture enables memory and peripheral spaces to be partitioned into secure and non-secure regions. No access to secure assets is possible from the non-secure world.

### 1.3.2 Debug

The SSE-200 implements the ARM CoreSight debug interface.

See the *ARM® CoreSight® Components Technical Reference Manual* for more information.

### 1.3.3 Interrupt controller architecture

The SSE-200 implements the ARM *Nested Vectored Interrupt Controller* (NVIC).

See the *ARM® Cortex®-M33 Processor Technical Reference Manual* for more information.

### 1.3.4 Advanced Microcontroller Bus Architecture

The SSE-200 complies with the:

- *Advanced High Performance Bus* (AHB5) protocol.

  See the *ARM® AMBA® 5 AHB Protocol Specification*.
- *Advanced Peripheral Bus* (APB4) protocol.

  See the *ARM® AMBA® APB Protocol Specification*.

The SSE-200 contains components that use ARM® TrustZone® technology that supports the ARMv8-M security extension for secure and non-secure states.

# Chapter 2
# **Hardware**

This chapter describes the functionality of the SSE-200.

It contains the following sections:

## 2.1 About the hardware components

The SSE-200 contains the following hardware components:

- Two Cortex®-M33 processors:
  - Optional FPU and DSP extensions and ETM.
  - Integrated instruction cache.

  For more information see the *ARM® Cortex®-M33 Processor Technical Reference Manual*.
- CoreSight® debug system with configurable Secure Debug and Trace.
- Secure AMBA® interconnect:
  - AHB5 bus matrix.
  - AHB5 TrustZone® *Memory Protection Controller* (MPC).
  - AHB5 TrustZone *Peripheral Protection Controller* (PPC).
  - AHB5 *Exclusive Access Monitor* (EAM).
  - AHB5 *Access Control Gates* (ACG).
  - AHB5 to APB Bridges.
  - Expansion AHB5 master and slave buses (two each).
- Memory system:
  - Static memory controllers for the four banks of SRAM.
  - AHB5 master bus to external code memory.
- Security components:
  - *Implementation Defined Attribution Unit* (IDAU).
  - Secure expansion ports.
  - System security controller.
  - System controller.
- Secure APB peripherals:
  - Three general-purpose timers with configurable security. (One timer is on the 32KHz (32,768Hz) domain and two are on the fast SYSCLK PD_SYS domain.)
  - A *Cortex-M System Design Kit* (CMSDK) dual timer with configurable security.
  - Three watchdog timers with fixed security. One secure watchdog is on the 32KHz domain and one secure and one non-secure is on the SYSCLK PD_SYS domain.
  - Two *Message Handling Units* (MHUs) allows software to raise interrupts.
- *Power Policy Units* (PPU) and CoreLink LPD-500 Low Power Distributor.

## 2.2 Top-level system partitioning

The SSE-200 components are organized into the following blocks or elements:

- Base element.
- CPU elements.
- Debug element.
- System control element.
- SRAM elements.

The top-level view of the SSE-200 Subsystem elements and the AHB5 and APB bus interconnections is shown in the following figure:

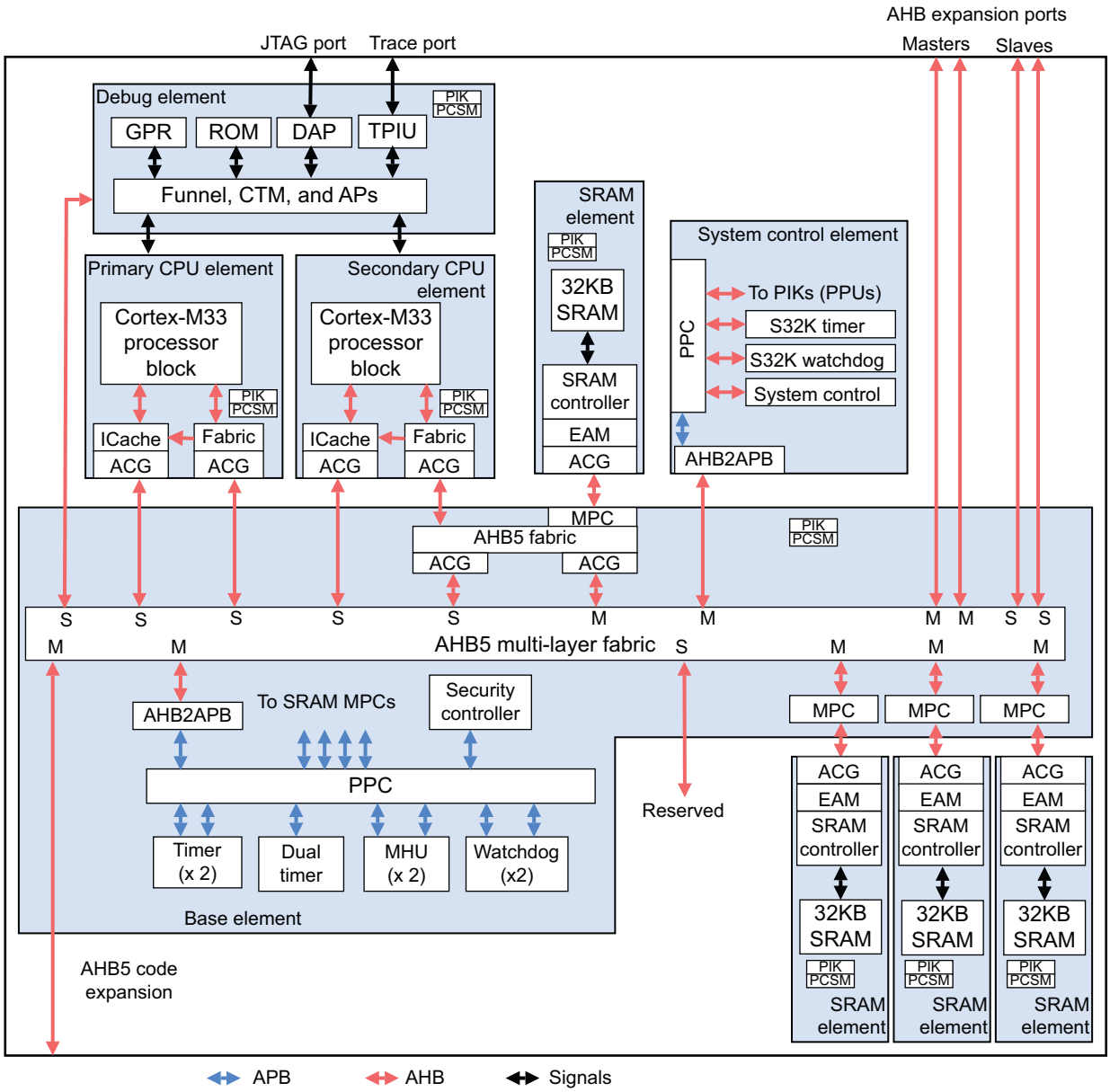


**Figure 2-1 Top-level element interconnections**

### 2.2.1 Configuration options

Some processor and system options are set by configuration parameters, for example:

- Reset value for the vector table offset addresses for both processors.
- CPU IDs.
- Cache size.
- SRAM size.
- Number of expansion interrupts for the processors and the wakeup controllers.
- Interrupt latencies.
- Presence of Floating Point Units and support for DSP extension instructions.
- Debug resources.
- Clock divider values.

### 2.2.2 Interface signals

The SSE-200 has the following interfaces at the boundary of the subsystem to allow customization by customers:

- Clock and reset signals.
- Processor-related signals:
  - Processor control and status.
  - Interrupts.
  - Configuration signals.
- Base element:
  - Two AHB5 master and two AHB5 slave expansion buses.
  - AHB5 code expansion bus.
- System control:
  - Static configuration signals.
  - Power control expansion interfaces.
  - External Wakeup Controller interrupt inputs.
- Debug and Trace:
  - Debug access.
  - Timestamp.
  - Cross Trigger Channel.
  - Debug APB expansion.
  - ATB Trace.
  - Debug authentication.
- Top-level static configuration signals.

## 2.3 CPU elements

There are two Cortex-M33 cores in the SSE-200:

- The primary core in the CPU0 element is synchronous to main interconnect and runs the operating system.
- The secondary core in the CPU1 element contains an FPU and DSP. It is synchronous to the main clock, but runs *N* times faster.

The Cortex-M33 processor has the following features:

- Three-stage pipeline.
- ARMv8-M Mainline profile.
- TrustZone-M Security.
- Eight SAU entries each.
- 16 MPU regions with eight secure and eight non-secure.
- IDAU defining high-level security memory mapping.

Each CPU has configuration parameters that can be set in the design stage to specify the processor features including:

- If the *Floating Point Unit* (FPU) is present.
- If the Digital Signal Processing extension instructions are included.
- If the coprocessor interface is present.
- The number of non-secure and secure MPU regions.
- The number of security attribution unit regions.
- The number of user interrupts
- The interrupt priority and interrupt latency.
- Debug resources and trace support.
- If the Wakeup Interrupt Controller is present.

## 2.4 Base element

The Base element provides the following features:

- A multilayer AHB5 interconnect for all of the subsystem elements and expansion buses.

  A separate AHB5 fabric interface to an SRAM element which functions as Tightly-Coupled Memory to the secondary processor.

- A Memory Protection Controller for four SRAM elements.

  The secondary processor, the multilayer AHB5 fabric, and one SRAM element are interconnected to allow the SRAM to function as *Tightly-Coupled Memory* (TCM) on the secondary processor data bus.

- An AHB to APB bus converter and TrustZone Peripheral Protection Controller for:
  - Two CMSDK Timers.
  - One CMSDK Dual Timer.
  - One CMSDK Watchdog timers.
  - Message Handling Units that allow inter-processor communication between the cores.

- Four AHB5 expansion ports:
  - Two slave expansion ports.
  - Two master expansion ports.

- A dedicated AHB5 interface to access code memory in embedded Flash or ROM.
- A security controller with expansion support.
- A single voltage domain and power-gated region.
- Two synchronous clock domains to allow having a fast and a slow core.

## 2.5 SRAM elements

Each SRAM element has the following features:

- One bank of single port SRAM, configurable as 8K, 16K, 32K, or 64K bytes.

  There are four banks, so the total SRAM size is four times the bank size.
- Zero clock-cycle latency.
- Single voltage domain and multiple power gated regions.
- ON/OFF/MEM_RET power policy support which enables complete power down and data retention.
- Access control for power and clock domain crossing.
- AHB5 interface with exclusive access support.
- Independent memory power control.

A Memory Protection Controller in the base element manages secure access.

The last bank of SRAM is the *Data Tightly Coupled Memory* (DTCM) that runs at the same speed as secondary core and provides high throughput.

## 2.6 System control element

The System control element provides the following features:

- AHB5 to APB protocol conversion with a Peripheral Protection Unit.
  See the *ARM® CoreLink™ SIE-200 System IP for Embedded Technical Reference Manual*.
- System control registers:
  - SPIDEN, SPNIDEN controls and overrides.
  - Last reset reason status.
  - General purpose retention register for general use.
- Reset generation.
- Always on components that run on the slow clock (for example 32KHz):
  - Watchdog reset and interrupt generation.
  - Timer.
- Power control:
  - *Power Dependency Control Matrix* (PDCM) generates external wakeup for elements with PPU and for expansion power domains.
  - Access to *Power Policy Units* (PPUs) within *Power Integration Kits* (PIKs).

    **Note**

    Power control is customizable by the customer to integrate control and communication with SSE-200 components and components outside the SSE-200 Subsystem. See also *Power control infrastructure* on page 2-10.
- Clock generation and control:
  - Clock divider and multiplexing settings.
  - Clock and reset override controls.
  - External Wakeup Interrupt Control to capture interrupts and wake up the **MAINCLK** and processors in hibernation on interrupt.
  - Generation of **FCLK** and **SYSCLK** from **MAINCLK** with clock dividers.
  - Dynamic hierarchical clock gating for PPU clocks.

## 2.7 Debug element

The Debug element provides the following features and interfaces:

- JTAG and *Serial Wire Out* (SWO) Debug.
- Single *Debug Access Port* (DAP) shared between both processors.
- Shared TPIU.

  The DAP and TPIU are implemented inside the expansion block.
- CTM and CTI.
- Timestamp Generator.
- Granular Power Requester to allow the debugger to selectively request parts of the SSE-200 to turn on.

The SWJ-DP is a combined JTAG-DP and SW-DP that enables you to connect either an SWD or JTAG probe to a target. It is a standard CoreSight debug port.

To make efficient use of package pins, the JTAG pins use an auto-detect mechanism that switches between JTAG-DP and SW-DP depending on which probe is connected.

The Cortex-M33 TPIU is an optional component that acts as a bridge between the on-chip trace data from the *Embedded Trace Macrocell* (ETM) and the *Instrumentation Trace Macrocell* (ITM), with separate IDs, to a data stream. The TPIU encapsulates IDs where required, and the data stream is then captured by a *Trace Port Analyzer* (TPA). The Cortex-M33 TPIU is specially designed for low-cost debug.

**Note**

The default implementation reuses the TPIU and SWJ/DP from the CPU package. This configuration is sufficient for basic use.

An example of debug integration beyond the SSE-200 Subsystem level is provided with the product deliverables.

## 2.8 Power control infrastructure

Low-power operation is essential for IoT endpoint devices that might rely on a battery or on harvested energy.

To control power usage, the Subsystem has multiple voltage domains, multiple power-gated regions, and supports clock-gating.

The subsystem supports the following power-control features:

- Multiple power-gated regions.

  A *Power Dependency Control Matrix* (PDCM) enables configuring the relationship between each power domain.

  *Power Integration Kits* (PIKs) provide access to the *Power Policy Units* (PPUs) that give give technology-independent power control of the domain.

  Integration of Q-channel and P-channel infrastructure components tie the key IP blocks in each power domain to the PPU.

- Low-power, autonomous wake, and sleep modes.
- Hierarchical clock-gating across the subsystem

# Chapter 3
# **Software**

Read this chapter for a description of the software available for use with the SSE-200.

It contains the following sections:

## 3.1 About the software

The SSE-200 Subsystem supports the following software deliverables:

- CMSIS compliant drivers.
- Flash programming support code (separate from mbed OS).
- Separately ported mbed OS which includes uVisor ported onto the SSE-200 Subsystem.
- Execution support for the SSE-200 *Fixed Virtual Platform* (FVP) and RTL simulators.
- Support for SSE-200 on MPS2 FPGA development platform.
- mbed OS driver support.
- Support for system security components (example, memory protection controllers).
- Support for example IO peripherals.

**Note**

For more information on mbed, see `www.mbed.com`.

## 3.2 Firmware

The Application Processor firmware consists of the code that is required to boot the subsystem up to the point where the OS execution starts.

The firmware contains the code that is required to:

- Set up the initial security environment.
- Support runtime processor power state control.
- Load mbed from boot media.

# Appendix A
# **Revisions**

This appendix describes the technical changes between released issues of this book.

**Table A-1 Issue A**

| Change | Location | Affects |
|---|---|---|
| First release | - | - |