Arm® CoreLink™ SSE-200 Subsystem for Embedded

Revision: r2p0

Technical Overview

arm

101123_0200_00_en

Arm® CoreLink™ SSE-200 Subsystem for Embedded

Technical Overview

Release Information

Document History

Issue	Date	Confidentiality	Change
A	20 December 2016	Non-Confidential	First release for r0p0 Beta (Arm DTO 0051)
0100-00	26 September 2017	Non-Confidential	First release for r1p0 EAC (Arm 101123).
0200-00	11 July 2018	Non-Confidential	First release for r2p0 REL

Non-Confidential 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.

Unrestricted Access is an Arm internal classification.

Product Status

The information in this document is Final, that is for a developed product.

Web Address

http://www.arm.com

Contents
Arm® CoreLink™ SSE-200 Subsystem for Embedded Technical Overview

Appendix A Revisions

Preface

This preface introduces the *Arm® CoreLink™ SSE-200 Subsystem for Embedded Technical Overview*.

It contains the following:

About this book

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

Product revision status

The r*m*p*n* identifier indicates the revision status of the product described in this book, for example, r*1*p*2*, where:

r*m* Identifies the major revision of the product, for example, r1.

p*n* Identifies the minor revision or modification status of the product, for example, p2.

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
This chapter introduces the Arm CoreLink SSE-200 Subsystem for Embedded.

Chapter 2 Hardware
This chapter describes the functionality of the SSE-200.

Chapter 3 Software
This chapter describes the software available for use with the SSE-200.

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

Glossary

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.

See the *Arm® Glossary* for more information.

Typographic conventions

italic
Introduces special terminology, denotes 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.

<and>
: Encloses replaceable terms for assembler syntax where they appear in code or code fragments. For example:

```
MRC p15, 0, <Rd>, <CRn>, <CRm>, <Opcode_2>
```

SMALL CAPITALS
: Used in body text for a few terms that have specific technical meanings, that are defined in the *Arm® Glossary*. For example, IMPLEMENTATION DEFINED, IMPLEMENTATION SPECIFIC, UNKNOWN, and UNPREDICTABLE.

Timing diagrams

The following figure explains the components used in timing diagrams. Variations, when they occur, have clear labels. You must not assume any timing information that is not explicit in the diagrams.

Shaded bus and signal areas are undefined, so the bus or signal can assume any value within the shaded area at that time. The actual level is unimportant and does not affect normal operation.

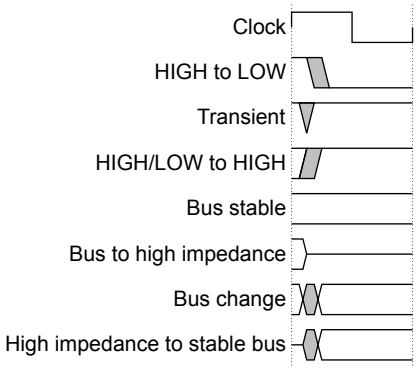

Figure 1 Key to timing diagram conventions

Signals

The signal conventions are:

Signal level
: The level of an asserted signal depends on whether the signal is active-HIGH or active-LOW. Asserted means:
- HIGH for active-HIGH signals.
- LOW for active-LOW signals.

Lowercase n
: At the start or end of a signal name denotes an active-LOW signal.

Additional reading

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

Arm publications

- *Arm® CoreLink™ SSE-200 Subsystem for Embedded Technical Reference Manual* (Arm 101104)
- *Arm® CoreLink™ SIE-200 System IP for Embedded Technical Reference Manual* (Arm DDI 0571).
- *Arm® Cortex®-M System Design Kit Technical Reference Manual* (Arm DDI 0479).
- *Arm® Cortex®-M33 Processor Technical Reference Manual* (Arm 100230).
- *Arm® Power Policy Unit Architecture Specification, version 1.1* (Arm DEN 0051).
- *Arm® CoreSight™ Architecture Specification, v2.0* (Arm IHI 0029).
- *Arm® CoreSight™ Components Technical Reference Manual* (Arm DDI 0314).
- *Arm® Embedded Trace Macrocell (ETMv4) Architecture Specification* (Arm IHI 0064).
- *Arm® AMBA® 5 AHB Protocol Specification* (Arm IHI 0033).
- *Arm® AMBA® APB Protocol Specification Version 2.0* (Arm IHI 0024).

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

- *Arm® CoreLink™ SSE-200 Subsystem for Embedded Configuration and Integration Manual* (Arm 100224).
- *Arm® CoreLink™ SSE-200 Subsystem for Embedded Release Note* (CG062-DC-06003).
- *Arm®v7-M Architecture Reference Manual* (Arm DDI 0403).
- *Arm®v8-M Architecture Reference Manual* (Arm DDI 0553).
- *Arm® Cortex®-M33 Processor Integration and Implementation Manual* (Arm 100323).
- *AMBA® Low Power Interface Specification, Arm® Q-Channel and P-Channel Interfaces* (Arm IHI 0068).
- *Arm® Debug Interface Architecture Specification ADIv5.0 to ADIv5.2* (Arm IHI 0031).
- *Arm® TrustZone® CryptoCell-312 Technical Reference Manual* (Arm 100774).

Other publications

None.

Feedback

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 *Arm CoreLink SSE-200 Subsystem for Embedded Technical Overview*.
- The number 101123_0200_00_en.
- If applicable, the page number(s) to which your comments refer.
- 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 for Embedded.

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.

This section contains the following subsections:

1.1.1 SSE-200 elements

The SSE-200 Subsystem for Embedded 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.
- AMBA AHB5 bus matrix for internal and expansion buses.
- System controller.
- Instruction cache.
- 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 software 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 extend and customize the subsystem for their application requirements.

1.1.2 SSE-200 block diagram

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

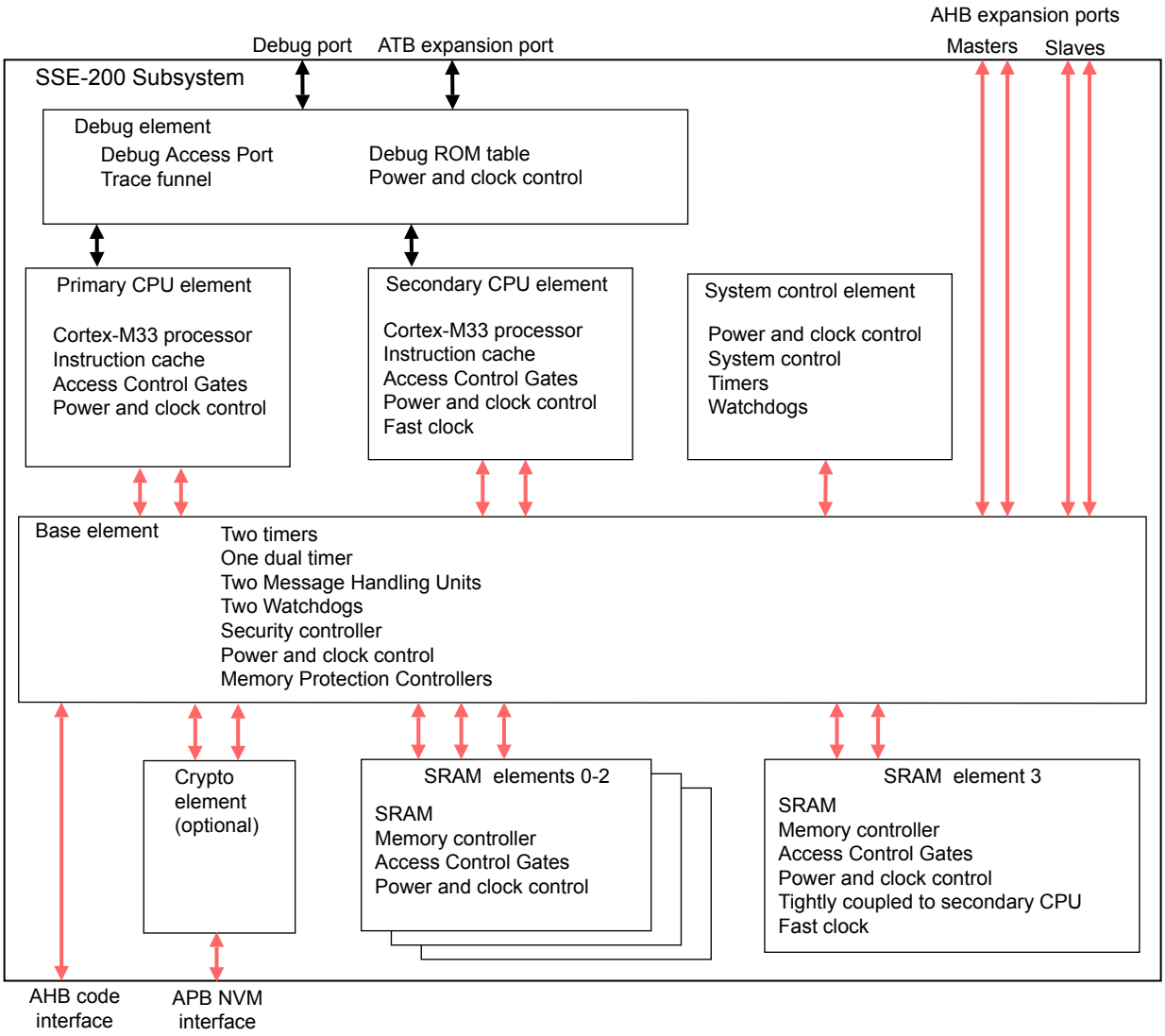

Figure 1-1 SSE-200 block diagram

1.1.3 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:

Compute subsystem

The SSE-200 Subsystem for Embedded 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 requires extra 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 has some way of communicating with other nodes or masters in the system. This could be wireless (WiFi, cellular, 802.15.4 ZigBee, Bluetooth, or Narrowband IoT) 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 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.

IoT hardware and software

The following figure shows a block diagram of the hardware and software in an IoT system:

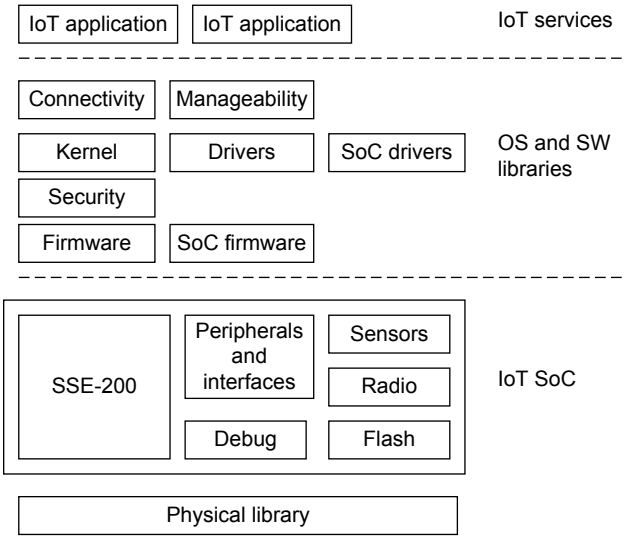

Figure 1-2 Hardware and software solution

1.2 Product deliverables

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

This section contains the following subsections:

1.2.1 Hardware deliverables

The hardware deliverables include the following:

- SSE-200 Verilog RTL that includes the SSE subsystem proprietary logic, and elements using 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 for Embedded Technical Reference Manual*.
- The *CoreLink™ SSE-200 Subsystem for Embedded 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.
- System level IP-XACT descriptions.
- UPF 2.0 power intent description.

1.2.2 Software

The separately available software includes the following:

- Arm Mbed OS. This is an open-source embedded operating system that is designed for IoT solutions.
- 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 that are made in the design flow can mean that some behavior that is 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:

- *1.3.1 Arm Architecture* on page 1-16.
- *1.3.2 Debug* on page 1-16.
- *1.3.3 Interrupt controller architecture* on page 1-16.
- *1.3.4 Advanced Microcontroller Bus Architecture* on page 1-16.

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.

For more information, see the following documents:

- *Arm® CoreSight™ Components Technical Reference Manual*.
- *Arm® Debug Interface Architecture Specification ADIv5.0 to ADIv5.2*.
- *Arm® CoreSight™ Architecture Specification, v2.0*.

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 AHB5 and APB4 protocols.

For more information, see:

- *Arm® AMBA® APB Protocol Specification*.
- *Arm® AMBA® 5 AHB 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.

1.3.5 Power Policy Unit architecture

The power domains in the SSE-200 are controlled by *Power Policy Units* (PPUs), which comply with the Arm PPU architecture.

See the *Arm® Power Policy Unit Architecture Specification, version 1.1* for more information.

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 *Floating-Point Unit* (FPU) and *Digital Signal Processor* (DSP) extensions (configurable).
  - *Embedded Trace Macrocell* (ETM).

  For more information, see the *Arm® Cortex®-M33 Processor Technical Reference Manual*.
- CoreSight debug system with configurable Secure Debug and Trace.
- Secure AMBA interconnect:
  - *Advanced High Performance Bus* (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 *Advanced Peripheral Bus* (APB) bridges.
  - Expansion AHB5 master and slave buses (two each).
- Memory system:
  - AHB5 multi-layer bus matrix.
  - Static memory controllers.
  - Multiple banks of SRAM.

    One bank of SRAM functions as *Tightly Coupled Memory* (TCM).
  - Instruction caches.
- Security components:
  - TrustZone CryptoCell-312 (optional).
  - *Implementation Defined Attribution Unit* (IDAU).
  - Secure expansion ports.
  - System Security Controller.
  - System Controller.
  - Secure debug with debug certificate controlled authentication.
- APB peripherals with security support:
  - Three general-purpose timers with configurable security. One timer is on the 32KHz domain and two are on the **SYSCLK** 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** domain.
  - Two *Message Handling Units* (MHUs) to facilitate communication between processors.
- Power-control components:
  - *Power Dependency Control Matrix* (PDCM).
  - *Power Policy Units* (PPU).
  - CoreLink LPD-500 Low Power Distributor.
  - Wakeup on interrupt from *External Wakeup Controllers* (EWC) and *Wakeup Interrupt Controllers* (WIC).

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.
- Crypto element.

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

ACG AHB5/APB Access Control Gate.

EAM AHB5 Exclusive Access Monitor.

MHU Message Handling Unit.

MPC AHB5 Memory Protection Controller.

MSC Master Security Controller.

PCSM Power Control State Machine.

PIK Power Integration Kit.

PPC AHB5/APB Peripheral Protection Controller.

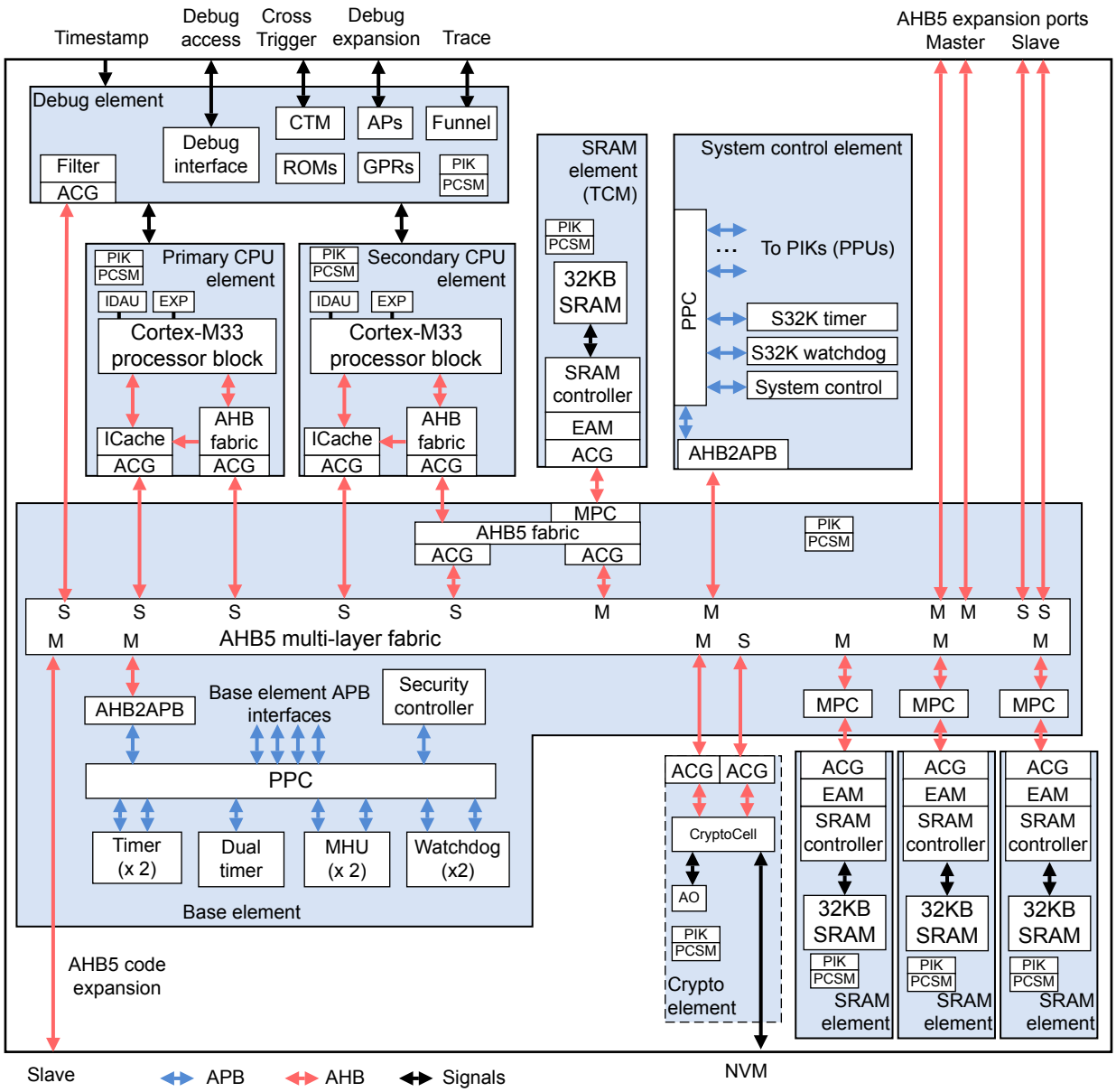

Figure 2-1 Top-level element interconnections

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.
- 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.
- Processor-related signals:
  - Processor control.
  - Interrupts.
  - Configuration signals.
- Base element:
  - AHB expansion.
- System control:
  - Static configuration signals.
  - Power and clock control LPI interfaces.
  - External Wakeup Controller interrupt inputs.
- Debug and Trace:
  - Debug access.
  - Timestamp.
  - Cross Trigger Channel.
  - Debug APB expansion.
  - ATB Trace.
  - Debug authentication.
- Crypto: This element integrates the CryptoCell-312 into the system to provide cryptographic acceleration. This element is optional, and it includes:
  - NVM APB interface.
  - *Debug Control Unit* (DCU) signals.
  - *Life Cycle State* (LCS) signals.
- System security controller expansion interface.
- 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 typically contains an FPU and/or DSP. It is synchronous to the main clock, but could run `N` times faster.

The Cortex-M33 processor has the following features:

- Three-stage pipeline.
- Armv8-M Mainline profile.
- TrustZone-M security.
- Up to eight SAU entries each (configurable).
- Up to 16 MPU regions with eight Secure and eight Non-secure (configurable).
- IDAU defining high-level security memory mapping.

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

- If the FPU is present.
- If the Digital Signal Processing extension instructions are included.
- 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 that is implemented in the NVIC.
- Debug resources and trace support.

2.4 Base element

The Base element provides the following features:

- A multilayer AHB5 interconnect for all the subsystem elements and expansion buses.
- A Memory Protection Controller for each SRAM element.
- AHB to APB bus converters and TrustZone Peripheral Protection Controllers for:
  - Two CMSDK Timers.
  - One CMSDK Dual Timer.
  - One CMSDK Watchdog timers.
  - Message Handling Units that can send messaging interrupts to each core.
- Two AHB5 slave expansion ports and three master expansion ports.
- A security controller with expansion support.
- A single voltage domain and power-gated region.
- Two synchronous clock domains.

2.5 SRAM elements

The SSE-200 supports four SRAM elements. Each SRAM element has the following features:

- One bank of single port SRAM.
- Zero clock cycle latency.
- ON/OFF/MEM_RET power policy support.
- Exclusive access support.

A Memory Protection Controller in the Base element manages Secure access.

Each of the four banks of contiguous SRAM has the following features:

- Fixed (per bank) 32KB size.
- *Exclusive Access Monitor* (EAM).
- Independent memory power control.

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.
  - Syndrome (status) of last reset.
  - 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 *2.8 Power control infrastructure* on page 2-27.
- 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.

Related reference

2.8 Power control infrastructure on page 2-27

2.7 Debug element

The Debug element provides the following features and interfaces:

- JTAG and *Serial Wire Debug* (SWD) supported.
- Single *Debug Access Port* (DAP) shared between both processors and other system level debug logic.
- Debug certificate access filter.
- Combining all trace sources within the system to a single shared ATB trace output to support a single TPIU trace output.
- CTM and CTI.
- Timestamp distribution from expansion logic to the debug logic of both processors.
- 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.

——— **Note** ———

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 which might rely on a battery or on harvested energy. SSE-200 uses two key methods to reduce the overall power of the system:

- Dynamic hierarchical clock control to reduce dynamic power.
- Multiple power-gated regions in the design to reduce leakage power.

Each power domain contains a *Power Integration Kit* (PIK) that performs the following:

- Integrates a *Power Policy Unit* (PPU) that provides technology-independent power control of the domain.
- Integrates Q-Channel and P-Channel infrastructure components to bring together the quiescent status and control of key IP blocks within the power domain to the PPU.

The PIK of each domain is primarily designed to deal with the power control of its associated power domain. However, some power domains are aware of the power state of other power domains, to maintain the correct operation of the system. The *Power Dependency Control Matrix* (PDCM) enables software to configure the relationship between each power domain.

2.9 Crypto element

The optional Crypto element provides the following features:

- Cryptographic acceleration for the protection of data-in-transit (communication protocols) and data-at-rest.
- Protection of various assets belonging to the IC or device manufacturer, service operators providing services over the target device and the user itself. These asset protection features include:
  - Image verification at boot or during runtime.
  - Authenticated debug.
  - *True Random Number Generation* (TRNG).
  - Lifecycle management.

For more information on the CryptoCell-312 , see the *Arm® TrustZone® CryptoCell-312 Technical Reference Manual*.

——— **Note** ———

You must have a license for the CryptoCell-312 IP to access the product documentation.

———————————

Chapter 3
Software

This chapter describes the software available for use with the SSE-200.

It contains the following section:

3.1 About the software

Application processor firmware, which is available separately, consists of the code that is required to boot the subsystem up to the point where the OS execution starts. Contact your Arm representative for details on the software and its location.

The firmware contains:

- Trusted Firmware for M-class (TF-M) that separates the Secure and Non-secure execution environment.
- *Cortex Microcontroller Software Interface Standard* (CMSIS) compliant drivers.
- Mbed OS driver support and code for applicable peripherals.

Note

For more information on Mbed, see *mbed.com*.

Appendix A
Revisions

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

It contains the following section:

- *A.1 Revisions* on page Appx-A-32.

A.1 Revisions

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

Table A-1 Issue A

Change	Location	Affects
First release	-	-

Table A-2 Differences between issue A and issue 0100-00

Change	Location	Affects
System block diagram updated (includes optional Crypto element)	-*1.1.2 SSE-200 block diagram* on page 1-12	r1p0
Feature list updated (added optional Crypto and Power-control components).	*2.1 About the hardware components* on page 2-18	r1p0
Top-level element interconnections block diagram updated; figure abbreviations added.	*2.2 Top-level system partitioning* on page 2-19	r1p0
Interface signals list updated to include Security and optional Crypto interfaces.	*2.2.2 Interface signals* on page 2-21	r1p0
Descriptions of SSE-200 elements updated to match TRM descriptions.	• *2.3 CPU elements* on page 2-22 • *2.4 Base element* on page 2-23 • *2.5 SRAM elements* on page 2-24 • *2.6 System control element* on page 2-25 • *2.7 Debug element* on page 2-26 • *2.8 Power control infrastructure* on page 2-27	r1p0
Added description of optional Crypto element.	*2.9 Crypto element* on page 2-28	r1p0

Table A-3 Differences between issue 0100-00 and issue 0200-00

Change	Location	Affects
The following documents addded as reference documents: • *Arm® CoreSight™ Architecture Specification, v2.0.* • *Arm® Debug Interface Architecture Specification ADIv5.0 to ADIv5.2.*	• *Additional reading* on page 8 • *1.3.2 Debug* on page 1-16	All revisions
Arm® Power Policy Unit Architecture Specification, version 1.1	• *Additional reading* on page 8 • *1.3.4 Advanced Microcontroller Bus Architecture* on page 1-16	All revisions
The following deliverables added: • System level IP-XACT descriptions. • UPF 2.0 power intent description.	*1.2.1 Hardware deliverables* on page 1-15	All revisions
• *AHB master bus to code memory* replaced with *AHB multi-layer bus matrix*. • *Secure debug with debug certificate controlled authentication* added. • *Two Message Handling Units (MHUs) allow software to raise interrupts* replaced with *Two Message Handling Units (MHUs) to facilitate communication between processors* .	*2.1 About the hardware components* on page 2-18	All revisions

Table A-3 Differences between issue 0100-00 and issue 0200-00 (continued)

Change	Location	Affects
Option *SRAM size* removed.	*2.2.1 Configuration options* on page 2-20	All revisions
• *Power control expansion interfaces* replaced by *Power and clock control LPI interface.* • *Security* replaced by *System securitycontroller expansion interface*	*2.2.2 Interface signals* on page 2-21	All revisions
Reference to configuration parameter *If the coprocessor interface is present* removed.	*2.3 CPU elements* on page 2-22	All revisions
Paragraph before the note, and part of the note removed.	*2.7 Debug element* on page 2-26	All revisions
Reference to asset protection feature *Provisioning of assets* removed.	*2.9 Crypto element* on page 2-28	All revisions
Reference to *Flash programming support code, which is separate from Mbed OS* removed.	*3.1 About the software* on page 3-30	All revisions