Arm® Musca-S1 Test Chip and Board

Technical Overview

arm

101756_0000_00_en

Arm® Musca-S1 Test Chip and Board

Technical Overview

Release Information

Document History

Issue	Date	Confidentiality	Change
0000-00	02 December 2019	Non-Confidential	First issue

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

www.arm.com

Conformance Notices

This section contains conformance notices.

Federal Communications Commission Notice

This device is test equipment and consequently is exempt from part 15 of the FCC Rules under section 15.103 (c).

CE Conformity

The *Waste Electrical and Electronic Equipment* (WEEE) marking, that is, the crossed out wheelie-bin figure, indicates that this product must not be disposed of with general waste within the European Union. To prevent possible harm to the environment from uncontrolled waste disposal, the user is required to recycle the product responsibly to promote reuse of material resources. To comply with EU law, you must dispose of the product in one of the following ways:

- Return it to the distributer where it was purchased. The distributer is required to arrange free collection when requested.
- Recycle it using local WEEE recycling facilities. These facilities are now very common and might provide free collection.
- If purchased directly from Arm, Arm provides free collection. Please e-mail *weee@arm.com* for instructions.

The CE Declaration of Conformity for this product is available on request.

The system should be powered down when not in use.

It is recommended that ESD precautions be taken when handling this product.

The product generates, uses, and can radiate radio frequency energy and may cause harmful interference to radio communications. There is no guarantee that interference will not occur in a particular installation. If this equipment causes harmful interference to radio or television reception, which can be determined by turning the equipment off or on, you are encouraged to try to correct the interference by one or more of the following measures:

- Ensure attached cables do not lie across any sensitive equipment.
- Reorient the receiving antenna.
- Increase the distance between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Note

It is recommended that wherever possible shielded interface cables be used.

Contents

Arm® Musca-S1 Test Chip and Board Technical Overview

Preface

This preface introduces the *Arm® Musca-S1 Test Chip and Board Technical Overview*.

It contains the following:

About this book

This book gives an overview of the Arm® Musca-S1 Test Chip and Board.

Intended audience

This book is written for experienced hardware and software developers to enable low-power, secure *Internet of Things* (IoT) endpoint development using the Musca-S1 test chip and board.

Using this book

This book is organized into the following chapters:

Chapter 1 Introduction
This chapter introduces the Arm Musca-S1 test chip and board.

Chapter 2 Hardware and software
This chapter gives an overview of the Musca-S1 development board hardware and software.

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.

`monospace`
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.

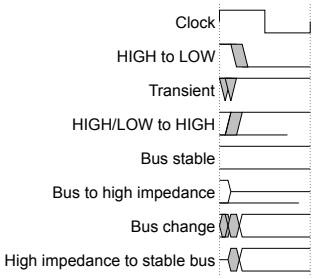

Figure 1 Key to timing diagram conventions

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, n 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® Musca-S1 Test Chip and Board Technical Reference Manual* (101835).
- *Arm® CoreLink™ SSE-200 Subsystem for Embedded Technical Overview (r1p0)* (101123).
- *Arm® CoreLink™ SSE-200 Subsystem for Embedded Technical Reference Manual (r1p0)* (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 (r0p2)* (100230).
- *PrimeCell UART (PL011) Technical Reference Manual* (Arm DDI 0183).
- *Arm® PrimeCell Real Time Clock (PL031) Technical Reference Manual* (Arm DDI 0224).
- *CoreSight™ Components Technical Reference Manual* (Arm DDI 0314).
- *Arm® DS-5 Arm DSTREAM User Guide* (Arm DUI 0481).
- *Arm® DS-5 Using the Debug Hardware Configuration Utilities* (Arm DUI 0498).

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

- *Arm® CryptoCell-312 Technical Reference Manual (r1p0)* (100774).
- *Arm® v7-M Architecture Reference Manual* (Arm DDI 0403).
- *Arm® v8-M Architecture Reference Manual* (Arm DDI 0553).
- *Arm® AMBA® 5 AHB Protocol Specification* (Arm IHI 0033).
- *Arm® AMBA® APB Protocol Specification Version 2.0* (Arm IHI 0024).

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 Musca-S1 Test Chip and Board Technical Overview*.
- The number 101756_0000_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
Introduction

This chapter introduces the Arm Musca-S1 test chip and board.

It contains the following sections:

1.1 Precautions

This section describes precautions that ensure safety and prevent damage to your Musca-S1 development board.

This section contains the following subsections:

1.1.1 Ensuring safety

The Musca-S1 development board operates at 5V supplied through the DAPLink 5V USB connector.

Warning

Do not use the Musca-S1 development board near equipment that is sensitive to electromagnetic emissions, for example, medical equipment.

1.1.2 Operating temperature

The Musca-S1 development board has been tested in the temperature range 15°C-30°C.

1.1.3 Preventing damage

The Musca-S1 development board is intended for use within a laboratory or engineering development environment.

Caution

To avoid damage to the Musca-S1 development board, observe the following precautions:

- Never subject the board to high electrostatic potentials. Observe *ElectroStatic Discharge* (ESD) precautions when handling any board.
- Always wear a grounding strap when handling the board.
- Only hold the board by the edges.
- Avoid touching the component pins or any other metallic element.
- Do not fit an Arduino Expansion Shield while the Musca-S1 development board is powered up.

1.2 About the Musca-S1 test chip and board

The Musca-S1 development board provides access to the Musca-S1 test chip.

Musca-S1 test chip and board

The Musca-S1 test chip demonstrates the foundation of single-chip secure *Internet of Things* (IoT) endpoints. The architecture integrates the recommendations of *Platform Security Architecture* (PSA) using the same subsystem as Musca-A (Arm CoreLink SSE-200 Subsystem for Embedded) but with the addition of:

- Dual on-chip eMRAM and SRAM.
- Secure memory subsystems.
- PSA Level 1 and Functional API certification.

The Musca-S1 test chip implements a SSE-200 subsystem (r1p0) in Samsung Foundry 28nm, *Fully Depleted Silicon on Insulator process* (28FDS). The implementation is ready to be used to form the core processing element of energy-efficiency mainstream IoT devices with secure PSA *Root-of-Trust* (RoT). Musca-S1 can also be used to prototype secure boot, on-chip storage execution and network device management through Trusted Firmware-M (TF-M), Arm Mbed™ OS, and Arm Pelion™ IoT platform integration.

The Musca-S1 development platform is bootable from on-chip eMRAM or off-chip QSPI (on-board Flash.

Major components and systems

The Musca-S1 development board provides the following main features:

- Musca-S1 test chip that includes, but is not limited to, the following:
  - CoreLink SSE-200 subsystem that contains two Arm Cortex-M33 (r0p2) processors.
  - 2MB on-chip eMRAM.
  - 2MB on-chip Code SRAM.
  - Peripheral and Arduino Expansion Shield interfaces.
- On-board DAPLink that provides the following access:
  - *Serial Wire or JTAG Debug Port* (SWJ-DP).
  - *USB Mass Storage Device* (USBMSD) for uploading new firmware.
  - USB serial port. The UART to the DAPLink does not support hardware flow control.
  - Remote reset.
- On-board:
  - 3-axis orientation and motion sensor (gyro sensor).
  - Temperature sensor/ADC/DAC.
  - *Quad Serial Peripheral Interface* (QSPI) 32MB boot flash.
- P-JTAG processor debug and SWD header.
- User RGB LED, status LEDs, user reset, and On/Off push buttons.
- The board is powered from USB 5V power or Li-ion rechargeable battery backup, battery not supplied, selectable by a jumper link.
- Headers for Arduino Expansion Shield to support development of custom designs:
  - 16 3V3 or 1V8 GPIO.
  - UART.
  - SPI.
  - I^2C.
  - I^2S three-channel, master only.
  - 3-channel *Pulse Width Modulation* (PWM).
  - 6-channel analog interface from the on-board combined ADC, DAC, and GPIO.

1.3 The Musca-S1 development board at a glance

The following figure shows the physical layout of the upper face of the Musca-S1 development board.

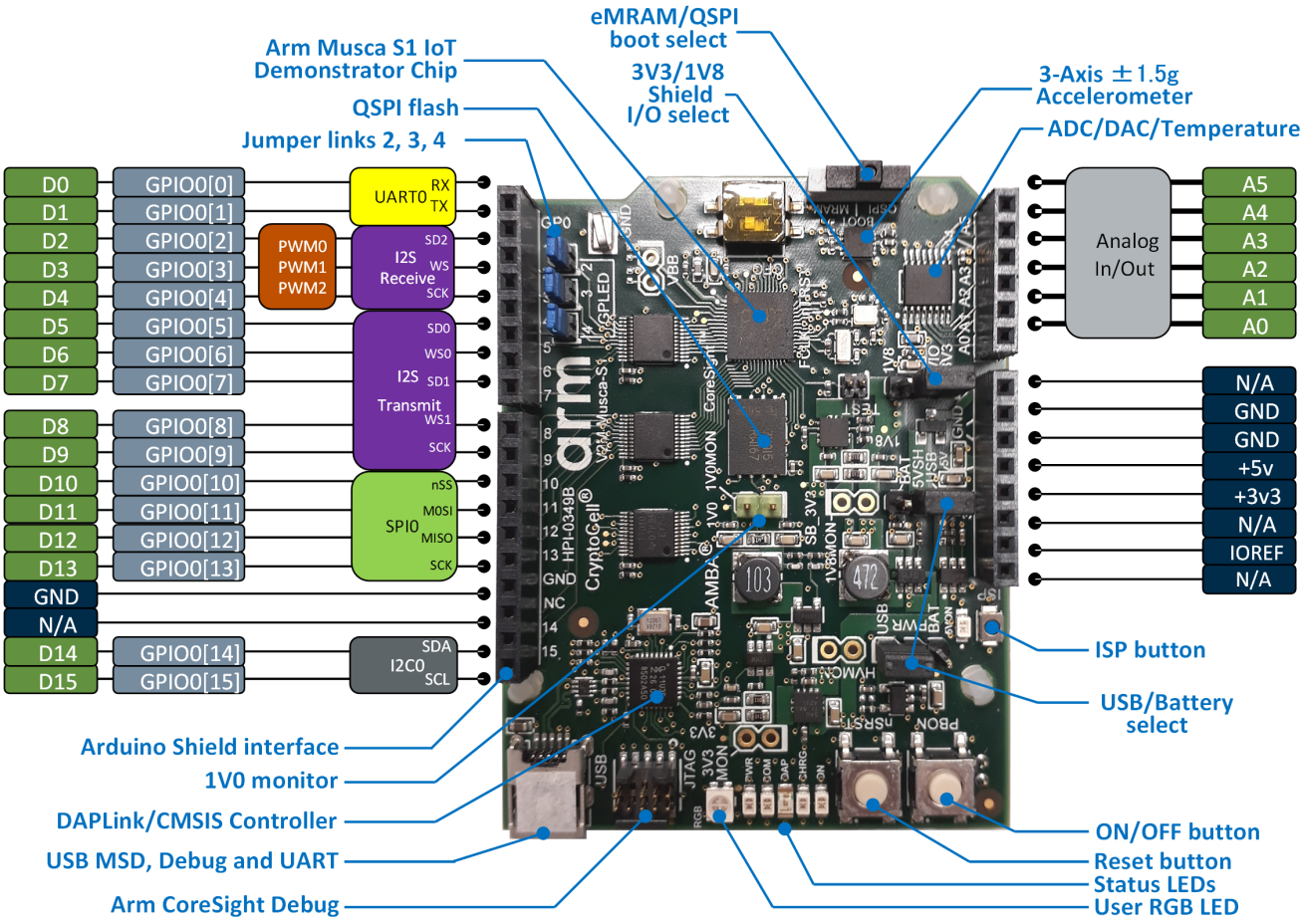

Figure 1-1 Musca-S1 development board

Note

The figure shows the functions that are multiplexed onto the Musca-S1 test chip I/O and which are available on the Arduino Expansion Shield.

The following table describes the Musca-S1 development board components.

Table 1-1 Board components

Component	Comment
Musca-S1 test chip	Samsung Foundry 28FDS eMRAM-enabled *Internet of Things* (IoT) test chip.
Boot selector slider switch	eMRAM or QSPI
Expansion Shield analog I/O connector	1V8 or 3V3 I/O. Selected by jumper link J12.
Expansion Shield power and voltage reference connector	-
Jumper link. Expansion Shield I/O voltage selector J12.	1V8 or 3V3. Default 3V3.

Table 1-1 Board components (continued)

Component	Comment
Jumper link. Expansion Shield power supply selector J19.	Battery or USB. Default USB. Use in conjunction with jumper link J18.
Jumper link. Board power supply selector J18.	Battery or USB. Default USB. Use in conjunction with jumper link J19.
1V0 supply test point	Musca-S1 test chip core power supply.
ISP push button DAPLink update	To update DAPLink
On/Off push button (PBON)	Labeled PBON on board
Cortex-M33 system reset and CoreSight component rest (nSRST)	Labeled nRST on board
ON LED	Green status LED. Board power supplies are active. Next to nRST button.
CHRG LED	Orange status LED. Li-ion battery charging in progress. Next to ON LED.
DAP LED	Blue status LED. DAP activity. Next to CHRG LED.
COM LED	Green status LED. USB UART activity. Next to DAP LED.
PWR LED	Orange status LED. Power is connected. Next to COM LED.
RGB user LED	Jumper 2 connects red to GPIO[2] and to Expansion Shield digital I/O connector 1. Jumper 3 connects green to GPIO[3] and to Expansion Shield digital I/O connector 1. Jumper 4 connects blue to GPIO[4]v and to Expansion Shield digital I/O connector 1.
CoreSight debug connector	SWJ-DP
USB mini B connector	Connects to DAPLink
Expansion Shield digital I/O connector	Jumper J12 selects 1V8 or 3V3.

1.4 Getting started

The Musca-S1 development board is controlled from a USB port that supports UART, *Mass Storage Device* (MSD), and CoreSight debug connection methods.

The board is factory-programmed with the DAPLink firmware and binary QSPI image to enable bootup.

Powering up into the operating state

The minimum actions to boot the development board are as follows:

1. Set the boot select switch to QSPI.
2. Connect a USB cable to the board.
3. Press the PBON button.
4. Connect a serial terminal to the USB UART. The serial port settings must be:
   - 115.2kBaud.
   - 8N1.
   - No hardware or software flow control.

To load a new user image, drag and drop the new image onto the drive labeled MUSCA_S.

Chapter 2
Hardware and software

This chapter gives an overview of the Musca-S1 development board hardware and software.

It contains the following sections:

2.1 Board hardware

The hardware infrastructure of the Musca-S1 development board provides access to the Musca-S1 test chip and supports Shield expansion.

Overview of the Musca-S1 development board hardware

The test chip interfaces connect directly between the test chip and the peripheral devices on the board, and between test chip and the Shield headers.

The following figure shows the hardware infrastructure of the Musca-S1 development board.

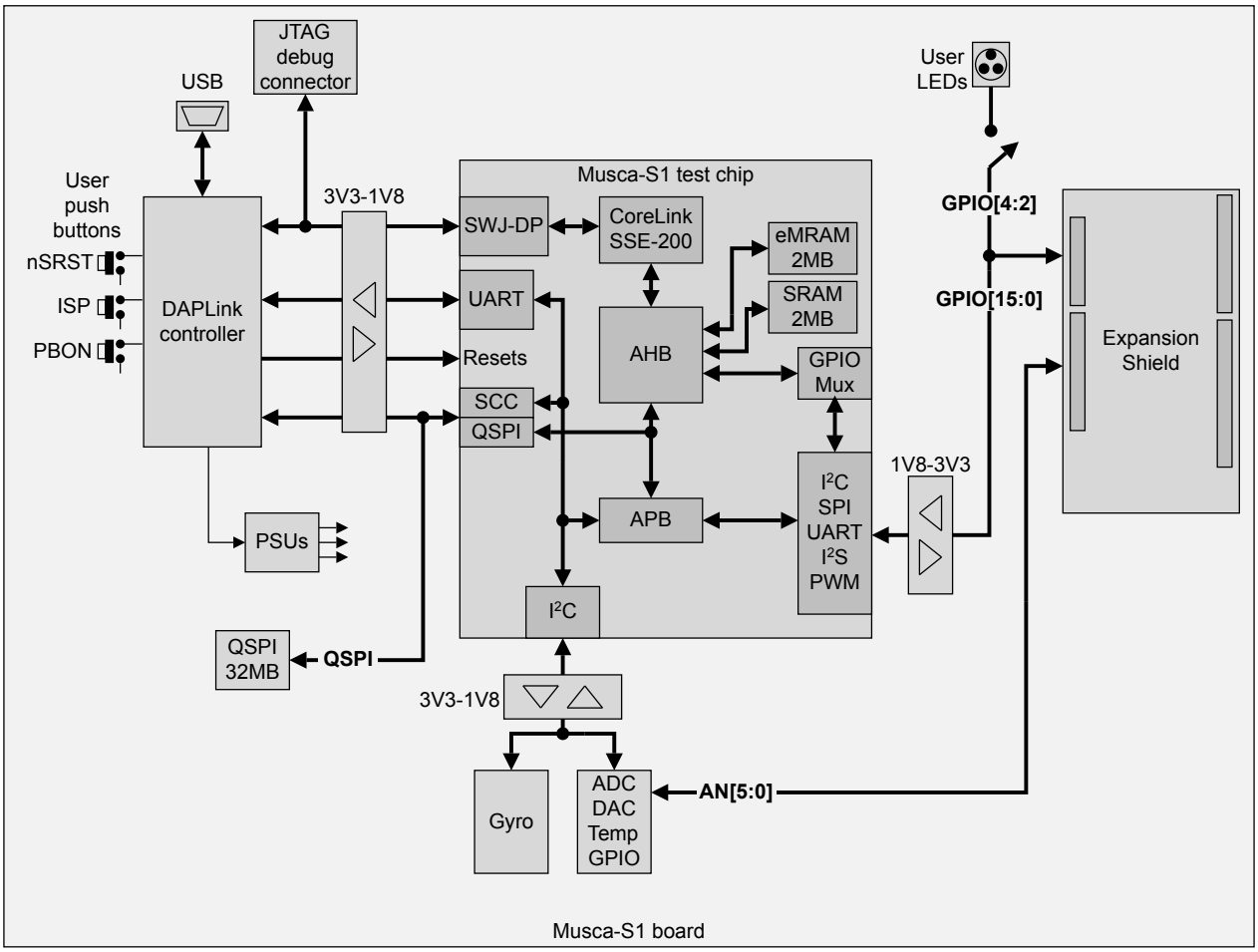

Figure 2-1 Hardware infrastructure of the Musca-S1 development board

Musca-S1 development board components and systems

The development board contains the following components and systems:

- One Musca-S1 test chip with CoreLink SSE-200 Subsystem for Embedded (r1p0). The SSE-200 subsystem includes, but is not limited to, the following:
  - CPU0: One Cortex-M33 (r0p2) processor. *Floating-point unit* (FPU), DSP, no coprocessor.
  - CPU1: One Cortex-M33 (r0p2) processor. FPU, DSP, no coprocessor. Clock system enables operation at ×N speed of CPU0 processor. Body-bias enabled transistors for low-power mode.
  - One 2KB instruction cache and one 2KB data cache for each processor.
  - 4 × 128KB SRAM. One 128KB bank, SRAM3, functions as *Tightly Coupled Memory* (TCM), Tightly Coupled to CPU1 and operating at CPU1 clock speed.

  - CryptoCell™-312 (r1p0) with 1Kbyte *One Time Programming* (OTP) emulated using simple registers reset by powerup reset only.
  - Timer, Watchdog peripherals, and system control.

  The following on-chip blocks are outside the SSE-200 subsystem.
  - 2MB Code SRAM.
  - 2×1MB eMRAM.
  - Clock system. Input clock sources from development board.
- Arduino Shield expansion with on-board level converters and a jumper link to enable the Shield voltage to be either the SoC voltage, 1V8, or 3V3. Enables custom designs by providing the following interfaces:
  - UART/USART.
  - I^2S, three-channel, master only.
  - SPI.
  - I^2C.
  - PWM.
  - 6-channel analog interface from the on-board combined ADC, DAC, and GPIO.
  - 16 1V8 or 3V3 GPIO.
  - 1Hz clock.
- On-board DAPLink that enables the following functionality over USB:
  - *Serial Wire Debug* (SWD).
  - *USB Mass Storage Device* (USBMSD) for uploading new firmware.
  - USB serial port. The UART to the DAPLink does not support hardware flow control.
  - Remote reset.
- On-board gyro sensor:
  - MMA7660FC 3-axis orientation and motion detection sensor.
  - I^2C interface to test chip.
- On-board combined ADC/DAC/temperature sensor:
  - AD5593.
  - 6-channel 3V3 ADC/DAC/GPIO interface to Arduino Shield.
  - Temperature indicator.
- Programmable boot select:
  - 32MB On-board QSPI boot flash.
  - 2×1MB on-chip boot eMRAM.
  - 2MB on-chip Code SRAM, after being preloaded with execution code.
  - Both Secure and Non-secure access.
- Debug connector that provides access to:
  - P-JTAG processor debug.
  - *Serial Wire Debug* (SWD).
- User push-button:
  - PBON On/Off push-button.
  - nSRST: Cortex-M33 system reset and CoreSight component reset.
  - ISP: Updates DAPLink firmware.
- RGB LED. Jumper connectors provide optional connections between the Arduino Expansion header and the Musca-S1 test chip:
  - Red LED connected to GPIO[2] pin, optional PWM0.
  - Green LED connected to GPIO[3] pin, optional PWM1.
  - Blue LED connected to GPIO[4] pin, optional PWM2.
- Status LEDs.
- 5V USB or battery power, selectable by slider switch:
  - DAPLink 5V USB connector.
  - CLN 523450, Lithium Ion, 3.7V, 950mAh (not supplied).

2.2 Overview of the Musca-S1 test chip

The Musca-S1 test chip is based on the SSE-200 subsystem which features two Cortex-M33 processors.

The SSE-200 subsystem is version r1p0 and the Cortex-M33 processors are version r0p2.

The test chip also implements a memory subsystem, external device interfaces, a clock generator, and *Serial Configuration Control* (SCC) registers for setting default powerup values.

See the *Arm® CoreLink™ SSE-200 Subsystem for Embedded Technical Reference Manual (r1p0)* for more information on the SSE-200 subsystem:

The following figure shows a high-level view of the architecture of the Musca-S1 test chip.

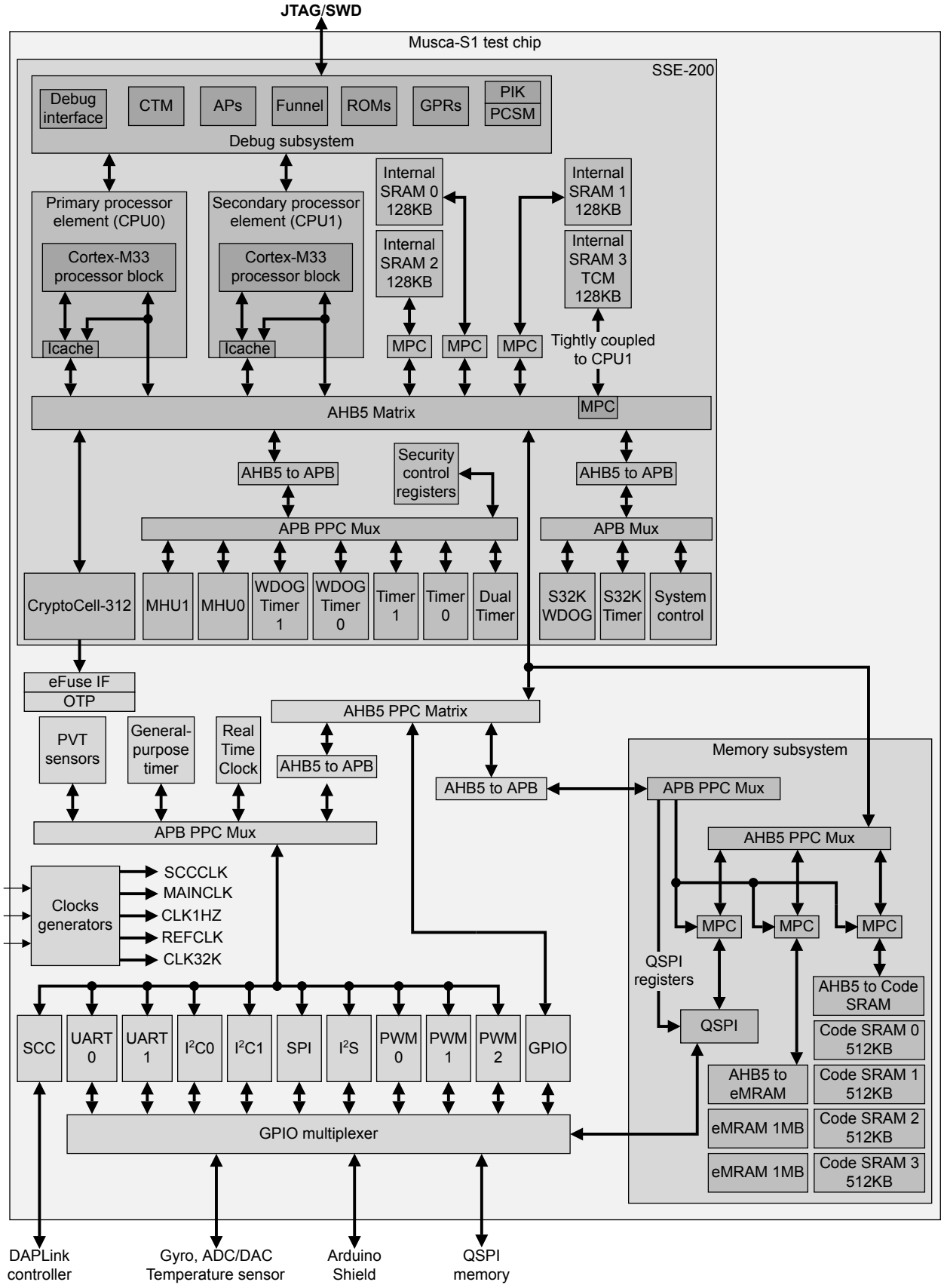

Figure 2-2 Musca-S1 test chip

Major components and systems of the Musca-S1 test chip

SSE-200 subsystem (r1p0)

- Two Cortex-M33 (r0p2) processors with FPU and DSP, and with no coprocessor:
  - CPU0: 50MHz. Used as main processor.
  - CPU1: 200MHz.
- Memory system:
  - One 2KB instruction cache and one 2KB data cache for each Cortex-M33 processor.
  - 4×128KB SRAM. One bank, SRAM3, functions as *Tightly Coupled Memory* (TCM), Tightly Coupled to CPU1 and operating at CPU1 clock speed.
- *Serial Wire Debug* (SWD).
- Secure AMBA interconnect:
  - AHB5 Bus matrix.
  - AHB5 *Exclusive Access Monitors* (EAMs).
  - AHB5 *Access Control Gates* (ACGs).
  - AHB5 to APB bridges.
  - Expansion AHB5 master and slave buses - two of each.
- Security components:
  - AHB5 TrustZone® *Memory Protection Controllers* (MPCs).
  - AHB5 TrustZone *Peripheral Protection Controllers* (PPCs).
  - *Implementation Defined Attribution Unit* (IDAU).
  - CryptoCell-312 (r1p0).
  - Secure and Non-secure configurable peripherals and memory access.
  - Secure boot.
- Secure APB peripherals:
  - One general-purpose timer with configurable security in the **S32KCLK** domain.
  - Two CMSDK timers, Timer0 and Timer1 with configurable security, in the **SYSCLK** domain.
  - One *Cortex®-M System Design Kit* (CMSDK) dual timer with configurable security.
  - One secure watchdog in the **S32KCLK** domain.
  - One secure watchdog in the **SYSCLK** domain.
  - One Non-secure watchdog in the **SYSCLK** domain.

Musca-S1 test chip outside the SSE-200 subsystem

- Two 1MB eMRAM memories.
- 2MB Code SRAM: 4 × 512KB independently power-enabled.
- One *Real Time Clock* (RTC) in the Always ON domain.
- One 32-bit general-purpose timer running at 32.768kHz with programmable interrupts.
- 16 external GPIO interrupts.
- 16 GPIO.
- Three *Process, Voltage, and Temperature* (PVT) sensors:
  - 501-stage ring oscillators. Software can read data from the sensors in the sensor peripheral and group registers.
- Three-channel I^2S:
  - Two master transmitters.
  - One master receiver.
- Three independent *Pulse Width Modulation* (PWM) outputs.
- Two UARTs, UART0 and UART1. The default connectivity is:
  - UART0 to Shield header.
  - UART1 to DAPLink. No hardware flow control.
- Two I^2C, I^2C0 and I^2C1, which can be used as master (default), or slave:
- One SPI interface which can be used as master (default), or slave.
- One alternate function I/O multiplexer.
- One QSPI for external flash control with *Execute in Place* (XIP) capability.
- Programmable boot select:
  - Internal Code eMRAM.
  - External QSPI Flash.
- External powerup reset.
- Three system clock sources:
  - External **REFCLK**, 32.768kHz.
  - External **FASTCLK**, 32MHz.
  - On-chip PLL. Output up to 200MHz.
- One JTAG/SWD debug port.
- One *Serial Configuration Controller* (SCC) with dual access port:
  - SCC serial during reset, accessible by DAPLink only while chip is under powerup reset.
  - APB after reset, accessible by software, or DAPLink while in debug mode (after reset is released).

2.3 Software, firmware, board, and tools setup

Arm supplies software and firmware for the Musca-S1 development board.

You can access software and firmware at the Arm Community pages which are accessible from *https://www.arm.com/musca*.

Connecting to the board

To power the board, connect the USB port to your computer and press the PBON user push button. The DAPLink interface appears in the Windows device manager as an Arm Mbed composite device, part of which is the Mbed serial port, UART. The following figure shows an example configuration that contains the Mbed composite device and the Mbed serial port.

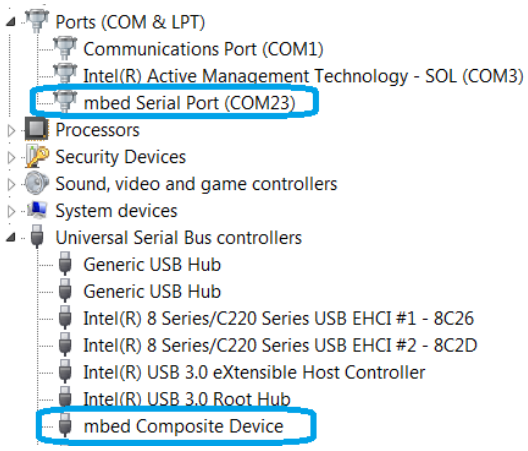

Figure 2-3 DAPLink interface

Note

- Other components of the Mbed composite device are not visible in the Windows device manager. See *2.1 Board hardware* on page 2-16 for the other components of the Mbed composite device.
- UART1 to the DAPLink does not support hardware flow control.

Updating DAPLink firmware

To update the DAPLink firmware, you can use the DAPLink drag and drop update method:

1. Press and hold the ISP button while powering up the board using the USB lead.
2. Delete the `firmware.bin` file that appears in the `CRP DISABLD USB` drive.
3. Copy `DAPLink_S1_DUAL.vxxx.bin` to the `CRP DISABLD drive`.
   - From a Windows system, you can simply Drag and Drop the file.
   - On Linux/Mac OS, use the following command:

     ```
     dd if={new_firmware.bin} of=/Volumes/CRP\ DISABLD/firmware.bin conv=notrunc
     ```
4. Power cycle the board using the USB lead. Do not press the ISP button during the power cycle.

Updating the application software image

To update the application image, perform the following steps:

1. Ensure that the boot switch is set to QSPI or eMRAM as required.
2. Power up the board by connecting the USB lead and pressing the PBON button.
3. Drop a `.bin` format software image onto the `MBED` drive, for example `blinky.bin`. The software image is programmed to QSPI or eMRAM depending on the boot selector slider switch position.
4. Power cycle the board or press the nSRST button to reset the system and boot from the new QSPI or eMRAM software image.

Note

The file `blinky.bin` is available at the Arm Community pages which are accessible from *https://www.arm.com/musca*.

DAPLink UART setting

The default DAPLink UART setting is 115,200 baud (8N1).

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-25.

A.1 Revisions

The following table lists the technical changes between released issues of this book.

Table A-1 Issue 101756_0000_00

Change	Location	Affects
No changes, first release.	-	-