Arm® Corstone™ SSE-300 with Cortex®-M55 and Ethos™-U55 : Example Subsystem for MPS3 (Partial Reconfiguration Design)

Revision: C

Application Note AN552

Non-Confidential

Copyright © 2021-2022 Arm Limited (or its affiliates).
All rights reserved.

Issue C

DAI 0552C

Arm® Corstone™ SSE-300 with Cortex®-M55 and Ethos™-U55 : Example Subsystem for MPS3 (Partial Reconfiguration Design)

Application Note AN552

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.

Release information

Document history

Issue	Date	Confidentiality	Change
A	27 May 2021	Non-Confidential	First Issue
B	12 November 2021	Non-Confidential	Update SSE-300 to r0p1-00eac0 and moving CDE module from Core partition to User partition Added clarifications and enhancements to the information contained within this document Notification that this is a development release and there is a known issue with trace support.
C	4 February 2022	Non-Confidential	Added section on availability of trace support Fixed interrupt mapping Fixed memory mapping conflict between areas of the documentation

Non-Confidential Proprietary Notice

This document is protected by copyright and other related rights and the practice or implementation of the information contained in this document may be protected by one or more patents or pending patent applications. No part of this document may be reproduced in any form by any means without the express prior written permission of Arm. No license, express or implied, by estoppel or otherwise to any intellectual property rights is granted by this document unless specifically stated.

Your access to the information in this document is conditional upon your acceptance that you will not use or permit others to use the information for the purposes of determining whether implementations infringe any third-party patents.

THIS DOCUMENT IS PROVIDED “AS IS”. ARM PROVIDES NO REPRESENTATIONS AND NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO THE DOCUMENT. For the avoidance of doubt, Arm makes no representation with respect to, and has undertaken no analysis to identify or understand the scope and content of, patents, copyrights, trade secrets, or other rights.

This document may include technical inaccuracies or typographical errors.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL ARM BE LIABLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF ANY USE OF THIS DOCUMENT, EVEN IF ARM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

This document consists solely of commercial items. You shall be responsible for ensuring that any use, duplication or disclosure of this document complies fully with any relevant export laws and regulations to assure that this document or any portion thereof is not exported, directly or indirectly, in violation of such export laws.

Use of the word “partner” in reference to Arm's customers is not intended to create or refer to any partnership relationship with any other company. Arm may make changes to this document at any time and without notice.

If any of the provisions contained in these terms conflict with any of the provisions of any click through or signed written agreement covering this document with Arm, then the click through or signed written agreement prevails over and supersedes the conflicting provisions of these terms. This document may be translated into other languages for convenience, and you agree that if there is any conflict between the English version of this document and any translation, the terms of the English version of the Agreement shall prevail.

The Arm corporate logo and words marked with ® or ™ are registered trademarks or trademarks of Arm Limited (or its affiliates) in the US and/or elsewhere. All rights reserved. Other brands and names mentioned in this document may be the trademarks of their respective owners. Please follow Arm's trademark usage guidelines at **http://www.arm.com/company/policies/trademarks**.

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.

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

developer.arm.com

Progressive terminology commitment

Arm values inclusive communities. Arm recognizes that we and our industry have used terms that can be offensive. Arm strives to lead the industry and create change.

This document includes terms that can be offensive. We will replace these terms in a future issue of this document. If you find offensive terms in this document, please email **terms@arm.com**.

LICENSE GRANTS

THE END USER LICENSE AGREEMENT FOR THE ARM SYSTEM OR SUBSYSTEM FOR AN ARM FPGA PROTOTYPING BOARD ("THE LICENCE"), LES-PRE-21902, DEFINES THE LICENCE GRANTS.

DELIVERABLES

Part A

Hardware Binaries:
Encrypted FPGA bitstream file containing various Arm technology including:

SSE-300 Subsystem
Cortex-M55 processor
Ethos-U55 Embedded ML Inference processor.

Software Binaries:
Motherboard Configuration Controller binary (mbb_v151.ebf), including Arm® Keil® USB and SD card drivers, and Analog Devices FMC EEPROM reader.
selftest binary (an552_st.axf) for Cortex-M55 in Corstone™ SSE-300.

Documentation:
Documentation, provided as PDF

Part B

Text configuration files (.txt) in the <install_dir>`/Boardfiles/MB/HBI0309x/` directory:

```
/board.txt
/AN552/an552_v3.txt
/AN552/images.txt
```

User Partial Reconfiguration partition RTL source code
RTL Example designs of Arm components in the Cortex-M55 kit known as CDE and DEC_CDE
Selftest example source code
Arm source code portions of the Self-test

Part C

None

Part D

None

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.

Contents

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.
Non-Confidential

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.
Non-Confidential

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.
Non-Confidential

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.
Non-Confidential

1 Introduction

1.1 Purpose of this application note

This application note describes the features and functionality of the AN552 Soft Macrocell Model (SMM), or AN552 subsystem, for use on the MPS3 prototyping board.

The AN552 SMM is a single-Cortex-M55, with Custom Datapath Extension, FPGA implementation of the Arm® Corstone™ SSE-300 with Cortex®-M55 and Ethos™-U55 Example Subsystem.

The example subsystem uses SIE-300 and SIE-200 components with CMSDK peripherals to provide a reference design.

1.2 Intended audience

This application note document is written for experienced hardware, System-on-Chip (SoC) and software engineers who might or might not have experience with Arm products. Such engineers typically have experience in writing Verilog and of performing synthesis but might have limited experience of integrating and implementing Arm products.

1.3 Conventions

The following subsections describe conventions used in Arm documents.

1.3.1 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: **https://developer.arm.com/glossary**.

1.3.2 Typographical conventions

Convention	Use
italic	Introduces 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 bold`	Denotes language keywords when used outside example code.
`monospace underline`	Denotes a permitted abbreviation for a command or option. You can enter the underlined text instead of the full command or option name.
<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.
⚠ Caution	This represents a recommendation which, if not followed, might lead to system failure or damage.
⚠ Warning	This represents a requirement for the system that, if not followed, might result in system failure or damage.
⚠ Danger	This represents a requirement for the system that, if not followed, will result in system failure or damage.
Note	This represents an important piece of information that needs your attention.
Tip	This represents a useful tip that might make it easier, better or faster to perform a task.
Remember	This is a reminder of something important that relates to the information you are reading.

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.

1.4 Additional reading

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

Table 1-1 Arm publications

Document name	Document ID	Licensee only
Arm® MPS3 FPGA Prototyping Board Technical Reference Manual	100765	No
Arm® Corstone™ SSE-300 Example Subsystem Technical Reference Manual	101773	No
Arm® Cortex®-M55 Processor Technical Reference Manual	101051	No
Arm® Corstone™ SSE-300 Example Subsystem Configuration and Integration Manual	101774	Yes
Arm® Corstone™ SSE-300 Example Subsystem Technical Overview	101772	No
Arm® Ethos™-U55 NPU Technical reference manual	102420	No
Arm® CoreLink™ SIE-200 System IP for Embedded Technical Reference Manual	DDI 0571	No
Arm® CoreLink™ SIE-300 AXI5 System IP for Embedded Technical Reference Manual	101526	No
Arm® Cortex®-M System Design Kit Technical Reference Manual	DDI 0479	No
Arm® CoreLink™ XHB-500 Bridge Technical Reference Manual	101375	No
MCBQVGA-TS-Display-v12 – Keil MCBSTM32F200 display board schematic	-	No
Arm® MPS3 FPGA Prototyping Board Getting Started Guide	-	No
Arm Custom Instructions: Enabling Innovation and Greater Flexibility on Arm (White Paper from Feb 2020)	-	No
Arm® Debug Interface Architecture Specification ADIv6.0.	IHI 0074	No

Table 1-2 Other publications

Document name	Document ID	Organization
Xilinx User Guide 909 – Dynamic Function Exchange, (was previously titled “Partial Reconfiguration”).	UG909	Xilinx

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.
Non-Confidential

1.5 Feedback

Arm welcomes feedback on this FPGA implementation and its documentation.

1.5.1 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.

1.5.2 Feedback on content

If you have comments on content, send an email to errata@arm.com and give:

- The title Arm® Corstone™ SSE-300 with Cortex®-M55 and Ethos™-U55 : Example Subsystem for MPS3 (Partial Reconfiguration Design) Application Note AN552.
- The number DAI 0552C.
- If applicable, the page number(s) to which your comments refer.
- A concise explanation of your comments.

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.

Arm also welcomes general suggestions for additions and improvements.

1.5.3 Other information

- Arm Documentation, https://developer.arm.com/documentation/
- Arm Technical Support Knowledge Articles, https://www.arm.com/support/technical-support
- Arm Support, https://www.arm.com/support
- Arm Glossary, https://developer.arm.com/documentation/aeg0014/g

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.

1.6 Terms and abbreviations

ACI	Arm Custom Instructions
AHB	Advanced High-performance Bus
APB	Advanced Peripheral Bus
BRAM	Block Random Access Memory
CDE	Custom Datapath Extension
CMSDK	Cortex-M System Design Kit
DMA	Direct Memory Access
DTCM	Data Tightly Coupled Memory
EAM	Exclusive Access Monitor
EPU	Extension Processing Unit
FPGA	Field Programmable Gate Array
FMC	FPGA Mezzanine Card
IDAU	Implementation Defined Attribution Unit
ITCM	Instruction Tightly Coupled Memory
KB	Kilobyte
LUT	Look Up Table
MB	Megabyte
MCC	Motherboard Configuration Controller
MPC	Memory Protection Controller
MSC	Manager Security Controller
PPC	Peripheral Protection Controller
RAM	Random Access Memory
RAZ/WI	Read As Zero / Write Ignored
RTL	Register Transfer Level
SCC	Serial Configuration Controller
SMM	Soft Macrocell Model
SPI	Serial Peripheral Interface
SRAM	Static Random Access Memory
TRM	Technical Reference Manual
UART	Universal Asynchronous Receiver Transmitter

1.7 Arm IP version details

This product uses the following IP packages.

Version	Description
r0p1-00eac0	Arm Corstone™ SSE-300 Example Subsystem The Arm Corstone SSE-300 Example Subsystem is a collection of pre-assembled elements to use as the basis of an Internet of Things (IoT) System on Chip (SoC).
r1p0-00eac0	Arm® Ethos™-U55 NPU The Ethos™-U55 is a Neural Processing Unit (NPU) which improves the inference performance of neural networks.
r1p0	CoreLink™ SIE-300 System IP for Embedded The SIE-300 AXI5 System IP for Embedded provides a set of configurable AXI5 security-aware components.
r3p1	CoreLink SIE-200 System IP for Embedded The CoreLink SIE-200 System IP for Embedded product is a collection of interconnect, peripheral, and TrustZone® controller components for use with a processor that complies with the ARMv8-M processor architecture.
BP210	Cortex-M System Design Kit Full version of the design kit supporting Cortex-M0, Cortex-M0 DesignStart®, Cortex-M0+, Cortex-M3 and Cortex-M4. Also contains the AHB Bus Matrix and advanced AHB components.
r1p1	Arm® CoreLink™ NIC-400
r1p3-00rel1	Arm® PrimeCell Synchronous Serial Port (PL022) Arm PrimeCell Synchronous Serial Port

Table 1-1 : Arm IP versions

Note

The rxpy identifier indicates the revision status of Arm IP referenced in this application note where:
rx: Identifies the major revision of the IP, for example, r1.
py: Identifies the minor revision or modification status of the product, for example, p2.

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.

1.8 Encryption key

Arm supplies the MPS3 prototyping board with a decryption key programmed into the FPGA. This key is needed to enable loading of prebuilt encrypted images.

Note

The FPGA programming file that is supplied as part of the bundle is encrypted.

Warning

A battery supplies power to the key storage area of the FPGA. Any keys stored in the FPGA might be lost when battery power is lost. If this happens you must return the board to Arm for reprogramming of the key

.

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.
Non-Confidential

2 Overview

The AN552 SMM is an implementation of the Arm® Corstone™ SSE-300 with Cortex®-M55 and Ethos™-U55 Example Subsystem in a single Cortex-M55 configuration and the full set of MPS3 Peripherals.

2.1 System block diagram

The following high-level block diagram shows the full MPS3 FPGA System :

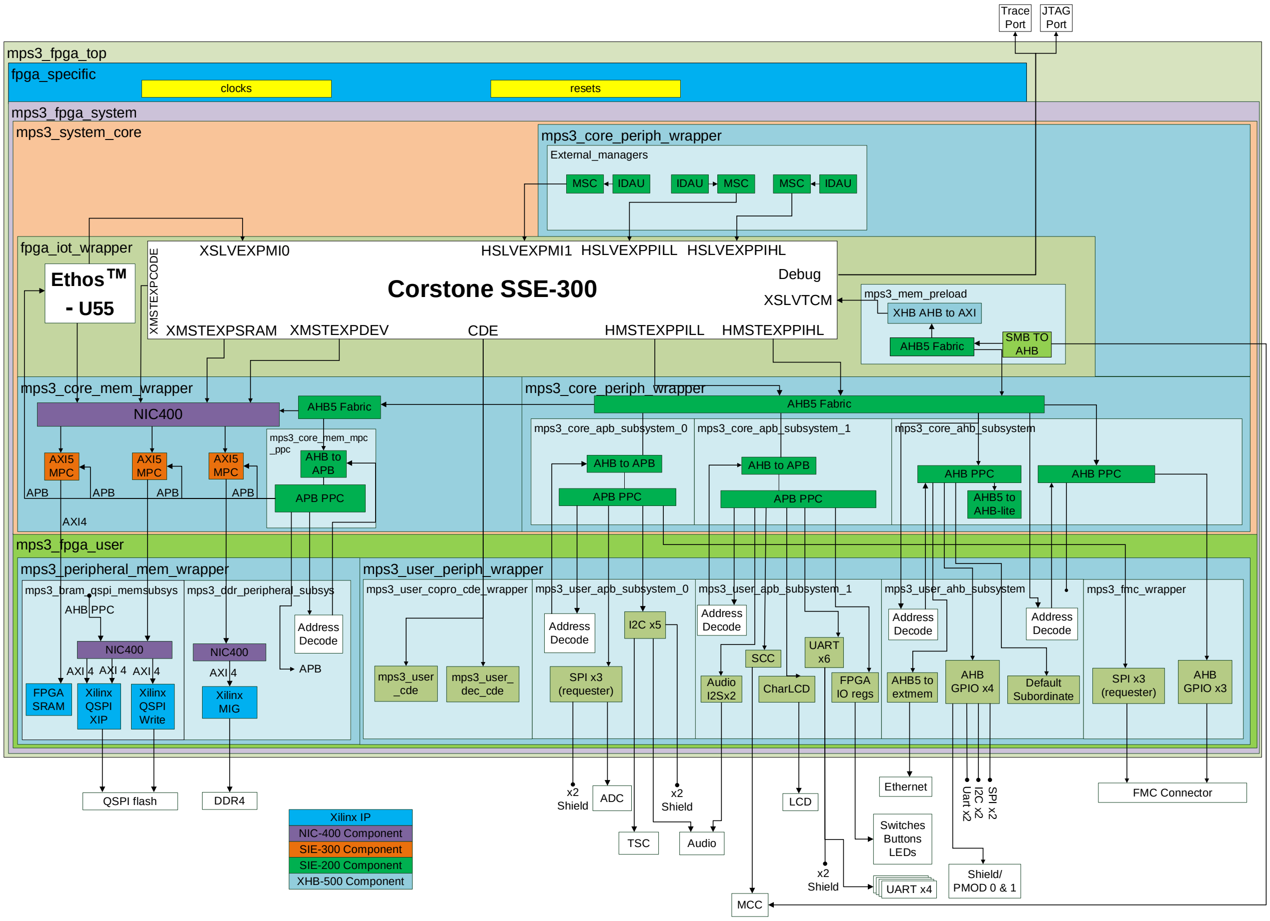


Figure 2-1 : MPS3 system overview

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.
Non-Confidential

2.2 SSE-300 Configuration Settings

The following table shows the configuration settings of the Corstone SSE-300 subsystem in the AN552 SMM. For information on the configuration settings see the *Arm® Corstone™ SSE-300 Example Subsystem Configuration and Integration Manual*.

2.2.1 Render Settings

Configuration Define	SSE-300 Default Value	AN552 Value
NUMCPU	0	0
PILEVEL	1	1
CPU0TYPE	3	3
CPU1TYPE	0	0
CPU2TYPE	0	0
CPU3TYPE	0	0
NUMNPU	1	1
NPU0TYPE	1	1
NPU1TYPE	0	0
NPU2TYPE	0	0
NPU3TYPE	0	0
NPU0_NUM_MACS	128	128
NPU1_NUM_MACS	256	256
NPU2_NUM_MACS	32	32
NPU3_NUM_MACS	64	64
NUM_AXI_SLAVES_EXP_MI	2	2
NUM_AHB_SLAVES_EXP_PIHL	1	1
NUM_AHB_SLAVES_EXP_PILL	1	1
EXPLOGIC_PRESENT	1	1
VMMPCBLKSIZE	7	11
CPU0_INITNSVTOR_ADDR_INIT	0x00000000	0x00000000
CPU0EXPNUMIRQ	64	100
CPU0EXPIRQDIS	64'b0	100'b0
CPU0_EXP_IRQTIER	65'b1	100'b1
CPU0_INT_IRQTIER	32'b1	32'b1
CPU0_EXP_IRQ_PULSE_SPT_PRESENT	64'b0	100'b0
CPU0_EXP_IRQ_SYNC_TO_CPU_PRESENT	65'b1	100'b1
CPU0_EXP_IRQ_SYNC_TO_EWIC_PRESENT	65'b1	100'b1
CPU0_EXP_NMI_PULSE_SPT_PRESENT	0	0
CPU0_EXP_NMI_SYNC_TO_CPU_PRESENT	1	1
CPU0_EXP_NMI_SYNC_TO_EWIC_PRESENT	1	1
DEBUGLEVEL	0	2
CPU0_ITM_PRESENT	1	1
CPU0_ETM_PRESENT	0	1
CPU0_FPU_PRESENT	1	1
CPU0_MVE_CONFIG	2	2
SECEXT	1	1
CPU0_MPU_S	8	16

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.

Configuration Define	SSE-300 Default Value	AN552 Value
CPU0_MPU_NS	8	16
CPU0_SAUDISABLE	0	0
CPU0_NUM_SAU_CONFIG	8	8
CPU0_DBGLVL	2	2
HASCPU0CPIF	1	1
CPU0_INSTR_CACHE_SIZE	0b01111	0b01111
CPU0_DATA_CACHE_SIZE	0b01111	0b01111
CPU0_IRQLVL	3	3
CPU0_ITGUBLKSZ	7	8
CPU0_DTGUBLKSZ	7	8
CPU0_RAR	1	1
CPU0_LOCKSTEP	0	0
CPU0_CFGITCMSZ	0b1001	0b1010
CPU0_CFGDTCMSZ	0b1001	0b1010
CPU0MCUROMADDR	0xE00FE	0xE00FE
CPU0MCUROMVALID	1	1
SOCVAR	0x0	0x0
SOCREV	0x0	0x0
SOCPRTID	0x7E0	0x7E0
SOCIMPLID	0x43B	0x43B
IMPLVAR	0x0	0x0
IMPLREV	0x0	0x0
IMPLPRTID	0x74A	0x74A
IMPLID	0x43B	0x43B
INITTCMEN	0b11	0b11
INITPAHBEN	1	1
LOCKDCAIC	0	0
TCM_MID_WIDTH	5	5
S_MID_WIDTH	5	6
TCM_ID_WIDTH	5	5
XS_ID_WIDTH	6	6
S_HMASTER_WIDTH	5	4
XOM_USER_SIGNAL_PRESENT	0	0
CPU0_PMC_PRESENT	0	0
NUMVMBANK	2	2
VMADDRWIDTH	18	20
HASCRYTO	0	0
HASCSS	0	0
LOGIC_RETENTION_PRESENT	0	0
NSMSCEXPRST	0xA5A5	0xA5A5
MPCEXPDIS	0x5A5A	0xFFF8
MSCEXPDIS	0x5A5A	0xFFF0
BRGEXPDIS	0x5A5A	0x5A5A
PERIPHPPCEXP3DIS	0x5A5A	0xFFFE
PERIPHPPCEXP2DIS	0x5A5A	0xE000

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.
Non-Confidential

Configuration Define	SSE-300 Default Value	AN552 Value
PERIPHPPCEXP1DIS	0x5A5A	**0x0E00**
PERIPHPPCEXP0DIS	0x5A5A	**0x1FC0**
MAINPPCEXP3DIS	0x5A5A	**0x5A5A**
MAINPPCEXP2DIS	0x5A5A	**0x5A5A**
MAINPPCEXP1DIS	0x5A5A	**0xFFF1**
MAINPPCEXP0DIS	0x5A5A	**0xBE00**
PDCMQCHWIDTH	4	4
HASCPU0IWIC	0	0
CPU0CPUIDRST	0	0
COLDRESET_MODE	0	0
BUSPROT_PRESENT	0	0
ECC_PRESENT	0	0
CPU0_CTI_PRESENT	1	1
CFGBIGEND	0	0
CFGMEMALIAS	0b10000	0b10000
CPU0_INITECCEN	0	0
PERIPHERAL_INTERCONNECT_ARBITRATION_SCHEME	“round”	“round”
CPU0_CFGPAHBZE	0b010	0b010
CPU0_LOCKPAHB	1	1
PERFORM_CONFIGCHECK	1	1

Table 3-1 Configuration settings

Note

The above configurations settings match the definitions in the SSE-300 configuration yaml file. The format of the value fields is specific to this configuration file.
Changes to the default configuration are in **Bold.**

2.2.2 Subsystem static input values

The SSE-300 subsystem in AN547 has several inputs which are tied off and therefore static, at the subsystem top level. These are detailed in the below table.

Input	Tie Off Value
CPU0_INITSVTOR [1]	25'h0200000
CPU0CFGFPU	1'b1
CPU0CFGMVE	2'b10
CPU0MPUNSDISABLE	1'b0
CPU0MPUSDISABLE	1'b0
CPU0CFGSSTCALIB	25'h0270FF
CPU0CFGNSSTCALIB	25'h0270FF
CPU0INITL1RSTDIS	1'b0

Table 2-1 : Subsystem static input values

Note

CPU0_INITSVTOR is the value for INITSVTOR0RST specified in the SSE-300 TRM.

2.3 SIE-300 components

The AN552 SMM uses the following SIE-300 components:

- AXI5 Memory Protection Controller.

  There are three MPCs implemented in the AN552 SMM and these are configured with the following block sizes:

  - SRAM MPC, 16KB block size.
  - QSPI MPC, 64KB block size.
  - DDR4 MPC, 1MB block size

2.4 SIE-200 components

The AN552 SMM uses the following SIE-200 components:

- TrustZone AHB5 peripheral protection controller
- TrustZone AHB5 manager security controller
- AHB5 bus matrix
- AHB5 to AHB5 synchronous bridge
- AHB5 to APB synchronous bridge
- TrustZone APB4 peripheral protection controller
- AHB5 default subordinate

2.5 Corelink XHB-500

The AN552 SMM implements one CoreLink XHB-500, configured for AHB to AXI mode.

2.6 Memory protection

The SIE-300 MPC, and SIE-200 PPC components can affect memory and I/O security management and must be configured as required for your application. For more information, see:

- *Arm® CoreLink™ SIE-200 System IP for Embedded Technical Reference Manual*
- *Arm® CoreLink™ SIE-300 AXI5 System IP for Embedded Technical Reference Manual*

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.
Non-Confidential

2.7 Memory map overview

The following figure shows the AN552 memory map and how it relates to the Armv8-M reference memory map. The figure includes IDAU security information for memory regions. For more information, see the *Arm® CoreLink™ SIE-200 System IP for Embedded Technical Reference Manual*.

For information on the SSE-300 subsystem peripherals, see the *Arm® Corstone™ SSE-300 Example Subsystem Technical Reference Manual*.

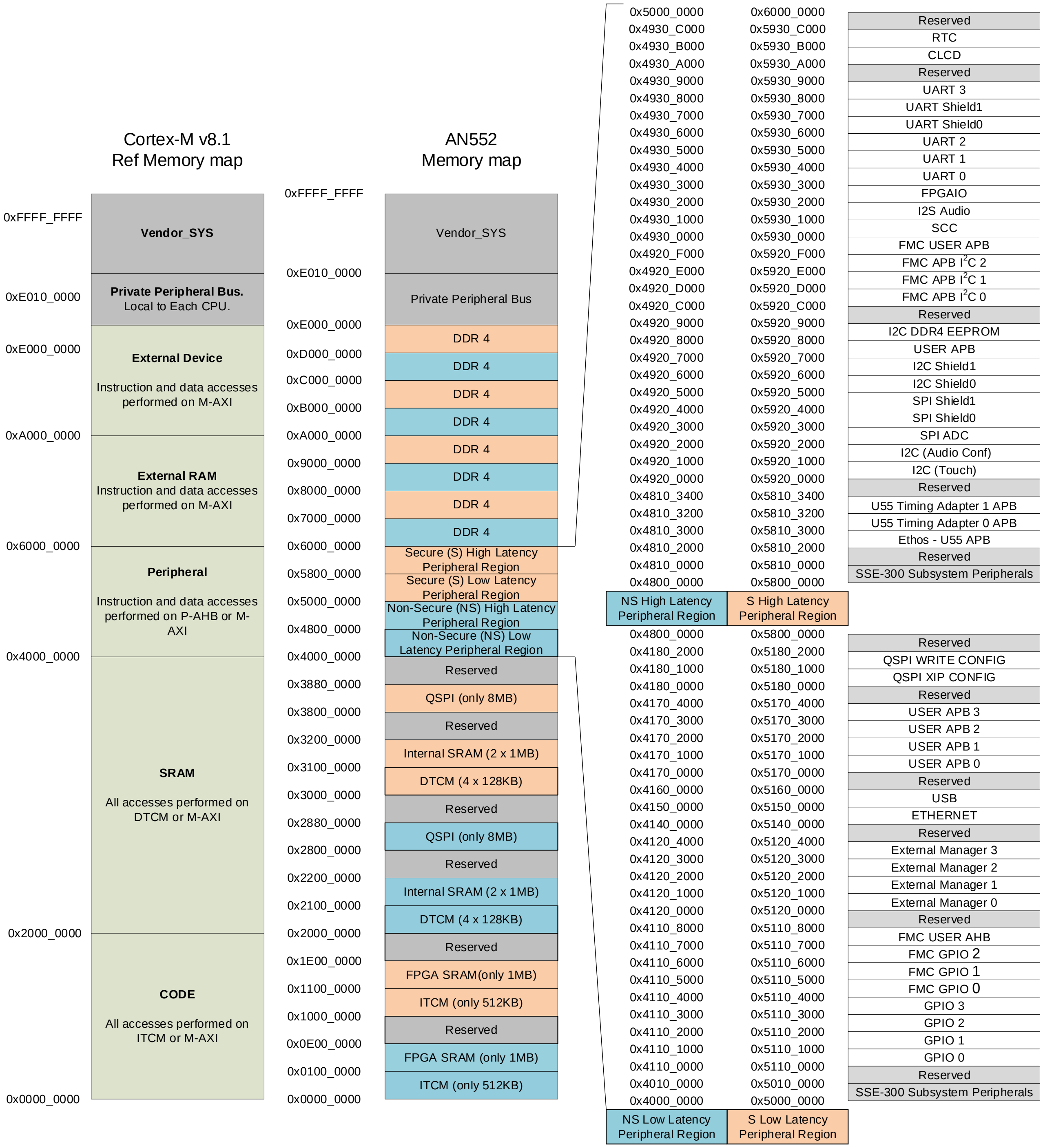


Figure 2-2 : Memory map

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.

The following table shows the AN552 memory map.

ROW	Address		Size	Region Name	Description	Alias with Row ID	IDAU Region Values		
ID	From	To					Security	IDAU ID	NSC
1	0x0000_0000	0x0007_FFFF	512KB	Code	ITCM[3]	5	NS	0	0
2	0x0008_0000	0x00FF_FFFF	15.5MB	Reserved	Reserved				
3	0x0100_0000	0x010F_FFFF	1MB	Code	FPGA SRAM (1MB)[1]	7			
4	0x0110_0000	0x0FFF_FFFF	239MB	Reserved	Reserved				
5	0x1000_0000	0x1007_FFFF	512KB	Code	ITCM[3]	1	S	1	CODE NSC
6	0x1008_0000	0x10FF_FFFF	15.5MB	Reserved	Reserved				
7	0x1100_0000	0x110F_FFFF	1MB	Code	FPGA SRAM (1MB) [1]	3			
8	0x1110_0000	0x1FFF_FFFF	239MB	Reserved	Reserved				
9	0x2000_0000	0x2007_FFFF	512KB	SRAM	DTCM (4 x banks of 128KB)[3]	15			
10	0x2008_0000	0x20FF_FFFF	15.5MB	Reserved	Reserved				
11	0x2100_0000	0x211F_FFFF	2MB	SRAM	Internal SRAM Area (SSE-300 implements 2x1MB)[3]				
12	0x2120_0000	0x27FF_FFFF	110MB	Reserved	Reserved				
13	0x2800_0000	0x287F_FFFF	8MB	SRAM	QSPI (8MB) [1]	19			
14	0x2880_0000	0x2FFF_FFFF	120MB	Reserved	Reserved				
15	0x3000_0000	0x3007_FFFF	512KB	SRAM	DTCM (4 x banks of 128KB)[3]	9	S	3	RAM NSC
16	0x3008_0000	0x30FF_FFFF	15.5MB	Reserved	Reserved				
17	0x3100_0000	0x311F_FFFF	2MB	SRAM	Internal SRAM Area (SSE-300 implements 2x1MB)[3]				
18	0x3120_0000	0x37FF_FFFF	110MB	Reserved	Reserved				
19	0x3800_0000	0x387F_FFFF	8MB	SRAM	QSPI (8MB) [1]	13			
20	0x3880_0000	0x3FFF_FFFF	120MB	Reserved	Reserved				
21	0x4000_0000	0x47FF_FFFF	128MB	Peripheral	Non-Secure Low Latency Peripheral Region	23	NS	4	0
22	0x4800_0000	0x4FFF_FFFF	128MB	Peripheral	Non-Secure High Latency Peripheral Region	24	NS	4	0
23	0x5000_0000	0x57FF_FFFF	128MB	Peripheral	Secure Low Latency Peripheral Region	21	S	5	0
24	0x5800_0000	0x5FFF_FFFF	128MB	Peripheral	Secure High Latency Peripheral Region	22	S	5	0
25	0x6000_0000	0x6FFF_FFFF	256MB	External RAM	DDR4[1]		NS	6	0
26	0x7000_0000	0x7FFF_FFFF	256MB	External RAM	DDR4[1]		S	7	0

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.
Non-Confidential

ROW	Address		Size	Region Name	Description	Alias with Row ID	IDAU Region Values		
ID	From	To					Security	IDAU ID	NSC
27	0x8000_0000	0x8FFF_FFFF	256MB	External device	DDR4[1]		NS	8	0
28	0x9000_0000	0x9FFF_FFFF	256MB	External device	DDR4[1]		S	9	0
29	0xA000_0000	0xAFFF_FFFF	256MB	External device	DDR4[1]		NS	A	0
30	0xB000_0000	0xBFFF_FFFF	256MB	External device	DDR4[1]		S	B	0
31	0xC000_0000	0xCFFF_FFFF	256MB	External device	DDR4[1]		NS	C	0
32	0xD000_0000	0xDFFF_FFFF	256MB	External device	DDR4[1]		S	D	0
33	0xE000_0000	0xE00F_FFFF	1MB	EPPB	External Private Peripheral Bus		Exempt		
34	0xE010_0000	0xE01F_FFFF	1MB	Vendor_SYS	Reserved		NS	E	0
35	0xE020_0000	0xEFFF_FFFF	254MB	Vendor_SYS	Maps to HMSTEXPPILL Expansion Interface[2]		NS	E	0
36	0xF000_0000	0xF00F_FFFF	1MB	Vendor_SYS	Reserved		Exempt		
37	0xF010_0000	0xF01F_FFFF	1MB	Vendor_SYS	Reserved		S	F	0
38	0xF020_0000	0xFFFF_FFFF	254MB	Vendor_SYS	Maps to HMSTEXPPILL Expansion Interface[2]		S	F	0

Table 2-2 : Memory map overview

Note

1. Security Access is controlled by MPC.
2. Accesses to these addresses results in an AHB5 error response.
3. For security settings, control and features, see the *Arm® Corstone™ SSE-300 Example Subsystem Technical Reference Manual*.

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.
Non-Confidential

2.8 Expansion system peripherals

All FPGA peripherals are mapped to four areas of the memory map. The addresses and interfaces to access the four regions are:

Non-secure Low Latency region:

- 0x4000_0000 - 0x47FF_FFFF
- Manager Peripheral Expansion Low Latency Interface HMSTEXPPILL

Non-secure High Latency region:

- 0x4800_0000 - 0x4FFF_FFFF
- Manager Peripheral Expansion High Latency Interface HMSTEXPPIHL

Secure Low Latency region:

- 0x5000_0000 - 0x57FF_FFFF
- Manager Peripheral Expansion Low Latency Interface HMSTEXPPILL

Secure High Latency region:

- 0x5800_0000 - 0x5FFF_FFFF
- Manager Peripheral Expansion High Latency Interface HMSTEXPPIHL

To support TrustZone-Arm v8M and allow Software to map these peripherals to Secure or Non-secure address space, all peripherals are mapped twice and either an APB PPC or an AHB PPC gates access to these peripherals.

2.8.1 Manager Peripheral Expansion Low Latency Interface memory maps (HMSTEXPPILL)

The following table shows the FPGA peripheral mapping to the Non-secure low latency region.

ROW ID	Address		Size	Description	Alias with ROW ID	Port
	From	To				
1	0x4000_0000	0x400F_FFFF		SSE-300 Subsystem Peripherals[1]		
2	0x4010_0000	0x410F_FFFF		Reserved		
3	0x4110_0000	0x4110_0FFF	4KB	CMSDK GPIO 0	30	AHB
4	0x4110_1000	0x4110_1FFF	4KB	CMSDK GPIO 1	31	
5	0x4110_2000	0x4110_2FFF	4KB	CMSDK GPIO 2	32	
6	0x4110_3000	0x4110_3FFF	4KB	CMSDK GPIO 3	33	
7	0x4110_4000	0x4110_4FFF	4KB	FMC CMSDK GPIO 0	34	
8	0x4110_5000	0x4110_5FFF	4KB	FMC CMSDK GPIO 1	35	
9	0x4110_6000	0x4110_6FFF	4KB	FMC CMSDK GPIO 2	36	
10	0x4110_7000	0x4110_7FFF	4KB	FMC USER AHB	37	
11	0x4110_8000	0x411F_FFFF		Reserved		
12	0x4120_0000	0x4120_0FFF	4KB	External Manager 0 (Unused)	39	AHB
13	0x4120_1000	0x4120_1FFF	4KB	External Manager 1 (Unused)	40	
14	0x4120_2000	0x4120_2FFF	4KB	External Manager 2 (Unused)	41	

ROW ID	Address		Size	Description	Alias with ROW ID	Port
	From	To				
15	0x4120_3000	0x4120_3FFF	4KB	External Manager 3 (Unused)	42	
16	0x4120_4000	0x413F_FFFF		Reserved		
17	0x4140_0000	0x414F_FFFF	1MB	Ethernet	44	AHB
18	0x4150_0000	0x415F_FFFF	1MB	USB	45	
19	0x4160_0000	0x416F_FFFF		Reserved		
20	0x4170_0000	0x4170_0FFF	4KB	User APB 0	47	APB (Mem)
21	0x4170_1000	0x4170_1FFF	4KB	User APB 1	48	
22	0x4170_2000	0x4170_2FFF	4KB	User APB 2	49	
23	0x4170_3000	0x4170_3FFF	4KB	User APB 3	50	
24	0x4170_4000	0x417F_FFFF		Reserved		
25	0x4180_0000	0x4180_0FFF	4KB	QSPI XIP Config	52	AHB
26	0x4180_1000	0x4180_1FFF	4KB	QSPI Write Config	53	
27	0x4180_2000	0x47FF_FFFF		Reserved		

Table 2-3 : FPGA peripheral mapping to the Non-secure low latency region

The following table shows the FPGA peripheral mapping to the Secure low latency region.

ROW ID	Address		Size	Description	Alias with ROW ID	Port
	From	To				
28	0x5000_0000	0x500F_FFFF		SSE-300 Subsystem Peripherals[1]		
29	0x5010_0000	0x510F_FFFF		Reserved		
30	0x5110_0000	0x5110_0FFF	4KB	CMSDK GPIO 0	3	AHB
31	0x5110_1000	0x5110_1FFF	4KB	CMSDK GPIO 1	4	
32	0x5110_2000	0x5110_2FFF	4KB	CMSDK GPIO 2	5	
33	0x5110_3000	0x5110_3FFF	4KB	CMSDK GPIO 3	6	
34	0x5110_4000	0x5110_4FFF	4KB	FMC CMSDK GPIO 0	7	
35	0x5110_5000	0x5110_5FFF	4KB	FMC CMSDK GPIO 1	8	
36	0x5110_6000	0x5110_6FFF	4KB	FMC CMSDK GPIO 2	9	
37	0x5110_7000	0x5110_7FFF	4KB	FMC USER AHB	10	
38	0x5110_8000	0x511F_FFFF		Reserved		
39	0x5120_0000	0x5120_0FFF	4KB	External Manager 0 (Unused)	12	AHB
40	0x5120_1000	0x5120_1FFF	4KB	External Manager 1 (Unused)	13	
41	0x5120_2000	0x5120_2FFF	4KB	External Manager 2 (Unused)	14	
42	0x5120_3000	0x5120_3FFF	4KB	External Manager 3 (Unused)	15	
43	0x5120_4000	0x513F_FFFF		Reserved		
44	0x5140_0000	0x514F_FFFF	1M	Ethernet	17	AHB
45	0x5150_0000	0x515F_FFFF	1M	USB	18	
46	0x5160_0000	0x516F_FFFF		Reserved		
47	0x5170_0000	0x5170_0FFF	4KB	User APB 0	20	APB (Mem)
48	0x5170_1000	0x5170_1FFF	4KB	User APB 1	21	
49	0x5170_2000	0x5170_2FFF	4KB	User APB 2	22	
50	0x5170_3000	0x5170_3FFF	4KB	User APB 3	23	
51	0x5170_4000	0x517F_FFFF		Reserved		

ROW ID	Address		Size	Description	Alias with ROW ID	Port
	From	To				
52	0x5180_0000	0x5180_0FFF	4KB	QSPI XIP Config	25	AHB
53	0x5180_1000	0x5180_1FFF	4KB	QSPI Write Config	26	
54	0x5180_2000	0x56FF_FFFF		Reserved		
55	0x5700_0000	0x5700_0FFF	4KB	SRAM Memory Protection Controller (MPC)		APB (Mem)
56	0x5700_1000	0x5700_1FFF	4KB	QSPI Memory Protection Controller (MPC)		
57	0x5700_2000	0x5700_2FFF	4KB	DDR4 Memory Protection Controller (MPC)		
58	0x5700_3000	0x57FF_FFFF		Reserved		

Table 2-4 : FPGA peripheral mapping to the Secure low latency region

Note

1. This is a reserved region for the SSE-300 Subsystem Peripherals, for details see the *Arm® Corstone™ SSE-300 Example Subsystem Technical Reference Manual.*

Reserved regions respond with RAZ/WI when accessed.

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.

2.8.2 Manager Peripheral Expansion High Latency Interface memory maps (HMSTEXPPIHL)

The following table shows the FPGA peripheral mapping to the Non-secure high latency region,

ROW ID	Address		Size	Description	Alias with ROW ID	Port
	From	To				
1	0x4800_0000	0x480F_FFFF		SSE-300 Subsystem Peripherals [1]		
2	0x4810_0000	0x4810_1FFF		Reserved		
3	0x4810_2000	0x4810_2FFF	4KB	Ethos - U55 APB	37	APB0
4	0x4810_3000	0x4810_31FF	0.5KB	U55 timing adapter 0 APB	38	
5	0x4810_3200	0x4810_33FF	0.5KB	U55 timing adapter 1 APB	39	
6	0x4810_3400	0x491F_FFFF		Reserved		
7	0x4920_0000	0x4920_0FFF	4KB	FPGA - SBCon I2C (Touch)	41	APB0
8	0x4920_1000	0x4920_1FFF	4KB	FPGA - SBCon I2C (Audio Conf)	42	
9	0x4920_2000	0x4920_2FFF	4KB	FPGA - PL022 (SPI ADC)	43	
10	0x4920_3000	0x4920_3FFF	4KB	FPGA - PL022 (SPI Shield 0)	44	
11	0x4920_4000	0x4920_4FFF	4KB	FPGA - PL022 (SPI Shield 1)	45	
12	0x4920_5000	0x4920_5FFF	4KB	SBCon (I2C – Shield 0)	46	
13	0x4920_6000	0x4920_6FFF	4KB	SBCon (I2C – Shield 1)	47	
14	0x4920_7000	0x4920_7FFF	4KB	USER APB	48	
15	0x4920_8000	0x4920_8FFF	4KB	FPGA - SBCon I2C (DDR4 EEPROM)	49	
16	0x4920_9000	0x4920_BFFF		Reserved		
17	0x4920_C000	0x4920_CFFF	4KB	FMC APB I^2C 0	51	APB0
18	0x4920_D000	0x4920_DFFF	4KB	FMC APB I^2C 1	52	
19	0x4920_E000	0x4920_EFFF	4KB	FMC APB I^2C 2	53	
20	0x4920_F000	0x4920_FFFF	4KB	FMC USER APB	54	
21	0x4930_0000	0x4930_0FFF	4KB	FPGA - SCC registers	55	APB1
22	0x4930_1000	0x4930_1FFF	4KB	FPGA - I2S (Audio)	56	
23	0x4930_2000	0x4930_2FFF	4KB	FPGA - IO (System Ctrl + I/O)	57	
24	0x4930_3000	0x4930_3FFF	4KB	UART0 - FPGA_UART0	58	
25	0x4930_4000	0x4930_4FFF	4KB	UART1 - FPGA_UART1	59	
26	0x4930_5000	0x4930_5FFF	4KB	UART2 - FPGA_UART2	60	
27	0x4930_6000	0x4930_6FFF	4KB	UART3 - UART Shield 0	61	
28	0x4930_7000	0x4930_7FFF	4KB	UART4 - UART Shield 1	62	
29	0x4930_8000	0x4930_8FFF	4KB	UART5 - FPGA_UART3	63	
30	0x4930_9000	0x4930_9FFF	4KB	Reserved		
31	0x4930_A000	0x4930_AFFF	4KB	CLCD Config Reg	65	
32	0x4930_B000	0x4930_BFFF	4KB	RTC	66	
33	0x4930_C000	0x4FFF_FFFF		Reserved		

Table 2-5: FPGA peripheral mapping to the Non-secure high latency region

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.

The following table shows the FPGA peripheral mapping to the Secure high latency region.

ROW ID	Address		Size	Description	Alias with ROW ID	Port
	From	To				
35	0x5800_0000	0x580F_FFFF		SSE-300 Subsystem Peripherals [1]		
36	0x5810_0000	0x5810_1FFF		Reserved		
37	0x5810_2000	0x5810_2FFF	4KB	Ethos - U55 APB	3	APB0
38	0x5810_3000	0x5810_31FF	0.5KB	U55 timing adapter 0 APB	4	
39	0x5810_3200	0x5810_33FF	0.5KB	U55 timing adapter 1 APB	5	
40	0x5810_3400	0x591F_FFFF		Reserved		
41	0x5920_0000	0x5920_0FFF	4KB	FPGA - SBCon I2C (Touch)	7	APB0
42	0x5920_1000	0x5920_1FFF	4KB	FPGA - SBCon I2C (Audio Conf)	8	
43	0x5920_2000	0x5920_2FFF	4KB	FPGA - PL022 (SPI ADC)	9	
44	0x5920_3000	0x5920_3FFF	4KB	FPGA - PL022 (SPI Shield 0)	10	
45	0x5920_4000	0x5920_4FFF	4KB	FPGA - PL022 (SPI Shield 1)	11	
46	0x5920_5000	0x5920_5FFF	4KB	SBCon (I2C – Shield 0)	12	
47	0x5920_6000	0x5920_6FFF	4KB	SBCon (I2C – Shield 1)	13	
48	0x5920_7000	0x5920_7FFF	4KB	USER APB	14	
49	0x5920_8000	0x5920_8FFF	4KB	FPGA - SBCon I2C (DDR4 EEPROM)	15	
50	0x5920_9000	0x592F_FFFF		Reserved		
51	0x5920_C000	0x5920_CFFF	4KB	FMC APB I^2C 0	17	APB0
52	0x5920_D000	0x5920_DFFF	4KB	FMC APB I^2C 1	18	
53	0x5920_E000	0x5920_EFFF	4KB	FMC APB I^2C 2	19	
54	0x5920_F000	0x5920_FFFF	4KB	FMC USER APB	20	
55	0x5930_0000	0x5930_0FFF	4KB	FPGA - SCC registers	21	APB1
56	0x5930_1000	0x5930_1FFF	4KB	FPGA - I2S (Audio)	22	
57	0x5930_2000	0x5930_2FFF	4KB	FPGA - IO (System Ctrl + I/O)	23	
58	0x5930_3000	0x5930_3FFF	4KB	UART0 - FPGA_UART0	24	
59	0x5930_4000	0x5930_4FFF	4KB	UART1 - FPGA_UART1	25	
60	0x5930_5000	0x5930_5FFF	4KB	UART2 - FPGA_UART2	26	
61	0x5930_6000	0x5930_6FFF	4KB	UART3 - UART Shield 0	27	
62	0x5930_7000	0x5930_7FFF	4KB	UART4 - UART Shield 1	28	
63	0x5930_8000	0x5930_8FFF	4KB	UART5 - FPGA_UART3	29	
64	0x5930_9000	0x5930_9FFF	4KB	Reserved		
65	0x5930_A000	0x5930_AFFF	4KB	CLCD Config Reg	31	
66	0x5930_B000	0x5930_BFFF	4KB	RTC	32	
67	0x5930_C000	0x5FFF_FFFF		Reserved		

Table 2-6: FPGA peripheral mapping to the Secure high latency region

Note

1. This is a reserved region for the SSE-300 Subsystem Peripherals, for details see the *Arm® Corstone™ SSE-300 Example Subsystem Technical Reference Manual.*

Reserved regions respond with RAZ/WI when accessed.

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.

2.9 FPGA Utilization

The AN552 SMM is designed for the MPS3 board which uses a Xilinx Kintex Ultrascale XCKU115 FPGA. The FPGA features up to 8MB BRAM (2160 Block RAM tiles) and up to 663,360 LUTs. The FPGA full part number is XCKU115-FLVB1760-1-C.

The provided AN552 SMM is divided into two logical partitions, the top partition containing the Corstone SSE-300 with Cortex-M55 and Ethos-U55, and a user partition containing an example user design. The two partitions are defined using the Xilinx partial reconfiguration flow. These partial reconfiguration partition have fixed locations and fixed resources. The available resources for the total FPGA, and the user partition are detailed below.

2.9.1 FPGA utilization

The following table shows the numbers of LUTs and BRAMs available in the FPGA, and the numbers used by the AN552 SMM.

Site Type	FPGA total	Used	Utilization %
LUTs	663,360	298,533	45
Block RAM Tile	2160	1088	50

Table 2-7: AN552 SMM total utilization

Note

These numbers relate to the full AN552 SMM. The values cannot be used to infer IP size, or the relative sizes of different IP blocks, because the implementation and system design can significantly differ depending on the target technology.

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.
Non-Confidential

2.9.2 User partition utilization

The user partition area supports 32% of the available FPGA resources. The remaining resources are reserved for the top partition.

Within this user partition, the provided example user design uses 34% of the available logic and 74% of the available memory resources. The user can modify and extend the provided user example design up to the full extent of the available user partition resources.

Note

The ability to fit a user design within the user partition may be affected by resources other than those listed below. In particular, routing requirements may restrict the ability of the user design to use all the resources listed in the table below.

Site Type	User partition total	Used	Utilization %
LUTs	211,128	69925	33
Block RAM Tile	736	287	39

Table 2-8 : User partition utilization

3 Programmers model

This programmers model is supplemental to the CMSDK, SIE-200 and SIE-300 documentation which describes many of the included components in more detail. The connectivity of the system is shown in the System block diagram.

3.1 ITCM

The primary boot memory is an ITCM which is implemented with 512KB of FPGA SRAM connected to the ITCM interface of the Cortex-M55 processor inside the subsystem:

- Size: 512KB of FPGA SRAM
- Address Range: 0x0000_0000 - 0x0007_FFFF
- Alias Range: 0x1000_0000 - 0x1007_FFFF

3.2 FPGA SRAM

The code memory is extended with 2MB of internal FPGA SRAM:

- Size: 1MB of FPGA SRAM
- Address Range: 0x0100_0000 - 0x010F_FFFF
- Alias Range: 0x1100_0000 - 0x110F_FFFF

3.3 DTCM

The primary data memory is provided by DTCM made up of 4 banks, each implemented as 128KB of internal FPGA SRAM connected to the 4 DTCM interfaces of the Cortex-M55 processor inside the subsystem:

- Size: 4 x 128KB of FPGA SRAM
- Address Range: 0x2000_0000 - 0x2007_FFFF
- Alias Range: 0x3000_0000 - 0x3007_FFFF

3.4 QSPI

The AN552 SMM provides 8MB of external Flash memory which is accessed through a read-only QSPI interface:

- Size: 8MB of Flash Memory
- Address Range: 0x2800_0000 - 0x287F_FFFF
- Alias Range: 0x3800_0000 - 0x387F_FFFF

3.5 DDR4

The AN552 SMM provides access to 2GB of External DDR4 memory through the DDR4 controller:

- Size: 2GB of DDR4 (4GB fitted, only 2GB accessible)
- Address Range: 0x6000_0000 - 0xDFFF_FFFF

3.6 AHB GPIO

The AN552 SMM uses seven CMSDK AHB GPIO blocks, each providing 16 bits of I/O. Four of these modules are connected to the two Arduino compatible headers Shields 0 and 1 as follows:

Shield	GPIO
SH0_IO [15:0]	GPIO0[15:0]
SH0_IO [17:16]	GPIO2[1:0]
SH1_IO [15:0]	GPIO1[15:0]
SH1_IO [17:16]	GPIO2[3:2]

Table 3-1 : GPIO mapping

The GPIO alternative function lines select whether peripherals or GPIOs are available on each pin. See Shield Support for mappings.

Three of these modules are connected to the HA, HB and LA FMC GPIO banks. These modules are provided as examples of how to connect between the available AHB ports and the FMC pins. Their connections may be modified, or the GPIO blocks removed entirely, depending on the user FMC application.

3.7 SPI

The AN552 SMM implements six PL022 SPI modules:

- One general purpose SPI module (SPI ADC) communicates with an onboard ADC. The analog pins of the Shield headers connect to the input channels of the ADC. Chip Select is managed by FPGA system control module.
- Two general purpose SPI modules connect to the Shield headers and provide an SPI interface on each header. These are alternative functions on the GPIO ports. See Shield Support for mappings. Select is managed by FPGA system control module.
- Three example SPI modules connect to various of the FMC GPIO pins, (HA, HB and LA). These modules are provided as examples of how to connect between the available APB ports and the FMC pins. Their connections may be modified, or the SPI modules removed entirely, depending on the user FMC application.

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.
Non-Confidential

3.8 SBCon (I^2C)

The AN552 SMM implements five SBCon serial modules:

- One SBCon module for use by the Colour LCD touch interface.
  The base memory addresses are:
  - 0x4920_0000 in the Non-secure high latency peripheral region.
  - 0x5920_0000 in the Secure high latency region.

- One SBCon module to configure the audio controller.
  The base memory addresses are:
  - 0x4920_1000 in the Non-secure high latency peripheral region.
  - 0x5920_1000 in the Secure high latency region.

- Two general purpose SBCon modules that connect to Shield 0 and Shield 1 and provide an I^2C interface on each header. These are alt-functions on the GPIO ports. See Shield Support for mappings.
  The base memory addresses are:
  - Shield 0: 0x4920_3000 in the Non-secure high latency peripheral region.
  - Shield 1: 0x4920_4000 in the Non-secure high latency peripheral region.
  - Shield 0: 0x5920_3000 in the Secure high latency peripheral region.
  - Shield 1: 0x5920_4000 in the Secure high latency peripheral region.

- One SBCon module, used to read EEPROM from DDR4 SODIMM.
  The base memory addresses are:
  - 0x4920_8000 in the Non-secure high latency peripheral region.
  - 0x5920_8000 in the Non-secure high latency peripheral region.

The selftest software provided with AN552 includes example code for the color LCD module control and audio interfaces.

The following table shows the two-wire SBCon registers in address offset order from the base memory address.

Offset	Register Name	Type	Reset	Description
0x000	SB_CONTROL	RAZ/WI	0x0	Bits[31:2]: Reserved
		RW	0b00	Read and set serial control bits: Bit[1] is SDA Bit[0] is SCL
0x004	SB_CONTROLC	RAZ/WI	0x0	Bits[31:2]: Reserved
		WO	0b00	Clear serial control bits: Bit[1] is SDA Bit[0] is SCL

Table 3-2 SBCon registers

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.
Non-Confidential

3.9 UART

The AN552 SMM implements six CMSDK UARTs:

- UART 0 – FPGA_UART0
  - 0x4930_3000 in the Non-secure high latency peripheral region
  - 0x5930_3000 in the Secure high latency peripheral region
- UART 1 – FPGA_UART1
  - 0x4930_4000 in the Non-secure high latency peripheral region
  - 0x5930_4000 in the Secure high latency peripheral region
- UART 2 – FPGA_UART2
  - 0x4930_5000 in the Non-secure high latency peripheral region
  - 0x5930_5000 in the Secure high latency peripheral region
- UART 3 - Shield 0
  - 0x4930_6000 in the Non-secure high latency peripheral region
  - 0x5930_6000 in the Secure high latency peripheral region
- UART 4 - Shield 1
  - 0x4930_7000 in the Non-secure high latency peripheral region
  - 0x5930_7000 in the Secure high latency peripheral region
- UART 5 - FPGA_UART3
  - 0x4930_8000 in the Non-secure high latency peripheral region
  - 0x5930_8000 in the Secure high latency peripheral region

UARTs 3 and 4 are alternative functions on the GPIO ports. See Shield Support for mappings.

3.10 Color LCD parallel interface

The color LCD module has two interfaces:

- Parallel bus for sending image data to the LCD.
- I^{2}C to transfer input data from the touch screen.

The color LCD module is a custom peripheral that provides an interface to a STMicroelectronics STMPE811QTR Port Expander with Advanced Touch Screen Controller on the Keil MCBSTM32C display board. The schematic is listed in the reference section, see Additional reading . The Keil display board contains an AM240320LG display panel and uses a Himax HX8347-D LCD controller.

The selftest software provided with the application note includes drivers and example code for both interfaces.

The base memory addresses of the color LCD parallel interface are:

- 0x4930_A000 in the Non-secure high latency peripheral region
- 0x5930_A000 in the Secure high latency peripheral region

The following table shows the memory map of the color LCD registers in address offset order from the base memory address

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.

Offset	Register Name	Type	Reset	Description
0x000	CHAR_COM	RW	0x0	Write command: A write to this address causes a write to the LCD command register. Read busy status: A read from this address causes a read from the LCD busy register.
0x004	CHAR_DAT	RW	0x0	Write data RAM. A write to this address causes a write to the LCD data register. Read data RAM. A read from this address causes a read from the LCD data register.
0x008	CHAR_RD	RAZ/WI	0x0	Bits[31:8]: Reserved.
		RO	0x0	Bits[7:0] : Captured data from an earlier read command. These bits contain the data from the last request read. Valid only when CHAR_RAW[0] is set.
0x00C	CHAR_RAW	RAZ/WI	0x0	Bits[31:1]: Reserved
		RW	0x0	Bit[0]: Access complete status. 1 indicates Access Complete and data in CHAR_RD is valid. Write 0 to clear access complete flag.
0x010	CHAR_MASK	RAZ/WI	0x0	Bits[31:1]: Reserved
		WO	0x0	Bit[0]: Write interrupt mask. Write 0 to enable Access Complete to generate an interrupt.
0x014	CHAR_STAT	RAZ/WI	0x0	Bits[31:1]: Reserved
		RO	0x0	Bit[0]: is the state of Access Complete ANDed with the CHAR_MASK.
0x04C	CHAR_MISC	RAZ/WI	0x0	Bits[31:7]: Reserved Bits[2]: Reserved
		RW		CLCD control lines:
			0b1	Bit[6]: CLCD_BL
			0b1	Bit[5]: CLCD_RD
			0b1	Bit[4]: CLCD_RS
			0b1	Bit[3]: CLCD_RESET
			0b1	Bit[1]: CLCD_WR
			0b1	Bit[0]: CLCD_CS

Table 3-3 : LCD control and data registers

3.11 Ethernet

The AN552 SMM design connects to an SMSC LAN9220 device through a static memory interface.

The base memory addresses of the Ethernet static memory interface are:

- 0x4140_0000 in the Non-secure low latency peripheral region.
- 0x5140_0000 in the Secure low latency peripheral region.

The selftest software includes example code for an internal loopback operation.

3.12 USB

The AN552 SMM design connects to a Hi-Speed USB OTG controller (ISP1763) device through a static memory interface.

The base memory addresses of the USB OTG static memory interface are:

- 0x4150_0000 in the Non-secure low latency peripheral region.
- 0x5150_0000 in the Secure low latency peripheral region.

The selftest software includes example code for an internal loopback operation.

3.13 Real Time Clock

The AN552 SMM uses the PL031 PrimeCell Real Time Clock Controller (RTC). A 1Hz counter in the RTC enables it to be used as a basic alarm function or long time-based counter.

The base memory addresses of the Real Time Clock controller are:

- 0x4930_B000 in the Non-secure high latency peripheral region.
- 0x4930_B000 in the Secure high latency peripheral region.

3.14 Audio I^{2}S

The I^{2}S interface supports transfer of digital audio to and from the Audio codec.

The base memory addresses of the I^{2}S audio interface are:

- 0x4930_1000 in the Non-secure high latency peripheral region.
- 0x5930_1000 in the Secure high latency peripheral region.

The following table shows the I^{2}S audio registers in address offset order from the base memory address.

Offset	Register Name	Type	Reset	Description
0x000	CONTROL	RAZ/WI	0x0	Bits[31:18], Bit[15], Bit[11], Bits[7:4]: Reserved.
		RW		Control lines:
			0b0	Bit[17]: Audio codec reset control (output pin)
			0b0	Bit[16]: FIFO reset
			0b10	Bits[14:12]: Rx Buffer IRQ Water Level Default 0b10, IRQ triggers when less than two-word space is available.
			0b10	Bits[10:8]: Tx Buffer IRQ Water Level Default 0b10, IRQ triggers when more than two-word space is available.
			0b0	Bit[3]: Rx Interrupt Enable
			0b0	Bit[2]: Rx Enable
			0b0	Bit[1]: Tx Interrupt Enable
			0b0	Bit[0]: Tx Enable
0x004	STATUS	RAZ/WI	0x0	Bits[31:6]: Reserved
		RO		Status Register
			0b0	Bit[5]: Rx Buffer Full
			0b1	Bit[4]: Rx Buffer Empty
			0b0	Bit[3]: Tx Buffer Full
			0b1	Bit[2]: Tx Buffer Empty
			0b0	Bit[1]: Rx Buffer Alert (Depends on Water level)
			0b1	Bit[0]: Tx Buffer Alert (Depends on Water level)
0x008	ERROR	RAZ/WI	0x0	Bits[31:2]: Reserved
		R/W1C		Error Status Register
			0b0	Bit[1]: Rx overrun. Set this bit to clear.
			0b0	Bit[0]: Tx overrun or underrun. Set this bit to clear.
0x00C	DIVIDE	RAZ/WI	0x0	Bits[31:10]: Reserved
		RW		Clock Divide Ratio Register (for left or right clock)
			0x20	Bits[9:0]: LRDIV (Left/Right).

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.
Non-Confidential

Offset	Register Name	Type	Reset	Description
0x010	TXBUF	W		Transmit Buffer FIFO Data Register. This is a write-only register.
			0x0	Bits[31:16]: Left channel
		W	0x0	Bits[15:0]: Right channel
0x014	RXBUF	RO		Receive Buffer FIFO Data Register.
			0x0	Bits[31:16]: Left channel
		RO	0x0	Bits[15:0]: Right channel
0x018-0x2FF	RESERVED	RAZ/WI	0x0	Reserved
0x300	ITCR	RAZ/WI	0x0	Bits[31:1]: Reserved
		RW		Integration Test Control Register
			0b0	Bit[0]: ITCR
0x304	ITIP1	RAZ/WI	0x0	Bits[31:1]: Reserved
		RO		Integration Test Input Register 1
			0b0	Bit[0]: SDIN
0x308	ITOP1	RAZ/WI	0x0	Bits[31:4]: Reserved
		RW		Integration Test Output Register 1
			0b0	Bit[3]: IRQOUT
			0b0	Bit[2]: LRCK
			0b0	Bit[1]: SCLK
			0b0	Bit[0]: SDOUT

Table 3-4 Audio I^{2}S register map

3.15 Audio configuration

The AN552 SMM implements a simple SBCon interface based on I^{2}C. It configures the Cirrus Logic Low Power Codec with Class D Speaker Driver, CS42L52 part on the MPS3 board.

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.

3.16 FPGA system control and I/O

The AN552 implements an FPGA system and I/O control block. The base memory addresses of the control block are:

- 0x4930_2000 in the Non-secure high latency peripheral region.
- 0x5930_2000 in the Secure high latency peripheral region.

The following table shows the FPGA system and I/O control registers in address offset order from the base memory address.

Offset	Register Name	Type	Reset	Description
0x000	FPGAIO->LED0			LED connections
		RAZ/WI	0x0	Bits[31:10]: Reserved
		RW	0x0	Bits[9:0]: LED
0x004	FPGAIO-> M55DBGCTRL	RAZ/WI	0x0	Bits[31:4]: Reserved
				Cortex-M55 control signals
		RW	0b1	Bit[3]: SPNIDEN
		RW	0b1	Bit[2]: SPIDEN
		RW	0b1	Bit[1]: NIDEN
		RW	0b1	Bit[0]: DBGEN
0x008	FPGAIO->BUTTON	RAZ/WI	0x0	Bits[31:2]: Reserved
				Buttons
		R	2b0	Bits[1:0]: Buttons
0x00C	FPGAIO->GPIOALT2			GPIO Alt Function 2 select:
		RAZ/WI	0x0	Bits[31:0]: Reserved
0x010	FPGAIO->CLK1HZ	RW	0x0	Bits[31:0]: 1Hz up counter
0x014	FPGAIO->CLK100HZ	RW	0x0	Bits[31:0]: 100Hz up counter
0x018	FPGAIO->COUNTER	RW	0x0	Bits[31:0]: Cycle Up Counter - Increments when 32-bit prescale counter equals zero and automatically reloads.
0x01C	FPGAIO->PRESCALE			Prescale Reload Value
		RW	0x0	Bits[31:0]: Reload value for prescale counter.
0x020	FPGAIO->PSCNTR			Prescale Counter Value
		RW	0x0	Bits[31:0]: Current value of the prescale counter. The prescale counter is reloaded with PRESCALE after reaching 0.
0x024	RESERVED	RAZ/WI	0x0	Reserved
0x028	FPGAIO->SWITCH			Switches
		RAZ/WI	0x0	Bits[31:8]: Reserved
		R	0x0	Bits[7:0]: Switches

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.

Offset	Register Name	Type	Reset	Description
0x04C	FPGAIO->MISC	RAZ/WI	0x0	Bits[31:3]: Reserved
				Miscellaneous control bits
		RW	0b1	Bit[2] :SHIELD1_SPI_nCS
		RW	0b1	Bit[1]: SHIELD0_SPI_nCS
		RW	0b1	Bit[0]: ADC_SPI_nCS

Table 3-5 : System control and I/O registers

Note

All counters are driven from FPGA generated clock PERIF_CLK.

3.17 Serial Configuration Controller

The AN552 SMM implements a communication channel between the MCC and the FPGA system through a Serial Configuration Controller, (SCC), interface.

The base memory addresses of the SCC are:

- 0x4930_0000 in the Non-secure high latency peripheral region.
- 0x5930_0000 in the Secure high latency peripheral region.

The following table shows the SCC registers in address offset order from the base memory address.

Note

The read-addresses and write-addresses of the SCC interface do not use Bits [1:0]. All address words are word-aligned.

Offset	Register Name	Type	Reset	Description
0x000	CFG_REG0	RAZ/WI	0x0	Bits[31:2]: Reserved
		RW	1b1	Bit[1]: CPU_WAIT ctrl
		RAZ/WI	0b0	Bit[0]: Reserved
0x004	CFG_REG1	RW	0x0	Bits[31:0]: DATA RW
0x008	CFG_REG2	RAZ/WI	0x0	Bits[31:1]: Reserved
		RW	0b0	Bit[0]: QSPI Read / Write select signal Read = 0, Write = 1
0x00C	CFG_REG3	RAZ/WI	0x0	Bits[31:0]: Reserved
0x010	CFG_REG4	RAZ/WI	0x0	Bits[31:4]: Reserved
		RW	0x0	Bits[3:0]: Board Revision [r]
0x014	CFG_REG5	RW	0x0	Bits[31:0]: ACLK Frequency in Hz
0x018 – 0x09C	RESERVED	RAZ/WI	0x0	-
0x0A0	SYS_CFGDATA_RTN	R		Bits[31:0]: DATA RW
0x0A4	SYS_CFGDATA_OUT	W		Bits[31:0]: DATA RW
0x0A8	SYS_CFGCTRL	R	1b0	Bit[31]: Start (generates interrupt on write to this bit)
		RW	1b0	Bit[30]: RW access
		RAZ/WI	0x0	Bits[29:26]: Reserved
		RW	0x0	Bits[25:20]: Function value
		RAZ/WI	0x0	Bits[19:12]: Reserved
		RW	0x0	Bits[11:0]: Device (value of 0/1/2 for supported clocks)
0x0AC	SYS_CFGSTAT	RAZ/WI		Bits[31:2]: Reserved
		R		Bit[1]: Error

Offset	Register Name	Type	Reset	Description
		R		Bit[0]: Complete
0x0B0 – 0xFF4	RESERVED	RAZ/WI		
0xFF8	SCC_AID	R	0x02	SCC AID register is read only Bits[31:24]: FPGA build number, (decimal)
		R	0x1	Bits[23:20]: MPS3 target board revision (A = 0, B = 1, C = 2)
		RAZ/WI	0x7	Bits[19:8]: Reserved
		R	0x8	Bits[7:0]: Number of SCC configuration register
0xFFC	SCC_ID	R	0x41	SCC ID register is read only Bits[31:24]: Implementer ID: 0x41 = Arm
		RAZ/WI	0x0	Bits[23:20]: Reserved
		R	0x5	Bits[19:16]: IP Architecture: 0x5 =AXI
		R	0x552	Bits[15:4]: Primary part number in Binary Coded Decimal, (BCD): 0x552 for AN552
		RAZ/WI	0x1	Bits[3:0]: Reserved

Table 3-6 : SCC registers

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.
Non-Confidential

4 Clock architecture

4.1 Clocks

The following sections describe:

- Input clocks from the MPS3 board to the FPGA.
- Clocks generated internally within the FPGA.

4.1.1 Source clocks

The following table shows clocks generated on the MPS3 board which are input clocks to the FPGA.

MPS3 clock	Input pin	Frequency	Note
REFCLK24MHZ	OSCCLK[0]	24MHz	24MHz reference
ACLK	OSCCLK[1]	32MHz	Programmable oscillator
MCLK	OSCCLK[2]	50MHz	Programmable oscillator
GPUCLK	OSCCLK[3]	50MHz	Programmable oscillator
AUDCLK	OSCCLK[4]	24.576MHz	Programmable oscillator
HDLCDCLK	OSCCLK[5]	23.75MHz	Programmable oscillator
DBGCLK	CS_TCK	Variable	JTAG input. Frequency set by debugger
CFGCLK	CFG_CLK	Variable	SCC register clock. Frequency set by MCC
DDR4_REF_CLK	c0_sys_clk_p/n	100MHz	Differential input clock to DDR4 controller
SMBM_CLK	SMBM_CLK	40MHz, (nominal)	SMB clock. Frequency set by MCC

Table 4-1 : Source clocks

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.
Non-Confidential

4.1.2 Clocks generated within the FPGA

The following table shows clocks generated within the FPGA from source clocks input from the MPS3 board.

FPGA generated clock	MPS3 source clock	Frequency	Note
MAINCLK	OSCCLK[1]	32MHz	Clock source for SSE-300 and all non- APB peripherals in the design
PERIF_CLK	OSCCLK[3]	25MHz	Clock source for APB peripherals
AUDMCLK	AUDCLK	12.288MHz	-
AUDSCLK	AUDCLK	3.072MHz	-
SDMCLK	REFCLK24MHZ	24MHz	-
CLK32KHZ	REFCLK24MHZ	32kHz	-
CLK100HZ	REFCLK24MHZ	100Hz	-
CLK1HZ	REFCLK24MHZ	1Hz	-
CFGCLK	CFG_CLK	Set by MCC	SCC register clock from MCC

Table 4-2 : Generated internal clocks

4.1.3 SSE-300 clocks

The following table shows clocks within the FPGA which are inputs to the SSE-300 subsystem.

SSE-300 clock input	FPGA generated clock	Frequency	Note
SYSCLK	MAINCLK	32MHz	Main System clock
CPU0CLK	MAINCLK	32MHz	CPU clock
AONCLK	MAINCLK	32MHz	Always On clock
CNTCLK	MAINCLK	32MHz	Counter clock
SLOWCLK	CLK32KHZ	32KHz	Slow clock

Table 4-3 : SSE-300 clocks

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.
Non-Confidential

5 FPGA Secure Privilege control

The SSE-300 Subsystem Secure Privilege and Non-secure Privilege control block provides expansion security control signals to control the security gating units outside the subsystem. The following table lists the connectivity of the system security extension signals.

Component Name	Components signals	Security expansion signals
USER MSC	msc_irq	SMSCEXPSTATUS[3:0]
	msc_irq_clear	SMSCEXPCLEAR[3:0]
	cfg_nonsec	NSMSCEXP[0]
APB PPC EXP 0	apb_ppc_irq	SPERIPHPPCEXPSTATUS[0]
	apb_ppc_clear	SPERIPHPPCEXPCLEAR[0]
	cfg_sec_resp	SECRESPCFG
	cfg_non_sec	PERIPHNSPPCEXP0[15:0]
	cfg_ap	PERIPHPPPCEXP0[15:0]
APB PPC EXP 1	apb_ppc_irq	SPERIPHPPCEXPSTATUS[1]
	apb_ppc_clear	SPERIPHPPCEXPCLEAR[1]
	cfg_sec_resp	SECRESPCFG
	cfg_non_sec	PERIPHNSPPCEXP1[15:0]
	cfg_ap	PERIPHPPPCEXP1[15:0]
APB PPC EXP 2	apb_ppc_irq	SPERIPHPPCEXPSTATUS[2]
	apb_ppc_clear	SPERIPHPPCEXPCLEAR[2]
	cfg_sec_resp	SECRESPCFG
	cfg_non_sec	PERIPHNSPPCEXP2[15:0]
	cfg_ap	PERIPHPPPCEXP2[15:0]
AHB PPC EXP 0	ahb_ppc_irq	SMAINPPCEXPSTATUS[0]
	ahb_ppc_clear	SMAINPPCEXPCLEAR[0]
	cfg_sec_resp	SECRESPCFG
	cfg_non_sec	MAINNSPPCEXP0[15:0]
	chg_ap	MAINPPPCEXP0[15:0]
AHB PPC EXP 1	ahb_ppc_irq	SMAINPPCEXPSTATUS[1]
	ahb_ppc_clear	SMAINPPCEXPCLEAR[1]
	cfg_sec_resp	SECRESPCFG
	cfg_non_sec	MAINNSPPCEXP1[15:0]
	chg_ap	MAINPPPCEXP1[15:0]
MPC SSRAM	secure_error_irq	SMPCEXPSTATUS[2]

Table 5-1 : Security expansion signals connectivity

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.
Non-Confidential

The following table lists the peripherals that are controlled by the SMSCEXP port.
Each MSC interface is controlled by SMSCEXPSTATUS[n] and SMSCEXPCLEAR[n].

AHB user MSC interface number<n>	Name
0	Reserved
1	User MSC 1
2	User MSC 2
3	User MSC 3
15:4	Reserved

Table 5-2 : Peripherals mapping of AHB MSC EXP

The following table lists the peripherals that are controlled by PERIPHERAL PPC EXP 0.
Each APB <n> interface is controlled by PERIPHNSPPCEXP0[n] and PERIPHPPPCEXP0[n].

APB PPC EXP 0 interface number<n>	Name
0	USER MEM APB 0
1	USER MEM APB 1
2	USER MEM APB 2
3	USER MEM APB 3
4	Ethos - U55 APB
5	U55 timing adapter 0 & 1 APB
12:6	Reserved
13	SSRAM Memory Protection Controller (MPC)
14	QSPI Memory Protection Controller (MPC)
15	DDR4 Memory Protection Controller (MPC)

Table 5-3 : Peripherals mapping of APB PPC EXP 0

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.
Non-Confidential

The following table lists the peripherals that are controlled by PERIPHERAL PPC EXP 1.
Each APB <n> interface is controlled by PERIPHNSPPCEXP1[n] and PERIPHPPPCEXP1[n].

APB PPC EXP 1 interface number<n>	Name
0	FPGA - SBCon I2C (Touch)
1	FPGA - SBCon I2C (Audio Conf)
2	FPGA - PL022 (SPI ADC)
3	FPGA - PL022 (SPI Shield 0)
4	FPGA - PL022 (SPI Shield 1)
5	SBCon (I2C – Shield 0)
6	SBCon (I2C – Shield 1)
7	User APB
8	I2C DDR4 EPROM
11:9	Reserved
12	FMC APB I^2C 0
13	FMC APB I^2C 1
14	FMC APB I^2C 2
15	FMC USER APB

Table 5-4 : Peripherals mapping of APB PPC EXP 1

The following table lists the peripherals that are controlled by PERIPHERAL PPC EXP 2.
Each APB <n> interface is controlled by PERIPHNSPPCEXP2[n] and PERIPHPPPCEXP2[n].

APB PPC EXP 2 interface number<n>	Name
0	FPGA - SCC registers
1	FPGA - I2S (Audio)
2	FPGA – I/O (System Ctrl + I/O)
3	UART0 - FPGA_UART0
4	UART1 - FPGA_UART1
5	UART2 - FPGA_UART2
6	UART3 - UART Shield 0
7	UART4 - UART Shield 1
8	UART5 - FPGA_UART3
9	Reserved
10	CLCD
11	RTC
15:12	Reserved

Table 5-5 : Peripherals mapping of APB PPC EXP 2

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.

The following table lists the peripherals that are controlled by MAIN PPC EXP 0.
Each APB <n> interface is controlled by MAINNSPPCEXP0[n] and MAINPPPCEXP0[n].

AHB PPC EXP 0 interface number<n>	Name
0	GPIO_0
1	GPIO_1
2	GPIO_2
3	GPIO_3
4	FMC GPIO 0
5	FMC GPIO 1
6	FMC GPIO 2
7	FMC AHB User
8	USB and Ethernet
15:7	Reserved

Table 5-6 : Peripherals mapping of AHB PPC EXP 0

The following table lists the peripherals that are controlled by MAIN PPC EXP 1.
Each APB <n> interface is controlled by MAINNSPPCEXP1[n] and MAINPPPCEXP1[n].

AHB PPC EXP 1 interface number<n>	Name
0	Reserved
1	AHB User 1
2	AHB User 2
3	AHB User 3
15:4	Reserved

Table 5-7 : Peripherals mapping of AHB PPC EXP 1

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.
Non-Confidential

6 Interrupt map

The following table shows how the interrupts in the AN552 SMM extend the SSE-300 interrupt map.

Interrupt Input	Interrupt Source	Source
IRQ[0]	Non-secure Watchdog reset Request	SSE-300
IRQ[1]	Non-secure Watchdog Interrupt	
IRQ[2]	SLOWCLK Timer	
IRQ[3]	Timer 0	
IRQ[4]	Timer 1	
IRQ[5]	Timer 2	
IRQ[6]	Reserved	
IRQ[7]	Reserved	
IRQ[8]	Reserved	
IRQ[9]	MPC Combined (Secure)	
IRQ[10]	PPC Combined (Secure)	
IRQ[11]	MSC Combined (Secure)	
IRQ[12]	Bridge Error Combined Interrupt (Secure)	
IRQ[13]	Reserved	
IRQ[14]	MGMT_PPU	
IRQ[15]	SYS_PPU	
IRQ[16]	CPU0_PPU	
IRQ[17]	Reserved	
IRQ[18]	Reserved	
IRQ[19]	Reserved	
IRQ[20]	Reserved	
IRQ[21]	Reserved	
IRQ[22]	Reserved	
IRQ[23]	Reserved	
IRQ[24]	Reserved	
IRQ[25]	Reserved	
IRQ[26]	DEBUG_PPU	
IRQ[27]	TIMER 3 AON	
IRQ[28]	CPU0CTIIRQ0	
IRQ[29]	CPU0CTIIRQ01	
IRQ[30]	Reserved	
IRQ[31]	Reserved	
IRQ[32]	System timestamp counter interrupt	FPGA System
IRQ[33]	UART 0 Receive Interrupt	
IRQ[34]	UART 0 Transmit Interrupt	
IRQ[35]	UART 1 Receive Interrupt	
IRQ[36]	UART 1 Transmit Interrupt	
IRQ[37]	UART 2 Receive Interrupt	

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.
Non-Confidential

Interrupt Input	Interrupt Source	Source
IRQ[38]	UART 2 Transmit Interrupt	
IRQ[39]	UART 3 Receive Interrupt	FPGA System
IRQ[40]	UART 3 Transmit Interrupt	
IRQ[41]	UART 4 Receive Interrupt	
IRQ[42]	UART 4 Transmit Interrupt	
IRQ[43]	UART 0 Combined Interrupt	
IRQ[44]	UART 1 Combined Interrupt	
IRQ[45]	UART 2 Combined Interrupt	
IRQ[46]	UART 3 Combined Interrupt	
IRQ[47]	UART 4 Combined Interrupt	
IRQ[48]	UART Overflow (0, 1, 2, 3, 4 & 5)	
IRQ[49]	Ethernet	
IRQ[50]	Audio I^2S	
IRQ[51]	Touch Screen	
IRQ[52]	USB	
IRQ[53]	SPI ADC	
IRQ[54]	SPI (Shield 0)	
IRQ[55]	SPI (Shield 1)	
IRQ[56]	U55 Interrupt	
IRQ[68:57]	Reserved	
IRQ[69]	GPIO 0 Combined Interrupt	
IRQ[70]	GPIO 1 Combined Interrupt	
IRQ[71]	GPIO 2 Combined Interrupt	
IRQ[72]	GPIO 3 Combined Interrupt	
IRQ[88:73]	GPIO 0 individual interrupts	
IRQ[104:89]	GPIO 1 individual interrupts	
IRQ[120:103]	GPIO 2 individual interrupts	
IRQ[124:121]	GPIO 3 individual interrupts	
IRQ[125]	UART 5 Receive Interrupt	
IRQ[126]	UART 5 Transmit Interrupt	
IRQ[127]	UART 5 Combined Interrupt	
IRQ[130:128]	Reserved	

Table 6-1 : Combined SSE-300 and FPGA system interrupt map

UART interrupts

There are six CMSDK UARTs in the AN552 SMM, each with the following interrupt pins:

- **TXINT**
- **RXINT**
- **TXOVRINT**
- **EXOVRINT**
- **UARTINT**

The **TXINT**, **RXINT** and **UARTINT** interrupt signals of each UART drive a single interrupt input of the SSE-300 Example Subsystem. In addition, the **TXOVERINT** and **EXOVRINT** interrupt signals of all six UARTs, twelve signals in all, are logically ORed together to drive IRQ[47].

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.
Non-Confidential

7 Shield support

This AN552 SMM supports external shield devices. To enable the Shield support, two SPI, two UART and two I²C interfaces are multiplexed with GPIO over the Shield Headers.

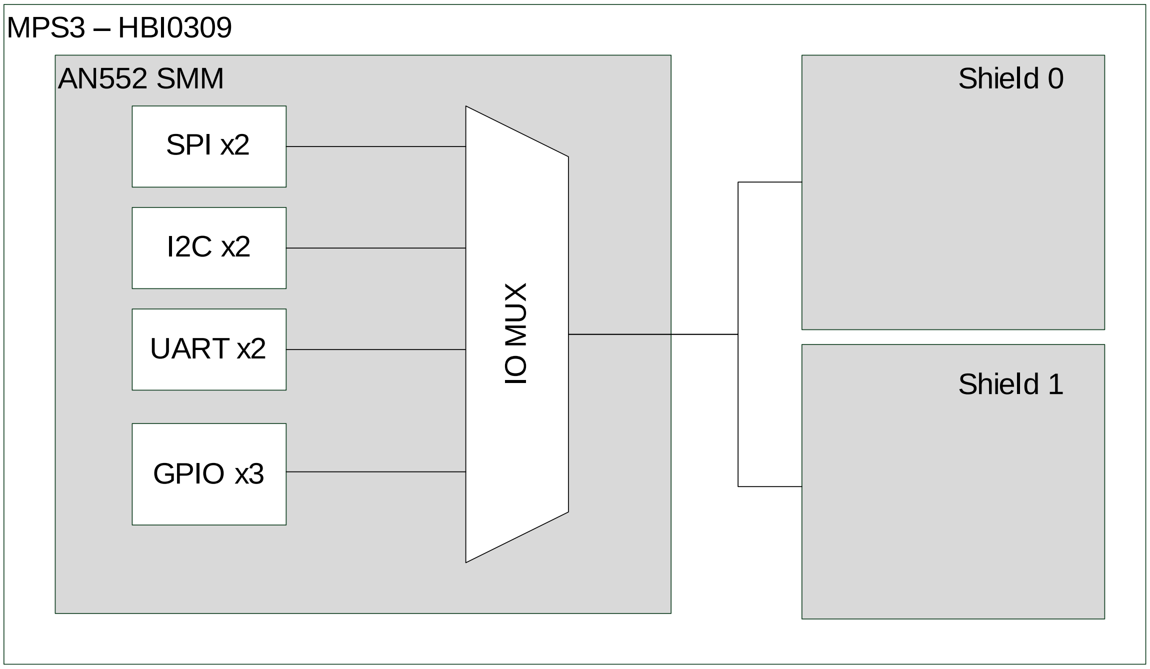


Figure 7-1 : Shield device expansion

Multiplexing is controlled by the alternative function output from the associated GPIO Register. A second alternative function is multiplexed for pins 1-9 of Shield 0 and these are controlled through GPIOALT2 in the FPGAIO Registers at address offset 0x0C.

The following table shows the multiplexed output functions ALTF1 and ALTF2.

Shield interface pin	GPIO	ALTF1	Description
SH0_IO0	GPIO0_0	UART3 RXD – SH0_RXD	Shield 0 UART Receive
SH0_IO1	GPIO0_1	UART3 TXD – SH0_TXD	Shield 0 UART Transmit
SH0_IO2	GPIO0_2	-	-
SH0_IO3	GPIO0_3	-	-
SH0_IO4	GPIO0_4	-	-
SH0_IO5	GPIO0_5	-	-
SH0_IO6	GPIO0_6	-	-
SH0_IO7	GPIO0_7	-	-
SH0_IO8	GPIO0_8	-	-
SH0_IO9	GPIO0_9	-	-
SH0_IO10	GPIO0_10	SPI3 SS – SH0_nCS	Shield 0 SPI Chip Select
SH0_IO11	GPIO0_11	SPI3 MOSI – SH0_DO	Shield 0 SPI Data Out

Shield interface pin	GPIO	ALTF1	Description
SH0_IO12	GPIO0_12	SPI3 MISO – SH0_DI	Shield 0 SPI Data In
SH0_IO13	GPIO0_13	SPI3 SCK – SH0_CLK	Shield 0 SPI Clock
SH0_IO14	GPIO0_14	SBCON2 SDA – SH0_SDA	Shield 0 I2C Data
SH0_IO15	GPIO0_15	SBCON2 SCL – SH0_SCL	Shield 0 I2C Clock
SH1_IO0	GPIO1_0	UART4 RXD – SH1_RXD	Shield 1 UART Receive
SH1_IO1	GPIO1_1	UART4 TXD – SH1_TXD	Shield 1 UART Transmit
SH1_IO2	GPIO1_2	-	-
SH1_IO3	GPIO1_3	-	-
SH1_IO4	GPIO1_4	-	-
SH1_IO5	GPIO1_5	-	-
SH1_IO6	GPIO1_6	-	-
SH1_IO7	GPIO1_7	-	-
SH1_IO8	GPIO1_8	-	-
SH1_IO9	GPIO1_9	-	-
SH1_IO10	GPIO1_10	SPI4 SS – SH1_nCS	Shield 1 SPI Chip Select
SH1_IO11	GPIO1_11	SPI4 MOSI – SH1_DO	Shield 1 SPI Data Out
SH1_IO12	GPIO1_12	SPI4 MISO – SH1_DI	Shield 1 SPI Data In
SH1_IO13	GPIO1_13	SPI4 SCK – SH1_CLK	Shield 1 SPI Clock
SH1_IO14	GPIO1_14	SBCON3 SDA – SH1_SDA	Shield 1 I2C Data
SH1_IO15	GPIO1_15	SBCON3 SCL – SH1_SCL	Shield 1 I2C Clock

Table 7-1 : Shield alternative function pinout

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.
Non-Confidential

8 FMC-HPC support

The AN552 SMM supports the FMC-HPC interface, fitted to the MPS3 board.

Due to the requirements of the partial reconfiguration flow, the pin connectivity and configuration of the FMC connector is fixed within the supplied encrypted bitstream. The following table lists the pin mapping of the FMC connector.

FMC Pins	Function	Configuration	FMC Wrapper pins
HA_P/N[23:0]	Bi-directional GPIO	24 Differential pairs set as 1.8V LVDS 100R termination	HA_I[23:0] HA_O[23:0] HA_T[23:0]
HB_P/N[21:0]	Bi-directional GPIO	22 Differential pairs set as 1.8V LVDS 100R termination	HB_I[21:0] HB_O[21:0] HB_T[21:0]
LA_P/N[33:0]	Bi-directional GPIO	34 Differential pairs set as 1.8V LVDS 100R termination	LA_I[33:0] LA_O[33:0] LA_T[33:0]
CLK_BIDIR_P/N[3:2]	Bi-directional Clock	2 Differential pairs set as 1.8V LVDS 100R termination	CLK_BIDIR[3:2] CLK_BIDIR [3:2] CLK_BIDIR [3:2]
CLK_M2C_P/N[1:0]	Input clocks	2 Differential pairs set as 1.8V LVDS 100R termination	CLK_M2C_I[1:0]
DP_M2C_P/N[9:0]	High-speed Serial Input	Unsupported	-
-	Reset Input Released after configuration	Negative sense reset from MCC	FMC_nPRSNT

Table 8-1 :FMC connector pin connectivity and configuration

Note

The fixed encrypted system bitstream provides the pinout and configuration, which cannot be modified by the user.

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.

8.1 User wrapper

The FMC I/O pins are connected from the top-level I/O, through the appropriate I/O differential buffers, to the `mps3_user_fmc_wrapper.v`, located within `<install_dir>/Luna/Logical/Resources/mps3_user_peripheral/AN552/peripheral_subsystem`

In addition to the I/O pins from the FMC-HPC connector, the user wrapper has four AHB ports and four APB ports. The memory locations of these ports are detailed in Memory map overview and Expansion system peripherals. The user can connect any suitable AHB or APB peripheral to these ports.

In the example design provided, three of the AHB ports are connected to AHB GPIO modules, and three of the APB ports are connected to APB SPI modules. These connections are provided as design examples for the user to modify or remove as required.

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.
Non-Confidential

8.2 GPIO pin control

The FMC GPIO pins, (HA, HB and LA), use the Xilinx IOBUFDS primitive. This primitive supports bi-directional differential signaling.

Direction of the IOBUFDS is controlled by the "T" pin, which is routed to the `mps3_user_fmc_wrapper.v` to allow user control.

- The "T" pin is asserted low, 0, for the user logic to drive signals out of the FMC connector.
- The "T" pin is asserted high, 1, for the FMC connector to drive signals into the user logic.

8.3 FMC memory map

The FMC port memory locations are detailed below. These locations are further detailed in the Memory Map Overview

8.3.1 FMC GPIO 0

- Size: 4KB
- Address Range: 0x4110_4000 - 0x4110_4FFF
- Alias Range: 0x5110_4000 - 0x5110_4FFF

8.3.2 FMC GPIO 1

- Size: 4KB
- Address Range: 0x4110_5000 - 0x4110_5FFF
- Alias Range: 0x5110_5000 - 0x5110_5FFF

8.3.3 FMC GPIO 2

- Size: 4KB
- Address Range: 0x4110_6000 - 0x4110_6FFF
- Alias Range: 0x5110_6000 - 0x5110_6FFF

8.3.4 FMC USER AHB

- Size: 4KB
- Address Range: 0x4110_7000 - 0x4110_7FFF
- Alias Range: 0x5110_7000 - 0x5110_7FFF

8.3.5 FMC APB I^{2}C 0

- Size: 4KB
- Address Range: 0x4920_C000 - 0x4920_CFFF
- Alias Range: 0x5920_C000 - 0x5920_CFFF

8.3.6 FMC APB I^{2}C 1

- Size: 4KB
- Address Range: 0x4920_D000 - 0x4920_DFFF

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.
Non-Confidential

- Alias Range: 0x5920_D000 - 0x5920_DFFF

8.3.7 FMC APB I^{2}C 2

- Size: 4KB
- Address Range: 0x4920_E000 - 0x4920_EFFF
- Alias Range: 0x5920_E000 - 0x5920_EFFF

8.3.8 FMC USER APB

- Size: 4KB
- Address Range: 0x4920_F000 - 0x4920_FFFF
- Alias Range: 0x5920_F000 - 0x5920_FFFF

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.
Non-Confidential

9 Arm Custom Instructions

Cortex-M55 cores support Arm Custom Instructions (ACIs) and implement the Custom Datapath Extension (CDE) for Armv8-M. For more information on ACI and CDE, see the *Arm® Cortex®-M55 Processor Technical Reference Manual*, and *Arm Custom Instructions: Enabling Innovation and Greater Flexibility on Arm* (White Paper from Feb 2020).

The current design implements connection to user modifiable example designs of mps3_user_cde and mps3_user_dec_cde modules. The CDE example module represents trigonometry functions as reference design for ACI implementation.

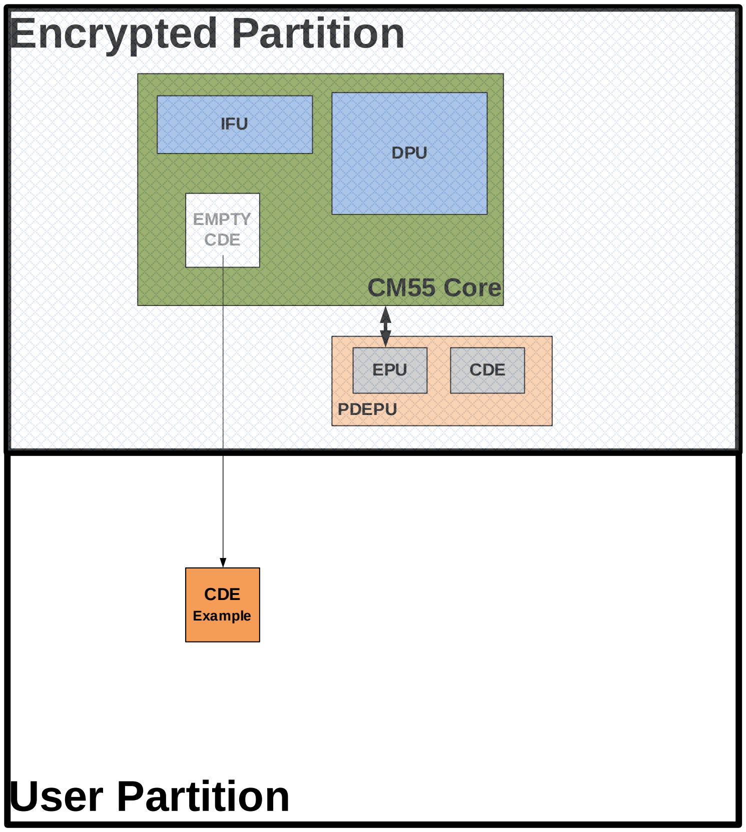


Figure 10-1 CDE modules in design

CDE example implementations are in the release bundle path:

- `Luna/Logical/Resources/mps3_user_peripheral/AN552/peripheral_subsystem/mps3_user_cde.sv`
- `Luna/Logical/Resources/mps3_user_peripheral/AN552/peripheral_subsystem/mps3_user_dec_cde.sv`

Selftest software can provide you with code examples for interaction with the current implementations of the CDE module.

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.
Non-Confidential

10 ZIP bundle

10.1 Bundle contents

The accompanying zip bundle contains:

- This Application Note Document.
- An example Keil® MDK Version 5.34 software project, that can be run on the MPS3 board peripherals and interfaces.
- The directory `Luna/Logical/Resources/mps3_user_peripheral/` which contains the user partition modifiable code.
- The directory `Luna/Logical/Resources/mps3_common_system/` which contains the top-level RTL code required for rebuilding the FPGA. This code should not be modified.
- The directory `Luna/FPGA/AN552/smm_toplevel/xilinx/user_pr_checkpoints/` which contains the pre-built FPGA databases to allow for FPGA place and route.
- `Boardfiles/` directory containing the directory structure and files to be loaded onto the MPS3 SD Card. This is required to configure the MPS3 board to load and run this implementation.

10.2 Bundle directory structure

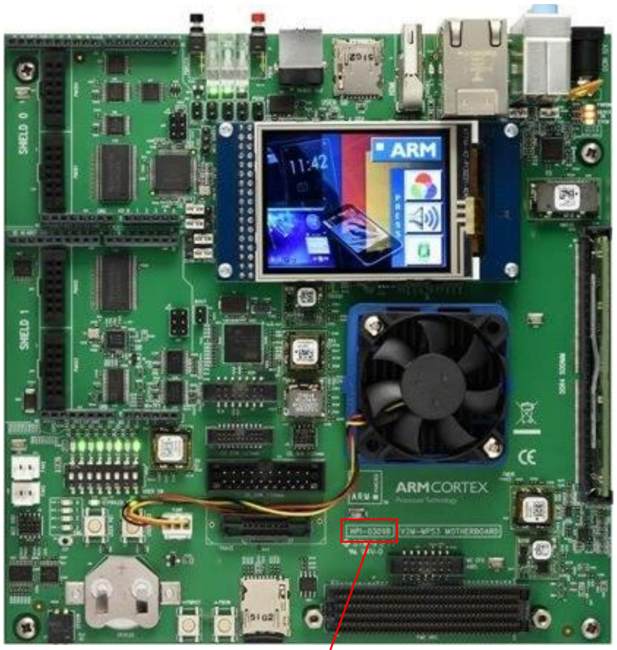
The directory structure of the bundle is shown below.

```
|-- Boardfiles
|    |-- MB
|    |    |-- BRD_LOG.TXT
|    |    |-- HBI0309B
|    |    `-- HBI0309C
|    |-- SOFTWARE
|    |    |-- an552_st.axf
|    `-- config.txt
|-- Docs
|    `-- DAI0552B_SSE300_with_M55_and_U55_FPGA_for_mps3.pdf
|-- Licence.pdf
|-- Luna
|    |-- FPGA
|    |    `-- AN552
|   `-- Logical

|       |-- AN552_SMM_SSE300

|       `-- Resources

|-- Software

|   `-- selftest

|       |-- apaaci

|       |-- apclcd

|       |-- apgpio

|       |-- aplan

|       |-- apleds

|       |-- apmain

|       |-- apmem

|       |-- apqspi

|       |-- aprtc

|       |-- apssp

|       |-- aptimer

|       |-- aptsc

|       |-- apuart

|       |-- apusb

|       |-- RTE

|       `-- v2m_mps3

|-- Release_Notes.txt

`-- revision_history.txt
```

11 Board revision and support

11.1 Identifying the MPS3 board revision

The bundle supports MPS3 board revisions B and C. The board revision, if not known, can be identified from the silk screen text, inside a marked box, on the board as shown in the picture below :



Board Part Number and Revision

Figure 11-1 : MPS3 board revision identifier

In this example the part number is “HBI0309B”. The last letter at the end of the part number denotes the board revision. The illustration shows a revision B board. Bundle support for specific MPS3 board revisions.

There are two subdirectories in the `Boardfiles/MB/` directory that correspond to the two supported revisions:

- `HBI0309B`
- `HBI0309C`

The contents of these directories, within the provided bundle, are identical but the MCC only uses the contents from the directory whose name matches the board part number and revision being used. See Identifying the MPS3 board revision for further details on how to identify the board part number and revision.

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.
Non-Confidential

12 Using AN552 on the MPS3 board

12.1 Prerequisites

Before attempting to use the board, you must:

Read the *Arm® MPS3 FPGA Prototyping Board Technical Reference Manual*.

- In particular, become familiar with the description of the configuration and boot flow.

You must be able to:

- Connect a PC to the MPS3 board Debug USB connector.
- Power the MPS3 board. The MPS3 board appears as a mapped drive named `V2M_MPS3`.
- Understand how to power up, reset, and establish a serial terminal over the USB connection to a host PC.

12.2 Loading a prebuilt image onto the MPS3 Board

To load the prebuilt AN552 image, follow these steps:

1. Power up the MPS3 board using the PBON push button and wait for the `V2M_MPS3` drive to appear.

2. Format the V2MMPS3 drive and copy the contents of `<install_dir>/Boardfiles` and paste them into the root directory of the attached V2M_MPS3 drive.

Note

You can manually modify and merge the contents for certain configuration files. Alternatively, you can restore the existing configuration files from the `/Boardfiles` directory. The affected configuration files are:

```
a. <install_dir>/Boardfiles/config.txt
b. <install_dir>/Boardfiles/MB/HBI0309X/board.txt
```

3. Eject the V2M_MPS3 volume from your computer to unmount the drive.

4. Power cycle the MPS3 board using the PBRST push button.

5. Start the MCC firmware update and FPGA configuration by pressing the PBON push button. The LEDs flash rapidly to indicate that new MCC firmware is being downloaded, (this only occurs the first time the firmware is updated), and that the prebuilt image is being downloaded onto the board.

When the FPGA configuration, and MCC active LEDs next to PBRST button show solid green and the user LEDs UL0-7 are lit in a walking pattern, (individually lit from lowest to highest and back again), the FPGA is programmed.

The color LCD touch screen shows the MPS3 splash screen. Simultaneously, if you have configured the UART to run, the debug UART terminal shows the selftest menu for Application Note AN552.

If the MPS3 board does not boot correctly, refer to the `log.txt` in the root directory of the MPS3 board which provides a log file of the files loaded at bootup.

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.
Non-Confidential

12.3 UART Serial ports

The AN552 SMM support four serial ports which are accessible through the MPS3 board Debug USB port:

- Serial Port 0 is connected to the MCC and outputs debug information about the status of the MCC.
- Serial Port 1 is connected to UART 0.
- Serial Port 2 is connected to UART 1.
- Serial Port 3 is connected to UART 2.

Note

The logical<>physical mapping of the serial ports on a host PC can be confusing due to the way the driver may allocate the port numbers. The serial port presented with the lowest number aligns to Serial Port 0 above.

12.4 UART serial port terminal emulator settings

All serial ports on the AN552 SMM use the following terminal/serial port settings:

Baud Rate:	115200 bps
New-Line:	CR (Serial port 0) And LF (Serial Port 1,2 and 3 Only)
Data:	8 bits
Parity:	none
Stop:	1 bit
Flow control:	none

12.5 MPS3 USB serial port drivers for Windows

For information on installing drivers to support the USB serial ports on the MPS3, see: https://community.arm.com/oss-platforms/w/docs/589/accessing-mps3-serial-ports-in-windows-10

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.
Non-Confidential

12.6 MCC Memory mapping

The MCC on the MPS3 has some visibility into the memory for initiating boot memory areas and configuring peripherals if needed. This access is limited to just 4x 64MB, so it is unable to cover the whole map, hence only those regions which are necessary for the design functionality are mapped.

The following table shows the memory map as viewed from the MCC.

CS	MCC SMB Address	MCC Internal	SSE-300 Address	Size	IOFPGA
1	0x0000_0000 - 0x0007_FFFF	0x6000_0000 - 0x6007_FFFF	0x0000_0000 - 0x0007_FFFF	512KB	ITCM NS
	0x0100_0000 – 0x011F_FFFF	0x6100_0000 - 0x6107_FFFF	0x1000_0000 - 0x1007_FFFF	512KB	ITCM S
	0x0200_0000 - 0x0207_FFFF	0x6200_0000 - 0x621F_FFFF	0x0100_0000 - 0x010F_FFFF	1MB	FPGA SRAM NS
	0x0300_0000 - 0x031F_FFFF	0x6300_0000 - 0x631F_FFFF	0x1100_0000 - 0x110F_FFFF	1 MB	FPGA SRAM S
2	0x0400_0000 - 0x04FF_FFFF	0x6400_0000 - 0x64FF_FFFF	0x4100_0000 - 0x41FF_FFFF	16 MB	Low Latency Peripherals NS
	0x0500_0000 - 0x05FF_FFFF	0x6500_0000 - 0x65FF_FFFF	0x4900_0000 - 0x49FF_FFFF	16 MB	High Latency Peripherals NS
	0x0600_0000 - 0x06FF_FFFF	0x6600_0000 - 0x66FF_FFFF	0x5100_0000 - 0x51FF_FFFF	16 MB	Low Latency Peripherals S
	0x0700_0000 - 0x07FF_FFFF	0x6700_0000 - 0x67FF_FFFF	0x5900_0000 - 0x59FF_FFFF	16 MB	High Latency Peripherals S
3	0x0800_0000 - 0x0BFF_FFFF	0x6800_0000 - 0x6BFF_FFFF	0x6000_0000 - 0x63FF_FFFF	64 MB	DDR4 NS
4	0x0C00_0000 - 0x0FFF_FFFF	0x6C00_0000 - 0x6FFF_FFFF	0x7000_0000 - 0x73FF_FFFF	64 MB	DDR4 S

Table 12-1 : MCC memory map

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.
Non-Confidential

13 Modifying and building AN552 FPGA images

13.1 Partial reconfiguration

AN552 for MPS3 uses the Xilinx partial reconfiguration, (PR), flow. With partial reconfiguration, specific design blocks can be allocated to a PR partition. These partitions can then be compiled to independent bitstreams. The PR bitstreams can be loaded to the FPGA, changing the functionality of the FPGA within the PR design block.

In this flow, the mps3_fpga_user subsystem is designed as a PR partition, and the contents of that partition can be modified by the user. The remaining functionality, (SSE-300 subsystem with Cortex®-M55 and Ethos^{TM}-U55), is delivered as a pre-compiled encrypted bitstream and cannot be modified.

To enable the user to compile the modified versions of the mps3_fpga_user subsystem, a Xilinx Design Checkpoint (DCP) file is provided. This is a preplaced design file containing all placement and routing for the enclosing top-level functionality which wraps around the mps3_fpga_user subsystem.

Note

For further understanding of partial reconfiguration using the Xilinx PR flow, see the *Xilinx User Guide 909 – Dynamic Function Exchange*, (was previously titled "Partial Reconfiguration").

With reference to the Xilinx Partial Reconfiguration terminology; "static image" aligns with the top-level encrypted bitstream, and Reconfigurable Module, (RM), aligns with PR partition.

13.2 Pre-requisites

To build the AN552 FPGA, the user must have a licensed copy of Xilinx Vivado ML Edition, version 2021.1 onwards. The license must also support partial reconfiguration.

The Vivado executable must be in the users path.

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.

13.3 Flow overview

The files provided to the user consist of;

- Top-level static DCP's :
  - `<install_Dir>/Luna/FPGA/AN552/smm_toplevel/xilinx/user_pr_checkpoints/mps3_fpga_top_static_base.dcp`
  - `<install_Dir>/Luna/FPGA/AN552/smm_toplevel/xilinx/user_pr_checkpoints/mps3_system_core_synth.dcp`
- Encrypted bitstream containing the top level and SSE-300 subsystem, `<install_Dir>/Boardfiles/MB/HBI0309X/AN552/552_t_X.bit.`
- Source files to build mps3_fpga_user PR partition.

In overview the flow consists of:

1. User synthesizes mps3_fpga_user into a DCP file.
2. The top level static DCP is combined with mps3_fpga_user DCP, and a stub DCP for the system core.
3. Place and route is then run. Note that since the top-level is preplaced and routed, only the mps3_fpga_user partition is placed and routed.
4. PR bitfile is produced for the mps3_fpga_user PR partition. Two files are produced for any PR partition; a clearing bitstream to clear the appropriate part of FPGA configuration memory, and the programming bitstream. These two bitstreams are named `552_uc_X.bit`, (clearing), and `552_u_X.bit`, (programming).
5. Top-level static encrypted bitfile downloaded to MPS3 board.
6. The two user PR partition bitfiles are downloaded to MPS3 board, (clear programming file followed by content programming file).
7. SSE-300 subsystem boots.

13.4 Flow detail

The user partition code is located in `<install_dir>/Luna/Logical/Resources/mps3_user_peripheral/AN552`. The top-level file, `mps3_fpga_user.v` is further located in the `<install_dir>/Luna/Logical/Resources/mps3_user_peripheral/AN552/user_wrapper` directory.

To build a new version of AN552, perform the following steps:

1. Modify the code in the hierarchy under `mps3_fpga_user.v` to include your new code.

   - The ports of `mps3_fpga_user.v` itself must not be changed as these match the provided top level DCP. It is strongly recommended that the user add their code within one of the existing hierarchical layers rather than directly into `mps3_fpga_user.v.`

2. Navigate to `<install_dir>/Luna/FPGA/AN552/smm_toplevel/xilinx/scripts`.

3. If different version numbers are required for the planned bitfiles, edit `user_pr_impl.tcl` and set the variable *FPGA_BUILD* to the desired single digit number.

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.
Non-Confidential

Note

The version number of the supplied files is 2, (decimal). The default value of FPGA_BUILD set in the user scripts is 2. Therefore, in order to avoid any new bitfiles overwriting the pre-compiled files it is suggested that the value of FPGA_BUILD is modified. This value can be any single decimal digit.

4. For a Linux system, execute `./user_pr_flow.scr`.
   For a Windows system execute `user_pr_flow.bat` from Vitis HLS Command Prompt.
   - When the flow has completed it produces two bitfiles, `552_u_X.bit`, and `552_uc_X.bit`. These are written to the `<install_dir>/Boardfiles/MB/HBI0309C/AN552` directory. "X" is the value of `FPGA_BUILD` written into `user_pr_impl.tcl`.

5. Copy the new bitfiles `552_u_X.bit`, and `552_uc_X.bit`. to the corresponding directory on the MPS3 board.

6. Edit the configuration file `an552_v3.txt`, in the same directory, to use the new files.

```
F1FILE: 552_uc_3.bit     ;FPGA1 Filename - clear system PR – change this line
F1MODE: FPGA             ;FPGA1 Programming Mode
F2FILE: 552_u_3.bit      ;FPGA2 Filename - write system PR– change this line
F2MODE: FPGA             ;FPGA2 Programming Mode
```

7. Power up the MPS3 board.

8. Check, using either the debug UART, or `log.txt` files, that the new files are successfully programmed.

The MPS3 board is now programmed with the user code.

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.
Non-Confidential

14 Software

14.1 Rebuilding software

Pre-requisites:

- The software directory from the bundle
- Keil µVision® 5.34 or later

To rebuild the software, perform the following steps with the provided software package:

1. Navigate to `<install_dir>/Software/selftest/`
2. Load `selftest_mpb.uvprojx` in Keil µVision
3. Once loaded, the project can be rebuilt by selecting one of the following:
    - Project - > Build Target
    - Project - > Rebuild all target files

The output can then be found in `<install_dir>/Software/selftest/an552_st.axf`

14.2 Loading software on the MPS3 board

Pre-requisites:

- MPS3 board powered and USB cable connected
- MPS3 USB mass storage open in a file explorer

To load the software, perform the following steps:

1. Copy the binary executable `<install_dir>/Software/selftest/an552_st.axf` to the board `<MPS3_dir>/Software` folder
2. Open `<MPS3_dir>MB/HBI0309X/AN552/images.txt` in a text editor
3. Add a new line for the new software you wish to run and make sure the other lines are commented out. The following example shows an552_st.axf selected and selftest.axf commented out.

```
;IMAGE0FILE: \SOFTWARE\selftest.axf; - selftest uSD

IMAGE0FILE: \SOFTWARE\an552_st.axf  ; - selftest uSD
```

The MPS3 can now be booted according to the instructions in the *Arm® MPS3 FPGA Prototyping Board Getting Started Guide* that is supplied with the MPS3 board.

15 Debug

In the AN552 SMM, the subsystem includes an example debug infrastructure that instantiatesDAP-Lite2, debug timestamp generator, Cortex-M55 TPIU, and MCU debug ROM table. The DAP-Lite2 is compliant with *Arm® Debug Interface Architecture Specification ADIv6.0*.

For more information about debug infrastructure, see the *Arm® Corstone™ SSE-300 Example Subsystem Technical Reference Manual*.

15.1 Debug Connectivity

The following table shows the supported connectivity between the MPS3 board debug connectors and supported debug in the FPGA implementation:

Debug Connector Type	P-JTAG Debug	SWD	4-bit Trace
20 pin Cortex debug and ETM	Yes	Yes	No
20 pin IDC	Yes	Yes	No
Mictor 38	Yes	Yes	No

Table 15-1 : Debug connectivity and support

The following picture shows the location of the debug connectors on the MPS3 board.

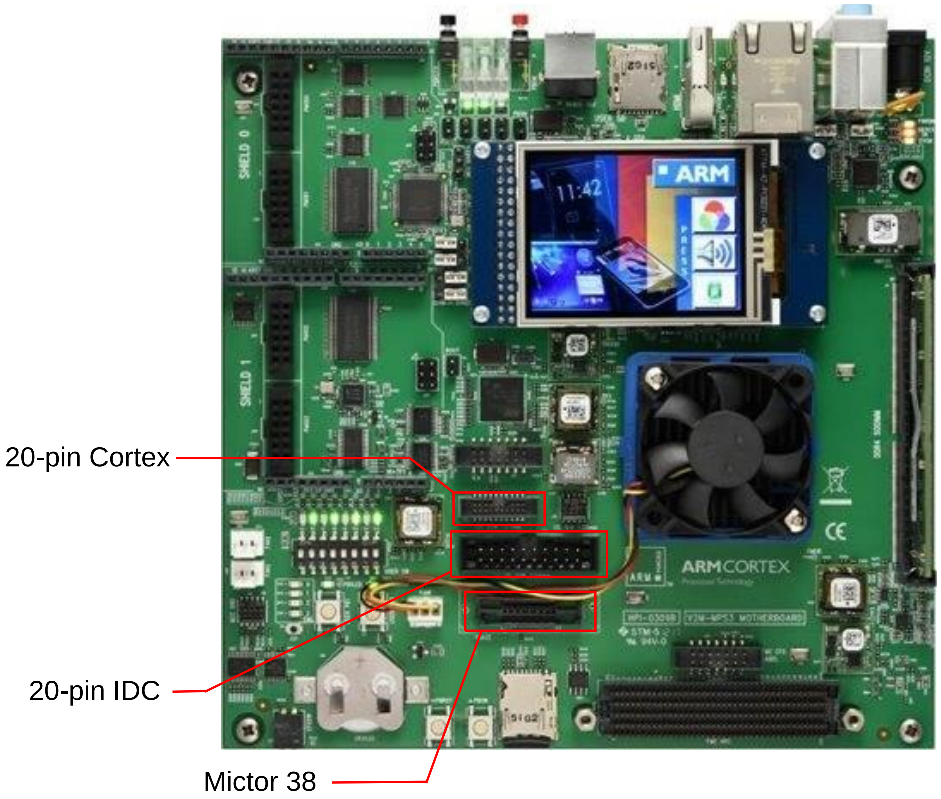


Figure 15-1 : MPS3 Prototyping Board debug connector locations

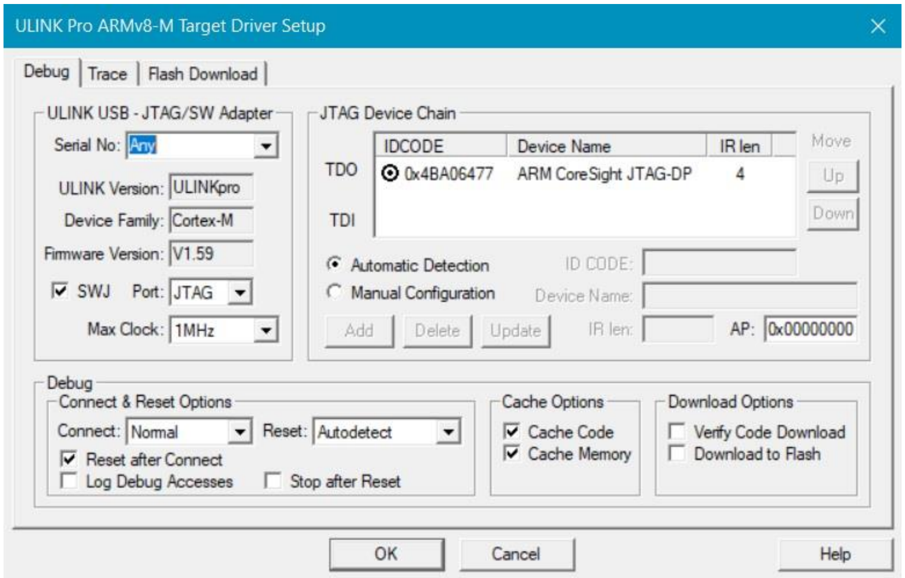
Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.

15.2 Debug support for Keil MDK

Debug has been tested using Keil uVision 5.34 using Arm® Keil® ULINK™ Pro Armv8-M Debugger or CMSIS-DAP Armv8-M Debugger.

If using the ULINK Pro Armv8-M Debugger, apply the following debug settings.

- Port: JTAG
- Reset: Autodetect
- Connect: Normal



Serial No: Any
ULINK Version: ULINKpro
Device Family: Cortex-M
Firmware Version: V1.59
☑ SWJ Port: JTAG
Max Clock: 1MHz

	IDCODE	Device Name	IR len
TDO	⊙ 0x4BA06477	ARM CoreSight JTAG-DP	4
TDI			

● Automatic Detection
○ Manual Configuration
ID CODE:
Device Name:
IR len:
AP: 0x00000000

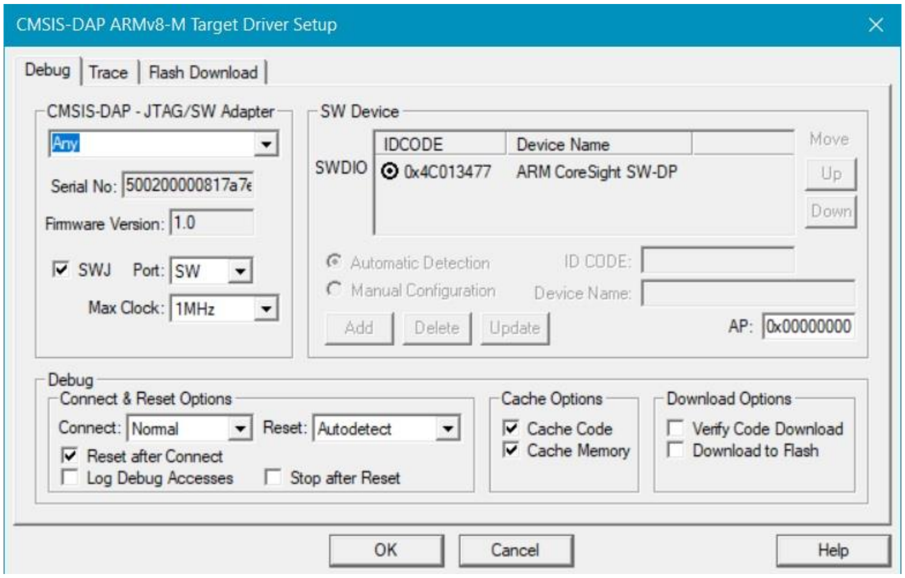
Connect: Normal
Reset: Autodetect
☑ Reset after Connect
☐ Log Debug Accesses
☐ Stop after Reset
☑ Cache Code
☑ Cache Memory
☐ Verify Code Download
☐ Download to Flash

Figure 15-2 :Keil MDK debug configuration

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.

If using the CMSIS-DAP Armv8-M debugger, apply the following settings.

- Port: SW
- Reset: Autodetect
- Connect: Normal



CMSIS-DAP ARMv8-M Target Driver Setup

Debug | Trace | Flash Download

CMSIS-DAP - JTAG/SW Adapter

Any

Serial No: 500200000817a7e

Firmware Version: 1.0

☑ SWJ Port: SW

Max Clock: 1MHz

SW Device

	IDCODE	Device Name
SWDIO	● 0x4C013477	ARM CoreSight SW-DP

● Automatic Detection ID CODE:

○ Manual Configuration Device Name:

AP: 0x00000000

Debug

Connect & Reset Options

Connect: Normal Reset: Autodetect

☑ Reset after Connect

□ Log Debug Accesses □ Stop after Reset

Cache Options

☑ Cache Code

☑ Cache Memory

Download Options

□ Verify Code Download

□ Download to Flash

Figure 15-3 :Keil MDK debug configuration

15.3 Trace support for Keil MDK

It is planned to include trace support for SSE-300 in future versions of the Keil Tool. Please follow the announcements of tool and pack updates related to the platform.

15.4 Debug and trace support for Arm Development Studio

Development Studio 2020.1 Silver edition or above is required as this provides the support for the subsystem in this implementation and was the version used for testing of this SMM.

15.4.1 Trace support for Arm Development Studio

This SMM has full 4-bit trace support through the use of DSTREAM and Arm Development Studio.

15.4.2 Pre-Requisites for establishing a debug session

Before establishing a debug connection to the Cortex-M55 processor, you must first ensure that:

- The MPS3 board is powered on and the FPGA bit file has loaded. See 12.2.
- The Development Studio debugger is power up and connected to the host running the Development Studio software.
- The debugger is connected to the MPS3 Prototyping Board through one of the debug connectors, the 20-pin Cortex, the 20-pin IDC, or the MICTOR 38 connector.

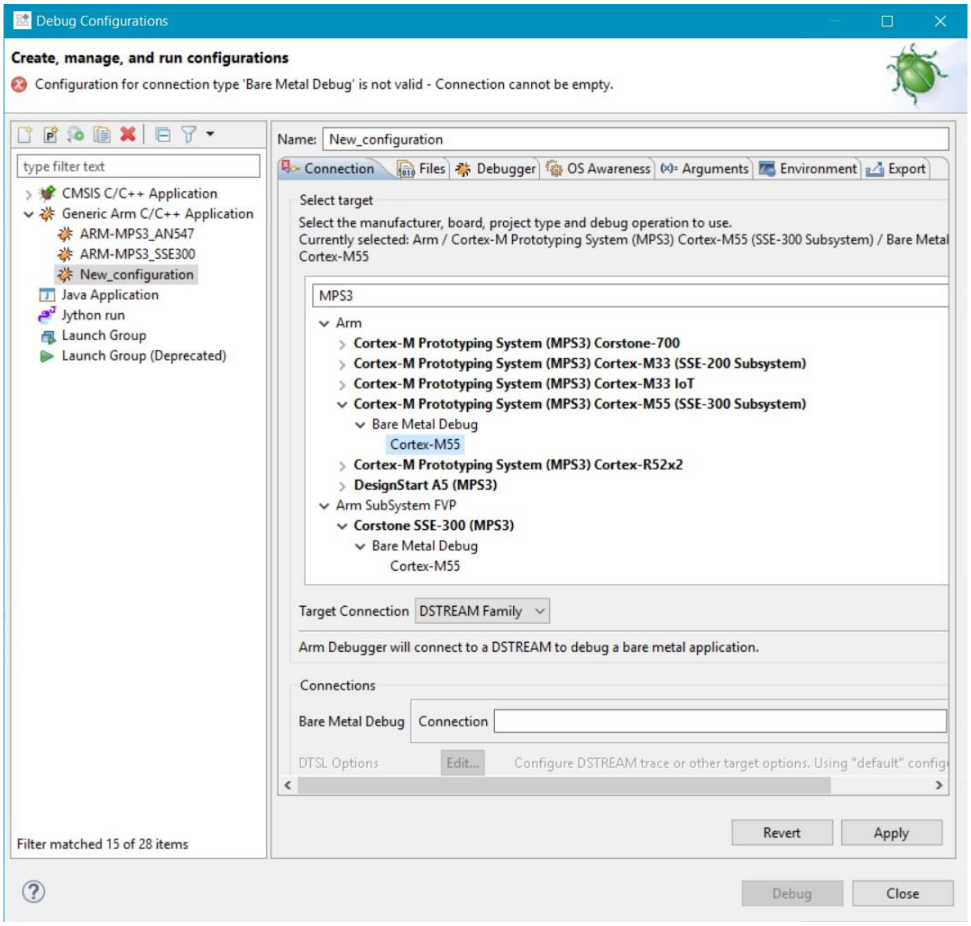
See 15.1 for the location of the debug connectors.

15.4.3 Establishing a debug session

1. Configure the debug session:
   a. Right-click in the Debug Control window and select Debug configurations. The Debug Configurations dialog box appears.
   b. Double left-click on the **Generic ArmC/C++ application**. This creates a new configuration.
   c. In the **Connection** tab, enter MPS3 in the search bar.

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.
Non-Confidential

d. Under Cortex-M Prototyping System (MPS3) Cortex-M55 (SSE-300 Subsystem), select Cortex-M55.



Debug Configurations

Create, manage, and run configurations

Configuration for connection type 'Bare Metal Debug' is not valid - Connection cannot be empty.

type filter text

- CMSIS C/C++ Application
- Generic Arm C/C++ Application
  - ARM-MPS3_AN547
  - ARM-MPS3_SSE300
  - New_configuration
- Java Application
- Jython run
- Launch Group
- Launch Group (Deprecated)

Filter matched 15 of 28 items

Name: New_configuration

Connection | Files | Debugger | OS Awareness | Arguments | Environment | Export

Select target

Select the manufacturer, board, project type and debug operation to use.
Currently selected: Arm / Cortex-M Prototyping System (MPS3) Cortex-M55 (SSE-300 Subsystem) / Bare Metal
Cortex-M55

MPS3

- Arm
  - Cortex-M Prototyping System (MPS3) Corstone-700
  - Cortex-M Prototyping System (MPS3) Cortex-M33 (SSE-200 Subsystem)
  - Cortex-M Prototyping System (MPS3) Cortex-M33 IoT
  - Cortex-M Prototyping System (MPS3) Cortex-M55 (SSE-300 Subsystem)
    - Bare Metal Debug
      - Cortex-M55
  - Cortex-M Prototyping System (MPS3) Cortex-R52x2
  - DesignStart A5 (MPS3)
- Arm SubSystem FVP
  - Corstone SSE-300 (MPS3)
    - Bare Metal Debug
      - Cortex-M55

Target Connection DSTREAM Family

Arm Debugger will connect to a DSTREAM to debug a bare metal application.

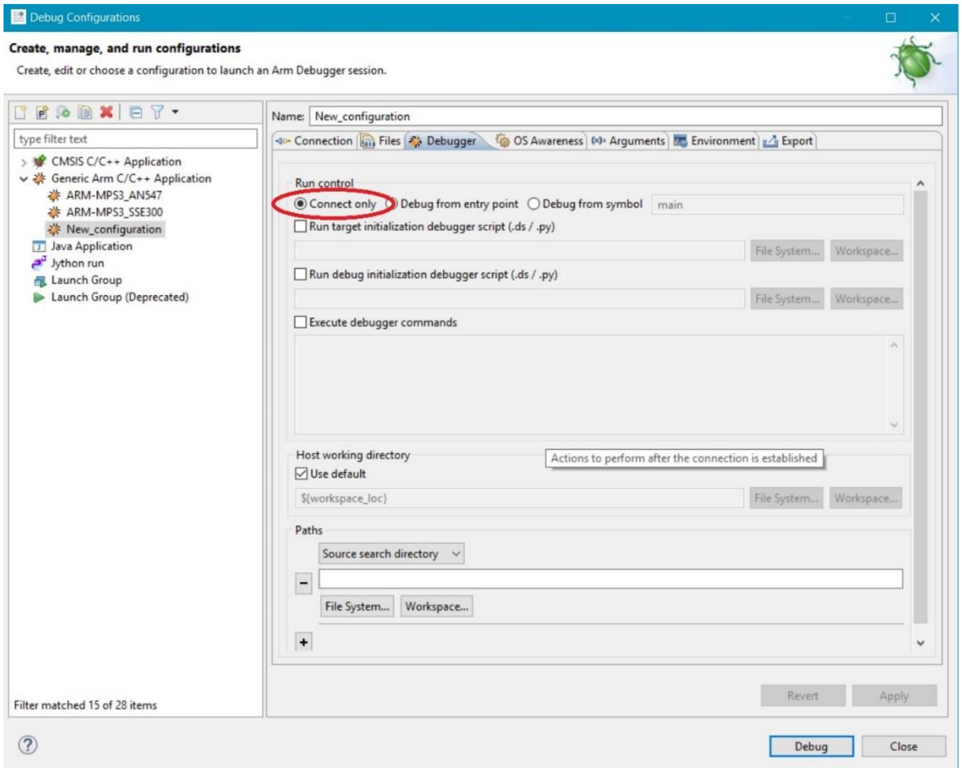
Connections

Bare Metal Debug | Connection

DTSL Options | Edit... | Configure DSTREAM trace or other target options. Using "default" config

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.
Non-Confidential

e. In the **Debugger** tab, select **Connect only**



Debug Configurations

Create, manage, and run configurations

Create, edit or choose a configuration to launch an Arm Debugger session.

type filter text

- CMSIS C/C++ Application
- Generic Arm C/C++ Application
  - ARM-MPS3_AN547
  - ARM-MPS3_SSE300
  - New_configuration
- Java Application
- Jython run
- Launch Group
- Launch Group (Deprecated)

Filter matched 15 of 28 items

Name: New_configuration

Connection | Files | Debugger | OS Awareness | Arguments | Environment | Export

Run control

● Connect only ○ Debug from entry point ○ Debug from symbol main

□ Run target initialization debugger script (.ds / .py)

File System... Workspace...

□ Run debug initialization debugger script (.ds / .py)

File System... Workspace...

□ Execute debugger commands

Host working directory

Actions to perform after the connection is established

☑ Use default

${workspace_loc}

File System... Workspace...

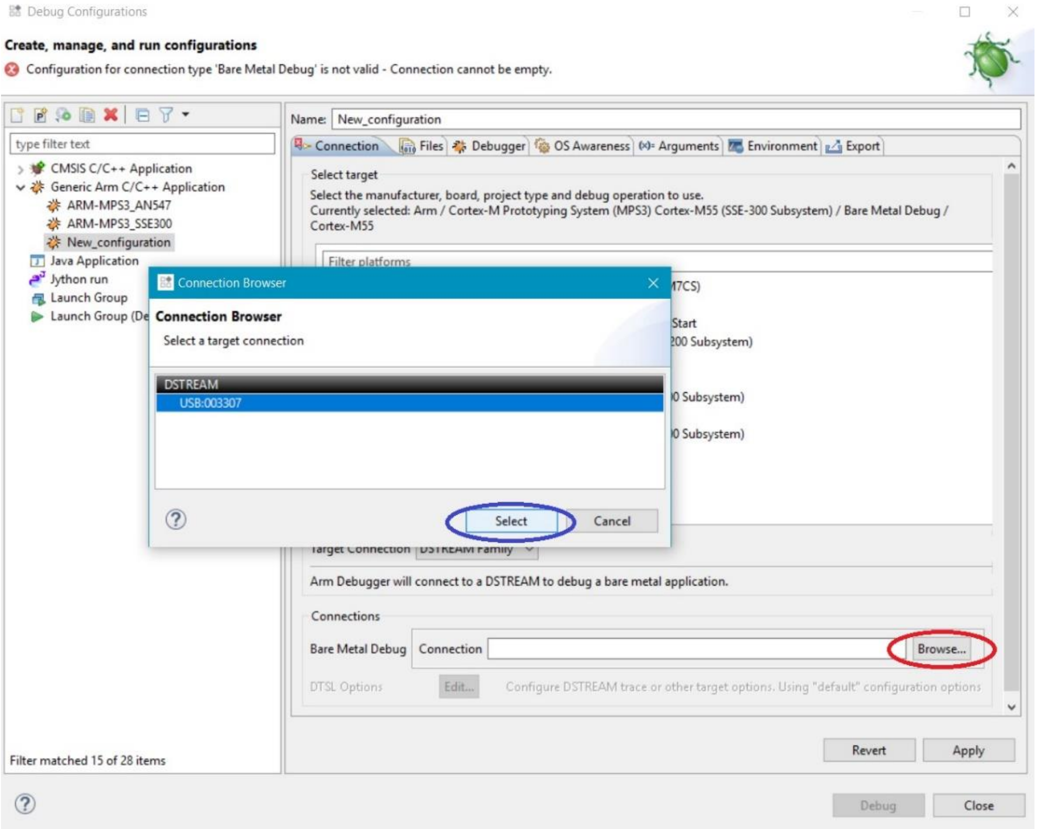
Paths

Source search directory

File System... Workspace...

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.

2. Establish a connection to the DSTREAM:
   a. Click the **Connection** tab.
   b. Select **Browse**, highlighted in red.
   c. A new window opens giving a list of all possible DSTREAMs.
   d. Select your DSTREAM from the options and then click **Select**, highlighted in blue.


Debug Configurations

Create, manage, and run configurations

Configuration for connection type 'Bare Metal Debug' is not valid - Connection cannot be empty.

Name: New_configuration

Select target

Select the manufacturer, board, project type and debug operation to use.
Currently selected: Arm / Cortex-M Prototyping System (MPS3) Cortex-M55 (SSE-300 Subsystem) / Bare Metal Debug / Cortex-M55

Connection Browser

Select a target connection

DSTREAM
USB:003307

Target Connection: DSTREAM Family

Arm Debugger will connect to a DSTREAM to debug a bare metal application.

Connections

Bare Metal Debug Connection

DTSL Options Edit... Configure DSTREAM trace or other target options. Using "default" configuration options

Filter matched 15 of 28 items

3. Click **Debug** to start your debug session.

Program execution at this stage can be either single-stepped or set to Run ▶.

Copyright © 2021-2022 Arm Limited (or its affiliates). All rights reserved.