DesignStart FPGA on Cloud: Cortex-M33 based platform

Technical Reference Manual

Non-Confidential

DesignStart FPGA on Cloud: Cortex-M33 based platform

Release Information

The following changes have been made to this document.

Change History

Date	Issue	Confidentiality	Change
23 October 2018	0000-00	Non-Confidential	First Release.

Arm Limited. Company 02557590 registered in England.
110 Fulbourn Road, Cambridge, England CB1 9NJ.
LES-PRE-20349

Contents

DesignStart FPGA on Cloud: Cortex-M33 based platform

1 Conventions and feedback

The following describes the typographical conventions and how to give feedback:

Typographical conventions

The following typographical conventions are used:

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

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

`monospace italic`
denotes arguments to commands and functions where the argument is to be replaced by a specific value.

`monospace bold`
denotes language keywords when used outside example code.

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

bold highlights interface elements, such as menu names. Denotes signal names. Also used for emphasis in descriptive lists, where appropriate.

Feedback on this product

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

- Your name and company.
- The serial number of the product.
- Details of the release you are using.
- Details of the platform you are using, such as the hardware platform, operating system type and version.
- A small standalone sample of code that reproduces the problem.
- A clear explanation of what you expected to happen, and what actually happened.
- The commands you used, including any command-line options.
- Sample output illustrating the problem.
- The version string of the tools, including the version number and build numbers.

Feedback on documentation

If you have comments on the documentation, e-mail `errata@arm.com`. Give:

- The title.
- The number, 101505_0000_00_en.
- If viewing online, the topic names to which your comments apply.
- If viewing a PDF version of a document, the page numbers to which your comments apply.
- A concise explanation of your comments.

Arm also welcomes general suggestions for additions and improvements.

Arm periodically provides updates and corrections to its documentation on the Arm Information Center, together with knowledge articles and Frequently Asked Questions (FAQs).

Other information

- Arm Information Center, http://infocenter.arm.com/help/index.jsp
- Arm Technical Support Knowledge Articles, http://infocenter.arm.com/help/topic/com.arm.doc.faqs/index.html
- Arm Support and Maintenance, http://www.arm.com/support/services/support-maintenance.php
- Arm Glossary, http://infocenter.arm.com/help/topic/com.arm.doc.aeg0014g/index.html

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.

2 Preface

2.1 Purpose of this application note

This application note discusses the operation of DesignStart FPGA on Cloud: Cortex-M33 based platform. DesignStart FPGA on Cloud: Cortex-M33 based platform is an FPGA implementation of an IoT Subsystem that uses SIE200 components together with CMSDK peripherals to provide an example design for the AWS F1 FPGA instances.

2.2 References

- *Arm DDI 0218 – PrimeCell® SingleMaster DMA Controller (PL081) Technical Reference Manual.*
- *Arm-ECM-0601256 – Armv8-M IoT Kit User Guide.*

2.3 Terms and abbreviations

CMSDK	*Cortex-M* System Design Kit.
DMA	Direct Memory Access.
MCC	Motherboard Configuration Controller.
RAM	Random Access Memory.
FPGA	Field Programmable Gate Array.
SCC	Serial Configuration Controller.
TRM	Technical Reference Manual.
APB	Advanced Peripheral Bus.
AHB	Advanced High-performance Bus.
RTL	Register Transfer Level.
SMM	Soft Macrocell Model.
MSC	Master Security Controller
PPC	Peripheral Protection Controller
EAM	Exclusive Access Controller
MPC	Memory Protection Controller
IDAU	Implementation Defined Attribution Unit
PCIe	PCI-Express
BAR	Base Address Register

2.4 Subsystem version details

This SMM is generated using various packages, which are detailed in the following figure.

Version	Descriptions
CG062 r1p0-00eac2	**Arm® Corelink™ SSE-200 Subsystem for Embedded** Full version of the design kit supporting Cortex-M33 Also contains the AHB Bus Matrix and advanced AHB components.
AT623/624 r0p2-rel0	**Arm® Cortex®-M33 and Arm® Cortex®-M33 FPU**
BP210 r1p0-01rel0	**Arm® Cortex®-M System Design Kit**
BP300 r3p1-00rel0	**Arm® CoreLink™ SIE-200 System IP for Embedded**
PL408 r0p0-00rel0	**Arm® CoreLink™ LPD-500 Low Power Interface Distributor**
TM100 r3p2-50rel0	**Arm® CoreSight™ SoC-400**
TM976 r0p2-00rel0	**Arm® CoreSight™ ETM-M33**
PL081 r1p2	**Arm® PrimeCell® Single Master DMA Controller**

Figure 2-1 Module versions

3 Overview

3.1 System block diagram

Figure 3-1 shows the high-level diagram of the full AWS F1 FPGA System.

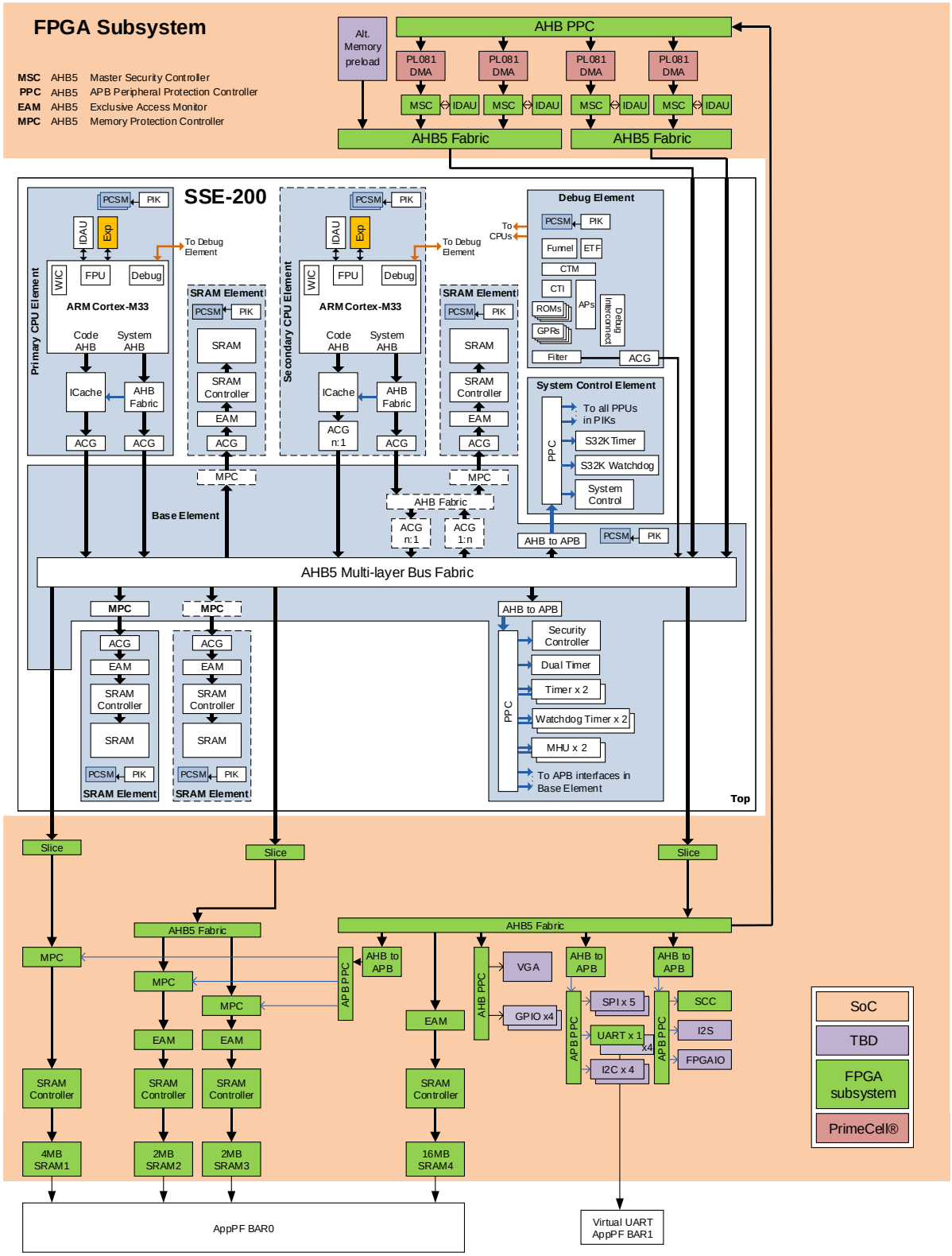

Figure 3-1 System overview

Note how the FPGA Subsystem extends the *Armv8-M IoT Kit* by adding to its expansion interfaces.

A slice has been added before the IoT kit SRAM to maintain FPGA timing.

3.2 SIE200 components

The following SIE200 components are used in this system:

- TrustZone AHB5 peripheral protection controller.
- TrustZone AHB5 master security controller.
- AHB5 bus matrix.
- AHB5 to AHB5 synchronous bridge.
- AHB5 to APB synchronous bridge.
- TrustZone APB4 peripheral protection controller.
- TrustZone AHB5 memory protection controller.
- AHB5 exclusive access monitor.
- AHB5 default slave.

3.3 Memory protection note

The SIE200 MPC and PPC components can affect memory and IO security management and must be configured as required for your application. Please see *Armv8-M IoT Kit User Guide* (Arm-ECM-0601256).

3.4 Memory map overview

This memory map includes information regarding IDAU security information for memory regions. For more information on these, please refer to the SIE200 components documentation.

ROW ID	Address From	Address To	Size	Region Name	Description	Alias With Row ID	IDAU Region Values Security	IDAUID	NSC
1	0x0000_0000	0x0DFF_FFFF	224MB	Code Memory	Maps to AHB5 Master Expansion Code Interface	3	NS	0	0
2	0x0E00_0000	0x0FFF_FFFF	32MB	Reserved	Reserved				
3	0x1000_0000	0x1DFF_FFFF	224MB	Code Memory	Maps to AHB5 Master Expansion Code Interface	1	S	1	CODE NSC2
4	0x1E00_0000	0x1FFF_FFFF	32MB	Reserved	Reserved				
5	0x2000_0000	0x20FF_FFFF	16MB	Internal SRAM	Internal SRAM Area.	8			
6	0x2100_0000	0x27FF_FFFF	112MB	Reserved	Reserved		NS	2	0
7	0x2800_0000	0x2FFF_FFFF	128MB	Expansion 0	Maps to AHB5 Master Expansion 0 Interface	10			
8	0x3000_0000	0x30FF_FFFF	16MB	Internal SRAM	Internal SRAM Area.	5			
9	0x3100_0000	0x37FF_FFFF	112MB	Reserved	Reserved		S	3	RAMNSC
10	0x3800_0000	0x3FFF_FFFF	128MB	Expansion 0	Maps to AHB5 Master Expansion 0 Interface	8			
11	0x4000_0000	0x4000_FFFF	64KB	Base Peripheral	Base Element Peripheral Region.	18			
12	0x4001_0000	0x4001_FFFF	64KB	Private CPU	CPU Element Peripheral Region.	19			
13	0x4002_0000	0x4002_FFFF	64KB	System Control	System Control Element Peripheral region.	20			
14	0x4003_0000	0x4003_FFFF		Reserved	Reserved		NS	4	0
15	0x4004_0000	0x4007_FFFF		Reserved	Reserved				
16	0x4008_0000	0x400F_FFFF	512KB	Base Peripheral	Base Element Peripheral Region.	23			
17	0x4010_0000	0x4FFF_FFFF	255MB	Expansion 1	Maps to AHB5 Master Expansion 1 Interface	24			
18	0x5000_0000	0x5000_FFFF	64KB	Base Peripheral	Base Element Peripheral Region.	11			
19	0x5001_0000	0x5001_FFFF	64KB	Private CPU	CPU Element Peripheral Region.	12			
20	0x5002_0000	0x5002_FFFF	64KB	System Control	System Control Element Peripheral region.	13	S	5	0
21	0x5003_0000	0x5003_FFFF		Reserved	Reserved				
22	0x5004_0000	0x5007_FFFF		Reserved	Reserved				
23	0x5008_0000	0x500F_FFFF	512KB	Base Peripheral	Base Element Peripheral Region.	16			

ROW ID	Address From	To	Size	Region Name	Description	Alias With Row ID	IDAU Region Values Security	IDAUID	NSC
24	0x5010_0000	0x5FFF_FFFF	255MB	Expansion 1	Maps to AHB5 Master Expansion 1 Interface	17			
25	0x6000_0000	0x6FFF_FFFF	256MB	Expansion 0	Maps to AHB5 Master Expansion 0 Interface	26	NS	6	0
26	0x7000_0000	0x7FFF_FFFF	256MB	Expansion 0	Maps to AHB5 Master Expansion 0 Interface	25	S	7	0
27	0x8000_0000	0x8FFF_FFFF	256MB	Expansion 1	Maps to AHB5 Master Expansion 1 Interface	28	NS	8	0
28	0x9000_0000	0x9FFF_FFFF	256MB	Expansion 1	Maps to AHB5 Master Expansion 1 Interface	27	S	9	0
29	0xA000_0000	0xAFFF_FFFF	256MB	Expansion 1	Maps to AHB5 Master Expansion 1 Interface	30	NS	A	0
30	0xB000_0000	0xBFFF_FFFF	256MB	Expansion 1	Maps to AHB5 Master Expansion 1 Interface	29	S	B	0
31	0xC000_0000	0xCFFF_FFFF	256MB	Expansion 1	Maps to AHB5 Master Expansion 1 Interface	32	NS	C	0
32	0xD000_0000	0xDFFF_FFFF	256MB	Expansion 1	Maps to AHB5 Master Expansion 1 Interface	31	S	D	0
34	0xE010_0000	0xEFFF_FFFF	255MB	Expansion 1	Maps to AHB5 Master Expansion 1 Interface	36	NS	E	0
35	0xF000_0000	0xF00F_FFFF	1MB	System Debug	System Debug.	33	Exempt		
36	0xF010_0000	0xFFFF_FFFF	255MB	Expansion 1	Maps to AHB5 Master Expansion 1 Interface	34	S	F	0

Table 1: Memory map overview

3.4.1 Synchronous SRAM for code (SRAM1)

4MB of SRAM memory is available in the code region of the memory map. The memory is named SRAM1 and is mapped both to the non-secure and Secure code memory region as shown in Table 2. To provide security gating, an MPC is place before this memory. It is called SSRAM1MPC, its configuration interface is located at 0x5800_7000 and its interrupt signal is connected to S_MPCEXP_STATUS[0]. All unused regions in the code memory space return bus error responses when accessed.

ROW ID	Address From	To	Size	Region Name	Description	Alias With Row ID	IDAU Region Values Security	IDAUID	NSC
1	**0x0000_0000**	**0x003F_FFFF**	**4MB**	Code Memory	**SRAM (SRAM1)**	5	NS	0	0
2	**0x0040_0000**	**0x007F_FFFF**	**4MB**		**SRAM1 alias**	6			
3	0x0080_0000	0x0DFF_FFFF	116MB		Not used. Returns Bus Errors when accessed.	-			
4	0x0E00_0000	0x0FFF_FFFF	32MB	Reserved	Reserved	-			
5	**0x1000_0000**	**0x103F_FFFF**	**4MB**	Code Memory	**SRAM (SRAM1)**	1	S	1	CODE NSC
6	**0x1040_0000**	**0x107F_FFFF**	**4MB**		**SRAM1 alias**	2			
7	0x1080_0000	0x1DFF_FFFF	116MB		Not used. Returns Bus Errors when accessed.	-			
8	0x1E00_0000	0x1FFF_FFFF	32MB	Reserved	Reserved	-			

Table 2: SRAM1 mapping to code memory

Because 4MB of memory exists in an 8MB window, the top 4MB of that window is aliased with the lower 4MB. As a result, both will share the same security setting. This ensures that there are no security holes that allow Secure and Non-secure access to the same physical location on the SRAM at the same time.

The SSRAM1MPC is configured as follows:

DATA_WIDTH	32bits	Data Width: 32bits
ADDR_WIDTH	22	Address Width. Set at 22bits to support 4 Mbyte of memory space.
MASTER_WIDTH	5	HMASTER signal width. 5 bit for 32 masters
USER_WIDTH	0	User signal width parameter, default: 1, ports tied if 0
BLK_SIZE	8	Block size: (1 << BLK_SIZE) bytes, min. value: 5, max. value: 20. Set at 8 for 256 byte blocks.
GATE_RESP	0	Response on data AHB when accessed during programming lock: 0 – Add wait states until lock is released (default) 1 – Drive bus error

Table 3: SSRAM1MPC configuration settings

3.4.2 Synchronous SRAM (SRAM2 and SRAM3)

4MB of SRAM memory is available in the expansion 0 region of the memory map. The memory is formed by the combination of memories SRAM2 and SRAM3. All unused regions shown in the table return bus error responses when accessed.

ROW ID	Address From	To	Size	Region Name	Description	Alias With Row ID	IDAU Region Values Security	IDAUID	NSC
1	0x2000_0000	0x2007_FFFF	32KB	SRAM	FPGA Block Ram	6	NS	2	0
2	0x2080_0000	0x27FF_FFFF	~128MB	Reserved	Reserved				
3	**0x2800_0000**	**0x281F_FFFF**	**2MB**	Expansion 0	**SRAM (SRAM2)**	8			
4	**0x2820_0000**	**0x283F_FFFF**	**2MB**		**SRAM (SRAM3)**	9			
5	0x2840_0000	0x2FFF_FFFF	124MB		Not used. Returns Bus Errors when accessed.				
6	0x3000_0000	0x3007_FFFF	32KB	SRAM	FPGA Block Ram	1	S	3	RAM NSC
7	0x3080_0000	0x37FF_FFFF	~128MB	Reserved	Reserved				
8	**0x3800_0000**	**0x381F_FFFF**	**2MB**	Expansion 0	**SRAM (SRAM2)**	3			
9	**0x3820_0000**	**0x383F_FFFF**	**2MB**		**SRAM (SRAM3)**	4			
10	0x3840_0000	0x3FFF_FFFF	124MB		Maps to AHB5 Master Expansion 0 Interface				

Table 4: SRAM2 and SRAM3 address mapping

An Exclusive Access Monitor and a Memory Protection Controller exist on the path of each SRAM. They support exclusive access and security gating, so that blocks of aliased memory can be assigned individually to Secure or Non-secure regions. The two MPCs are as follows:

- SSRAM2MPC is the MPC for SSRAM2. Its APB interface is mapped to address 0x5800_8000 and its interrupt signal is connected to S_MPCEXP_STATUS[1].
- SSRAM3MPC is the MPC for SSRAM3. Its APB interface is mapped to address 0x5800_9000 and its interrupt signal is connected to S_MPCEXP_STATUS[2].

Both SSRAM1MPC and SSRAM2MPC have the same configuration settings as listed in Table 5.

Parameter	Configuration	Description
DATA_WIDTH	32bits	Data Width: 32bits
ADDR_WIDTH	22	Address Width. Set at 22bits to support 4 Mbyte of memory space.
MASTER_WIDTH	5	HMASTER signal width. 5 bit for 32 masters
USER_WIDTH	0	User signal width parameter, default: 1, ports tied if 0
BLK_SIZE	8	Block size: (1 << BLK_SIZE) bytes, min. value: 5, max. value: 20. Set at 8 for 256 byte blocks.
GATE_RESP	0	Response on data AHB when accessed during programming lock: 0 – Add wait states until lock is released (default) 1 – Drive bus error

Table 5: SSRAM2MPC and SSRAM3MPC configuration settings

3.4.3 Synchronous SRAM (SRAM4)

The memory map includes 16MB of SRAM memory in the expansion 1 region. All unused regions shown in the table return bus error responses when accessed. These memories are currently mapped only to Non-secure SRAM space as follows:

ROW ID	Address From	To	Size	Region Name	Description	Alias With Row ID	IDAU Region Values Security	IDAUID	NSC
1	**0x8000_0000**	**0x80FF_FFFF**	**16MB**	AHB Master Expansion 1 Interface Area	**SRAM4**				
2	0x8100_0001	0x8FFF_FFFF	246MB		Not used. Returns Bus Errors when accessed.		NS	8	0

Table 6: SRAM4

3.4.4 Expansion system peripherals

Other than the SRAMs, all FPGA peripherals that are extensions to the IoT lot are mapped into two key areas of the memory map:

- 0x4010_0000 to 0x4FFF_FFFF Non-secure region, which maps to AHB Master Expansion 1 interface.
- 0x5010_0000 to 0x5FFF_FFFF Secure region, which maps to AHB Master Expansion 1 interface.

Table 7 shows how these peripherals are mapped.

To support TrustZone-Armv8M, and allow software to map these peripherals to Secure or Non-secure address space, many peripherals are mapped twice, and either APB PPC or AHB PPC is then used to gate access to these peripherals. An FPGA Secure Privilege Control block and a Non-secure Privilege Control block then provide controls to these PPC.

For expansion AHB Masters within the system, a Master Security Controller (MSC) is added to each master with an associated IDAU. Masters that have IDAU are:

- PL081 DMA Engine. All DMAs can be mapped as Secure or Non-secure Masters. The intention is to support the use case in which, for each pair of DMAs that shared a single AHB expansion interface, one is mapped as Secure and another is mapped as non-Secure.

ROW ID	Address		Size	Description	Alias With Row ID	IDAU Region Values	
	From	To				Security	ID
1	0x4010_0000	0x4010_0FFF	4K	GPIO 0	24		
2	0x4010_1000	0x4010_1FFF	4K	GPIO 1	25		
3	0x4010_2000	0x4010_2FFF	4K	GPIO 2	26		
4	0x4010_3000	0x4010_3FFF	4K	GPIO 3	27		
5	0x4010_4000	0x4010_FFFF		Not used. Returns Bus Errors when accessed.			
6	0x4011_0000	0x4011_0FFF	4K	DMA 0	29		
7	0x4011_1000	0x4011_1FFF	4K	DMA 1	30		
8	0x4011_2000	0x4011_2FFF	4K	DMA 2	31		
9	0x4011_3000	0x4011_3FFF	4K	DMA 3	32		
10	0x4011_4000	0x401F_FFFF		Not used. Returns Bus Errors when accessed.			
11	0x4020_0000	0x4020_0FFF	4K	UART 0 – Virtual UART	34		
12	0x4020_1000	0x4020_DFFF	52K	Reserved	35	NS	4
13	0x4020_E000	0x402F_FFFF		Not used. Returns Bus Errors when accessed.			
14	0x4030_0000	0x4030_0FFF	4K	FPGA - SCC registers	37		
15	0x4030_1000	0x4030_1FFF	4K	Reserved	38		
16	0x4030_2000	0x4030_2FFF	4K	FPGA - IO (System Ctrl + I/O)	39		
17	0x4030_3000	0x40FF_FFFF		Not used. Returns Bus Errors when accessed.			
18	0x4100_0000	0x4113_FFFF	320K	Reserved	40		
19	0x4114_0000	0x41FF_FFFF		Not used. Returns Bus Errors when accessed.			
20	0x4200_0000	0x420F_FFFF	1M	Reserved	42		
21	0x4210_0000	0x4800_6FFF		Not used. Returns Bus Errors when accessed.			
22	0x4800_7000	0x4800_7FFF	4K	FPGA Non-Secure Privilege Control			
23	0x4800_8000	0x4FFF_FFFF		Not used. Returns Bus Errors when accessed.			
24	0x5010_0000	0x5010_0FFF	4K	GPIO 0	1		
25	0x5010_1000	0x5010_1FFF	4K	GPIO 1	2		
26	0x5010_2000	0x5010_2FFF	4K	GPIO 2	3		
27	0x5010_3000	0x5010_3FFF	4K	GPIO 3	4		
28	0x5010_4000	0x5010_FFFF		Not used. Returns Bus Errors when accessed.			
29	0x5011_0000	0x5011_0FFF	4K	DMA 0	6		
30	0x5011_1000	0x5011_1FFF	4K	DMA 1	7		
31	0x5011_2000	0x5011_2FFF	4K	DMA 2	8		
32	0x5011_3000	0x5011_3FFF	4K	DMA 3	9	S	5
33	0x5011_4000	0x501F_FFFF		Not used. Returns Bus Errors when accessed.			
34	0x5020_0000	0x5020_0FFF	4K	UART 0 – Virtual UART	11		
35	0x5020_1000	0x5020_DFFF	52K	Reserved	12		
36	0x5020_E000	0x502F_FFFF		Not used. Returns Bus Errors when accessed.			
37	0x5030_0000	0x5030_0FFF	4K	FPGA - SCC registers	14		
38	0x5030_1000	0x5030_1FFF	4K	Reserved	15		
39	0x5030_1000	0x5030_2FFF	4K	FPGA - IO (System Ctrl + I/O)	16		

ROW ID	Address		Size	Description	Alias With Row ID	IDAU Region Values	
	From	To				Security	ID
38	0x5030_3000	0x50FF_FFFF		Not used. Returns Bus Errors when accessed.			
39	0x5100_0000	0x5113_FFFF	320K	Reserved	18		
40	0x5114_0000	0x51FF_FFFF		Not used. Returns Bus Errors when accessed.			
41	0x5200_0000	0x520F_FFFF	1M	Reserved	20		
42	0x5210_0000	0x5800_6FFF		Not used. Returns Bus Errors when accessed.			
43	0x5800_7000	0x5800_7FFF	4K	SSRAM1 Memory Protection Controller (MPC)			
44	0x5800_8000	0x5800_8FFF	4K	SSRAM2 Memory Protection Controller (MPC)			
45	0x5800_9000	0x5800_9FFF	4K	SSRAM3 Memory Protection Controller (MPC)			
46	0x5800_A000	0x5FFF_FFFF		Not used. Returns Bus Errors when accessed.			

Table 7: FPGA expansion peripheral map

4 Programmers Model

4.1 CMSDK and SIE200 components

This programmer's model is supplemental to the CMSDK IoT kit and Armv8-M IoT kit documentation, which covers many of the included components in more detail. Figure 3-1 System overview shows the connectivity of the system.

4.2 SRAMs

4.2.1 SRAM1

SRAM1 is in the CODE region. It forms a 64-bit SRAM. Although 8MB of memory space is allocated, only 4MB is used.

4.2.2 SRAM2 & SRAM3

Although 8MB of memory space is allocated, only 4MB is used.

This memory is also accessible at 0x38000000.

Note: SRAM2 and SRAM3 are in the SRAM region. Running code from SRAM region is slower than from CODE region, because the internal bus structure is not optimized for running programs from this region.

4.2.3 SRAM4

A 16MB SRAM4 area is available, and the memory map allocates the address-range 0x80000000 - 0x80FFFFFF. This enables large test programs, for example uClinux, to be used in the External RAM region of the Cortex-M memory space.

Note: SRAM4 is in the SRAM region. Running code from SRAM region is slower than from CODE region because the internal bus structure is not optimized for running programs from this region.

4.3 UART

The SMM implements one CMSDK UARTs:

- UART 0 – Virtual UART

4.4 FPGA system control and I/O

The SMM implements an FPGA system control block.

Address	Name	Information
0x40028000 0x50028000	FPGAIO->LED0	LED connections [31:2] : Reserved [1:0] : vLED[1:0]
0x40028004 0x50028004	RESERVED	
0x40028008 0x50028008	FPGAIO->BUTTON	Buttons [31:2] : Reserved [1:0] : Buttons (vDIP[1:0])
0x4002800C 0x5002800C	RESERVED	
0x40028010 0x50028010	FPGAIO->CLK1HZ	1Hz up counter
0x40028014 0x50028014	FPGAIO->CLK100HZ	100Hz up counter
0x40028018 0x50028018	FPGAIO->COUNTER	Cycle Up Counter Increments when 32-bit prescale counter reach zero.
0x4002801C 0x5002801C	FPGAIO->PRESCALE	Bit[31:0] – reload valu*e for* prescale counter.
0x40028020 0x50028020	FPGAIO->PSCNTR	32-bit Prescale counter – current value of the pre-scaler counter. The Cycle Up Counter increment when the prescale down counter reach 0. The pre-scaler counter is reloaded with PRESCALE after reaching 0.
0x40028024 0x40028024	RESERVED	
0x4002804C 0x5002804C	FPGAIO->MISC	Misc control [31:0] : Reserved

Table 8: System control and I/O memory map

4.5 Serial Communication Controller

The SMM implements communication between the host and the FPGA system through a *Serial Communication Controller* (SCC) interface. The interface is mapped to BAR0 (TODO ref).

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

Address	Name	Information
0x000	CFG_REG0	Bits[31:0] Reserved
0x004	CFG_REG1	Bits [31:0] Reserved
0x008	CFG_REG2	Reserved
0x00C	CFG_REG3	Bits [31:0] Reserved
0x010	CFG_REG4	Bits [31:0] Reserved
0x014	RESERVED	-
0x018	RESERVED	-
0x01C	RESERVED	-
0x020 – 0x09C	RESERVED	-
0x0A0	SYS_CFGDATA_RTN	32bit DATA [r/w]
0x0A4	SYS_CFGDATA_OUT	32bit DATA [r/w]
0x0A8	SYS_CFGCTRL	Bit[31] : Start (generates interrupt on write to this bit) Bit[30] : R/W access Bits[29:26] : Reserved Bits[25:20] : Function value Bits[19:12] : Reserved Bits[11:0] : Device (value of 0/1/2 for supported clocks)
0x0AC	SYS_CFGSTAT	Bit 0 : Complete Bit 1 : Error
0x0AD – 0x0FC	RESERVED	-
0x100	RESERVED	-
0x104 – 0xFF4	RESERVED	-
0xFF8	SCC_AID	SCC AID register is read only Bits[31:8] :Reserved Bits[7:0] number of SCC configuration register
0xFFC	SCC_ID	SCC ID register is read only Bits[31:24] : Implementer ID: 0x41 = Arm Bits[23:20] : Reserved Bits[19:16] : IP Architecture: 0x4 =AHB Bits[15:4] : Primary part number: 505 = <TODO AN???> Bits[3:0] : Reserved

Table 9: SCC register memory map

5 Clock and reset architecture

The following tables list clocks entering and generated by the SMM.

5.1 Clocks

5.1.1 Source clocks

The following clocks are inputs to the system.

Clock	Input Pin	Frequency	Note
OSC0	OSCCLK[0]	250MHz	

Table 10: Source clocks

5.1.2 Internal clocks

The following clocks are generated internally from the source clocks.

Clock	Source	Frequency	Note
MAINCLK	OSC0	50MHz	
S32KCLK	OSC0	32kHz	
clk_100hz	OSC0	100Hz	

Table 11: Generated internal clocks

5.1.3 Clocks connecting to the IoT kit

The following clocks connect to the IoT kit. Both clocks are provided to the IoT kit and clocks generated by the kit

Clock	Source / Direction	Frequency	Note
MAINCLK	OSC0	50MHz	Main Clock Input
SYSCLK	Output	50MHz	Main System Clock
S32KCLK	S32KCLK	32kHz	Asynchronous 32KHz clock input
TRACECLK	Output	50MHz	TPIU trace port clock
SWCLKTCK	OSC0	50MHz	SW/JTAG DP clock
TRACECLKIN	OSC0	50MHz	TPIU trace port clock input

Table 12: IoT kit clocks

5.2 Resets

5.2.1 Source resets

The following resets are inputs to the system.

Reset	Input Pin	Note
CB_NPOR	vDIP[0]	Controls the SW preload interfaces and memories
CB_NRST	vDIP[1]	Controls the rest of the system
rst_main_n	rst_main_n	Master reset from AWS framework

Table 13: Source resets

6 FPGA secure privilege control

The IoT kit subsystem's Secure Privilege Control Block and Non-secure Privilege Block are able to provides expansion security control signals to control the various security gating units within the subsystem. The following table lists the connectivity of the system security extension signal. More details are available in *Armv8-M IoT Kit User Guide* (Arm-ECM-0601256).

Component name	Components signals	Security expansion signals
DMA 0 MSC	msc_irq	S_MSCEXP_STATUS[0]
	msc_irq_clear	S_MSCEXP_CLEAR[0]
	cfg_nonsec	NS_MSCEXP[0]
DMA 1 MSC	msc_irq	S_MSCEXP_STATUS[1]
	msc_irq_clear	S_MSCEXP_CLEAR[1]
	cfg_nonsec	NS_MSCEXP[1]
DMA 2 MSC	msc_irq	S_MSCEXP_STATUS[2]
	msc_irq_clear	S_MSCEXP_CLEAR[2]
	cfg_nonsec	NS_MSCEXP[2]
DMA 3 MSC	msc_irq	S_MSCEXP_STATUS[3]
	msc_irq_clear	S_MSCEXP_CLEAR[3]
	cfg_nonsec	NS_MSCEXP[3]
APB PPC EXP 0	apb_ppc_irq	S_APBPPCEXP_STATUS[0]
	apb_ppc_clear	S_APBPPCEXP_CLEAR[0]
	cfg_sec_resp	SEC_RESP_CFG
	cfg_non_sec	APB_NS_PPCEXP0[15:0]
	cfg_ap	APB_P_PPCEXP0[15:0]
APB PPC EXP 1	apb_ppc_irq	S_APBPPCEXP_STATUS[1]
	apb_ppc_clear	S_APBPPCEXP_CLEAR[1]
	cfg_sec_resp	SEC_RESP_CFG
	cfg_non_sec	APB_NS_PPCEXP1[15:0]
	cfg_ap	APB_P_PPCEXP1[15:0]
APB PPC EXP 2	apb_ppc_irq	S_APBPPCEXP_STATUS[2]
	apb_ppc_clear	S_APBPPCEXP_CLEAR[2]
	cfg_sec_resp	SEC_RESP_CFG
	cfg_non_sec	APB_NS_PPCEXP2[15:0]
	cfg_ap	APB_P_PPCEXP2[15:0]
AHB PPC EXP 0	ahb_ppc_irq	S_AHBPPCEXP_STATUS[0]
	ahb_ppc_clear	S_AHBPPCEXP_CLEAR[0]
	cfg_sec_resp	SEC_RESP_CFG
	cfg_non_sec	AHB_NS_PPCEXP0[15:0]
	chg_ap	AHB_P_PPCEXP0[15:0]
AHB PPC EXP 1	ahb_ppc_irq	S_AHBPPCEXP_STATUS[1]

Component name	Components signals	Security expansion signals
	ahb_ppc_clear	S_AHBPPCEXP_CLEAR[1]
	cfg_sec_resp	SEC_RESP_CFG
	cfg_non_sec	AHB_NS_PPCEXP1[15:0]
	chg_ap	AHB_P_PPCEXP1[15:0]
MPC SSRAM0	secure_error_irq	S_MPCEXP_STATUS[0]
MPC SSRAM1	secure_error_irq	S_MPCEXP_STATUS[1]
MPC SSRAM2	secure_error_irq	S_MPCEXP_STATUS[2]

Table 14: Security expansion signals connectivity

The following table lists the peripherals that are controlled by APB PPC EXP 0. Each APB <n> interface is controlled by APB_NS_PPCEXP0[n] and APB_P_PPCEXP0[n].

APB PPC EXP 0 Interface Number <n>	Name
0	SSRAM1 Memory Protection Controller (MPC)
1	SSRAM2 Memory Protection Controller (MPC)
2	SSRAM3 Memory Protection Controller (MPC)
15:3	Reserved

Table 15: Peripherals mapping of APB PPC EXP 0

The following table lists the peripherals that are controlled by APB PPC EXP 1. Each APB <n> interface is controlled by APB_NS_PPCEXP1[n] and APB_P_PPCEXP1[n].

APB PPC EXP 1 Interface Number <n>	Name
0	Reserved
1	Reserved
2	Reserved
3	Reserved
4	Reserved
5	UART_0
6	Reserved
7	Reserved
8	Reserved
9	Reserved
10	Reserved
11	Reserved
12	Reserved
13	Reserved
15:14	Reserved

Table 16: Peripherals mapping of APB PPC EXP 1

The following table lists the peripherals that are controlled by APB PPC EXP 2. Each APB <n> interface is controlled by APB_NS_PPCEXP2[n] and APB_P_PPCEXP2[n].

APB PPC EXP 0 Interface Number <n>	Name
0	SCC
1	Reserved
2	FPGAIO
15:3	Reserved

Table 17: Peripherals mapping of APB PPC EXP 2

The following table lists the peripherals that are controlled by AHB PPC EXP 0 . each APB <n> interface is controlled by AHB_NS_PPCEXP0[n] and AHB_P_PPCEXP0[n].

AHB PPC EXP 0 Interface Number <n>	Name
0	Reserved
1	Reserved
2	Reserved
3	Reserved
4	Reserved
15:5	Reserved

Table 18: Peripherals mapping of AHB PPC EXP 0

The following table lists the peripherals that are controlled by AHB PPC EXP 1. Each APB <n> interface is controlled by AHB_NS_PPCEXP1[n] and AHB_P_PPCEXP0[n].

AHB PPC EXP 0 Interface Number <n>	Name
0	DMA_0
1	DMA_1
2	DMA_2
3	DMA_3
15:4	Reserved

Table 19: Peripherals mapping of AHB PPC EXP1

The following table lists the *Master Security Controllers* (MSCs) that are controlled by NS_MSCEXP signals. These control signals are used to map each peripheral connected to their associated MSCs as Secure or Non-secure Masters.

NS_MSCEXP bits	Name
0	MSC cfg_nonsec for DMA0
1	MSC cfg_nonsec for DMA1
2	MSC cfg_nonsec for DMA2
3	MSC cfg_nonsec for DMA3
15:4	Reserved

Table 20: Peripherals mapping of AHB PPC EXP1

7 Interrupt map

The interrupts in the FPGA subsystem extend the *Armv8-M IoT Kit* interrupt map by adding to the expansion area as follows:

Interrupt Input	Interrupt Source
NMI	Combined Secure Watchdog, S32K Watchdog and NMI_Expansion
IRQ[0]	Non-Secure Watchdog Reset Request
IRQ[1]	Non-Secure Watchdog Interrupt
IRQ[2]	S32K Timer
IRQ[3]	Timer 0
IRQ[4]	Timer 1
IRQ[5]	Dual Timer
IRQ[8:6]	Reserved
IRQ[9]	MPC Combined (Secure)
IRQ[10]	PPC Combined (Secure)
IRQ[11]	MSC Combined (Secure)
IRQ[12]	Bridge Error Combined Interrupt (Secure)
IRQ[31:13]	Reserved
IRQ[32]	UART 0 Receive Interrupt
IRQ[33]	UART 0 Transmit Interrupt
IRQ[34]	Reserved
IRQ[35]	Reserved
IRQ[36]	Reserved
IRQ[37]	Reserved
IRQ[38]	Reserved
IRQ[39]	Reserved
IRQ[40]	Reserved
IRQ[41]	Reserved
IRQ[42]	UART 0 Combined Interrupt
IRQ[43]	Reserved
IRQ[44]	Reserved
IRQ[45]	Reserved
IRQ[46]	Reserved
IRQ[47]	UART0 Overflow
IRQ[48]	Reserved
IRQ[49]	Reserved
IRQ[50]	Reserved
IRQ[51]	Reserved
IRQ[52]	Reserved
IRQ[53]	Reserved
IRQ[54]	Reserved

IRQ[55]	Reserved
IRQ[56]	DMA #0 Error Interrupt Request
IRQ[57]	DMA #0 Terminal Count Interrupt Request
IRQ[58]	DMA #0 Combined Interrupt Request
IRQ[59]	DMA #1 Error Interrupt Request
IRQ[60]	DMA #1 Terminal Count Interrupt Request
IRQ[61]	DMA #1 Combined Interrupt Request
IRQ[62]	DMA #2 Error Interrupt Request
IRQ[63]	DMA #2 Terminal Count Interrupt Request
IRQ[64]	DMA #2 Combined Interrupt Request
IRQ[65]	DMA #3 Error Interrupt Request
IRQ[66]	DMA #3 Terminal Count Interrupt Request
IRQ[67]	DMA #3 Combined Interrupt Request
IRQ[68]	Reserved
IRQ[69]	Reserved
IRQ[70]	Reserved
IRQ[71]	Reserved
IRQ[87:72]	Reserved
IRQ[103:88]	Reserved
IRQ[119:104]	Reserved
IRQ[123:120]	Reserved

Table 21: FPGA expansion interrupt map

7.1 UARTS interrupts

The system includes one CMSDK UART, which has the following interrupt pins:

- TXINT.
- RXINT.
- TXOVRINT.
- EXOVRINT.
- UARTINT.

The TXINT, RXINT and UARTINT interrupt signals drive a single interrupt input of the Cortex-M33 CPU. In addition, the two interrupt signals TXOVERINT and EXOVRINT are logically ORed together to drive IRQ[47].

8 Configurations

8.1 IoT subsystem

The IoT subsystem has a number of configurable options, which are listed in the following table.

Parameter	Implemented Values	Default Values	Description
INITSVTOR0_RST [31:0]	0x1000_0000	0x1000_0000	Reset Value of the Secure Vector table offset address register in the System Control Register.
INITNSVTOR0 [31:0]	0x0000_0000	0x0000_0000	Reset Value of the Non-Secure Vector table offset address at the Cortex-M33 CPU Core.
CPU0WAIT_RST	0	0	CPU0 wait at boot '0' boot normally, '1' wait at boot. CB_NRST is de-asserted by the host after the SW preload is finished.
CPU1WAIT_RST	1	1	CPU1 wait at boot '0' boot normally, '1' wait at boot.
EXP_NUMIRQ	92	64	Specifies the number of expansion interrupt. This therefore means that the Cortex-M33 NVIC has 92+32 = 124 interrupts.
EXP_IRQ_DIS_0 [EXP_NUMIRQ-1:0]	All set to low.	All set to high.	Disables support for individual expansion interrupts on Primary CPU Core, allowing a range of non-contiguous interrupts IRQDIS[i] = 1'b1 indicates that IRQ[i] is not present
EXP_SYS_ID_PRESENT [31:16]	0xFFFF	0xFFFF	Each bit *n* of this vector defines if an AHB Master with HMASTERID = *n* exist in the system. Bit 15 down to 0 are all IDs reserved for internal use and not available on this interface.
LP_HAS_CRYPTO	0	0	The design does not contain the Arm® TrustZone® Cryptocell-312.
CPU0_FPU	1	0	Floating Point Unit (FPU) is present on the Cortex-M33 CPU
CPU0_DSP	1	0	Digital Signal Processing (DSP) extension instructions are included on the Cortex-M33 CPU.
CPU0_MPU_NS	8	8	Number of Non-Secure MPU entries on the Cortex-M33 CPU
CPU0_MPU_S	8	8	Number of Secure MPU entries on the Cortex-M33 CPU
CPU0_SAU	8	8	Number of SAU entries on the Cortex-M33 CPU
CPU0_IRQ_LVL	4	4	Number of interrupt priority implemented in the NVIC, equal to $2^{CPU0\_IRQ\_LVL}$. Supports 3 to 8 bits. Currently at 4 which therefore provides 16 levels of interrupt priority.
CPU1_FPU	1	1	Floating Point Unit (FPU) is present on the Cortex-M33 CPU
CPU1_DSP	1	1	Digital Signal Processing (DSP) extension instructions are included on the Cortex-M33 CPU.
CPU1_MPU_NS	8	8	Number of Non-Secure MPU entries on the Cortex-M33 CPU
CPU1_MPU_S	8	8	Number of Secure MPU entries on the Cortex-M33 CPU
CPU0_SAU	8	8	Number of SAU entries on the Cortex-M33 CPU
CPU1_IRQ_LVL	4	4	Number of interrupt priority implemented in the NVIC, equal to $2^{CPU0\_IRQ\_LVL}$. Supports 3 to 8 bits. Currently at 4 which therefore provides 16 levels of interrupt priority.

Table 22: Top level user configurable parameters

8.2 Cortex-M33

To configure the Cortex-M33 CPU core, refer to document Arm-ECM-0601256 – Armv8-M IoT Kit User Guide, Section 3.5, CPU element for parameters used in IoT kit.

9 Host interfaces

9.1 PCIe mapping

9.1.1 AppPF BAR0

This *Base Address Register* (BAR) is used to setup the system before releasing CB_NRST. This BAR provides backdoor access to the SCC, and to the SRAM memories in the following table.

Address	Size	Function
0x0000_0000- 0x003F_FFFF	4MB	SRAM1
0x0040_0000- 0x005F_FFFF	2MB	SRAM2
0x0060_0000- 0x007F_FFFF	2MB	SRAM3
0xC000_0000- 0xC000_0FFF	4kB	SCC
0x1000_0000- 0x1FFF_FFFF	16MB	SRAM4

Table 23: PCIe AppPF BAR0 address map

9.1.2 AppPF BAR1

This BAR handles the Virtual UART. It is intended to be used with the provided driver.

Address	Size	Function
0x0000_0000	32b	Virtual UART TX [0] Data to the FPGA [31:1] Reserved
0x0000_0004	32b	Virtual UART RX [0] Data from the FPGA [31:1] Reserved
0x0000_0008	32b	Virtual UART Status [0] RX FIFO full [1] TX FIFO empty [31:2] Reserved

Table 24: PCIe BAR1 address map

9.1.3 AppPF BAR4

This BAR is currently unused.

9.1.4 MgmtPF BAR4

This BAR is currently unused.

9.2 vLED and vDIP mapping

Signal	Function	Note
vLED[0]	rst_main_n	From AWS
vLED[1]	Reserved	Tied to ‘1’.
vLED[2]	sh_flr_assert	From AWS
vLED[3]	CB_NPOR	
vLED[4]	CB_NRST	
vLED[5]	sh_cl_pwr_state[0]	
vLED[6]	sh_cl_pwr_state[1]	
vLED[7]	Reserved	Tied to ‘0’
vLED[8]	sh_cl_ddr_is_ready	
vLED[9]	Reserved	Tied to ‘0’
vLED[10]	cb_npor	After sync stage
vLED[11]	cb_nrst	After sync stage
vLED[12]	Reserved	Tied to ‘0’
vLED[13]	Reserved	Tied to ‘0’
vLED[14]	USER_LED[0]	
vLED[15]	USER_LED[1]	

Table 25: Virtual LED mapping

Signal	Function	Note
vDIP[0]	CB_NPOR	
vDIP[1]	CB_NRST	
vDIP[13:2]	Reserved	
vDIP[14]	USER_BUTTON[0]	
vDIP[15]	USER_BUTTON[1]	

Table 26: Virtual DIP mapping