Project Argus DC-SCM 2.0

Revision 1.0
May 15, 2023

Authors
Lenovo: Stewart Nguyen, Sean Chang, Matt Lin, Vicky Huang, Terry Hong, Melos Chen, Hann Wang, CSP Design team
Cloudflare: Jun Qi Lau, Xiaomin Shen, Ryan Chow, Giovanni Pereira Zantedeschi, Nnamdi Ajah, Hardware System Engineering team, Infrastructure Security team

Table of Contents

1. License 7
1.1. OPTION B: Open Web Foundation (OWF) CLA 7
1.2 Acknowledgements 8
2. Compliance with OCP Tenets 9
2.1. Openness 9
2.2. Efficiency 9
2.3. Impact 9
2.4. Scale 9
2.5. Sustainability 9
3. Version Table 10
4. Scope 11
5. Overview 12
6. Rack Compatibility 13
7. Physical Specifications 13
7.1 Block Diagram 13
7.2 PCB Overview 14
7.2.1 Board Stack-up 14
7.2.2 Board Placement Top Side 15
7.2.3 Board Placement Bottom Side 16
7.2.4 Board Mechanical 17
8. Thermal Design Requirements 18
8.1 Thermal Design Conditions 18
8.2 Sensor Locations on Board 18
9. I/O System 19
9.1 DC-SCI Card Edge Connector Requirement 19
9.2 Gold Finger Plating Requirement 19
9.3 HPM Connector Requirement 20
9.4 DC-SCI Pin Definition 20
9.5 Project Argus DC-SCI Signal Descriptions and Examples 27
9.5.1 LVDS Tunneling Protocol and Interface (LTPI) 27

9.5.2 SGPIO 28
9.5.3 I2C/I3C 29
9.5.4 eSPI 31
9.5.5 QSPI and SPI 31
9.5.6 USB 33
9.5.7 PCIE/Clock 34
9.5.8 PECI 35
9.5.9 JTAG 36
9.5.10 NC-SI 36
9.5.11 UART 37
9.5.12 HPM Power Button 38
9.6 Power States & Boot Sequence 38
9.6.1 Virtual Reseat 41
9.7 Platform Root of Trust (PRoT) 42
9.8 DC-SCM CPLD 43
9.8.1 Secure Boot and Dual Boot 43
9.8.2 LTPI 44
9.8.3 SGPIO 45
9.8.4 I2C 46
9.8.5 JTAG 46
9.8.6 UART 46
9.9 Externally Accessible Buttons and LEDs 47
9.10 TPM 47
9.11 Intrusion Detection 48
10. Rear Side Power, I/O, Expansion Board and Midplane Subsystems 48
11. Mechanical 49
11.1 General Overview 49
11.2 Board Dimensions and Keep-out Zones 49
11.3 I/O Faceplate Bracket Subassembly 52
11.4 Module Assembly Overview 53
11.5 Chassis Bay Opening Requirement 54
11.6 Front Panel Definition 55

11.6.1 Front I/O 55
11.6.2 Button 55
11.6.3 LEDs 56
11.7 Internal Lock Mechanism 57
12. Onboard Power System 58
12.1 Power Block Diagram 58
12.2 Power Consumption 59
13. Environmental Regulations/Environmental Requirements 59
14. Prescribed Materials 60
15. Software Support (recommended) 60
16. System Firmware 60
16.1 BMC Firmware 60
16.1.1 Minimum Bootable Device Tree 61
16.2 HWRoT Firmware 61
16.2.1 HWRoT Secure Boot Mode 62
16.2.2 HWRoT Secure Boot Process 62
16.2.3 BMC Secure Boot Process 62
16.2.4 UEFI Secure Boot Process 63
16.3 DC-SCM CPLD firmware 63
17. Hardware Management 63
18. Security (only for Platform Boards and Systems) 64
19. Interoperability 64
19.1 HPM FRU Requirements 64
20. References 66
Appendix A - Checklist for IC approval of this Specification (to be completed by contributor(s) of this Spec) 67

List of Figures

Figure 1 Block Diagram....13
Figure 2 Board Stackup....14
Figure 3 Board Placement Top Side....15
Figure 4 Board Placement Bottom Side....16
Figure 5 Board Mechanical....17
Figure 6 Sensor Locations on the Board....18
Figure 7 Card Edge Connector Dimensions – Top Side (“B” Pins)....19
Figure 8 Straddle Mount Connector Dimensions (mm)....20
Figure 9 DC-SCI LVDS Differential Channels between DC-SCM and HPM....27
Figure 10 Project Argus I2C/I3C Block Diagram....30
Figure 11 eSPI Block Diagram....31
Figure 12 Project Argus SPI Topology between DC-SCM and HPM....32
Figure 13 Project Argus USB Block Diagram....33
Figure 14 Project Argus UART Block Diagram....37
Figure 15 Presence Detection and Power Protection Example....39
Figure 16 Discovery Sequence....41
Figure 17 AST1060 Block Diagram....43
Figure 18 Project Argus UART Block Diagram....46
Figure 19 UART Connector on I/O Panel....47
Figure 20 Project Argus Intrusion Detection Block Diagram....48
Figure 21 Mechanical Overview....49
Figure 22 Board Dimensions....50
Figure 23 Keep-out Zones – Top-side....50
Figure 24 Keep-out Zones – Bottom-side....51
Figure 25 Keep-out Zones – Side....51
Figure 26 Faceplate Bracket Subassembly....52
Figure 27 Module Assembly Overview....53
Figure 28 Chassis Bay Opening Dimensions....54
Figure 29 Project Argus Front Panel Definition....55
Figure 30 Project Argus Front Panel I/O Ports....55
Figure 31 Project Argus Front Panel Buttons....56
Figure 32 Project Argus Front Panel LED....56
Figure 33 Project Argus Internal Lock Mechanism....57
Figure 34 Disassembling the Module from Enclosure....58
Figure 35 Project Argus Power Delivery Block Diagram....58

List of Tables

Table 1 DC-SCI Pinout Overview....21
Table 2 Side A Pinout....24
Table 3 Side B Pinout....26
Table 4 LTPI Signal Descriptions....28
Table 5 DC-SCI LTPI Pin Assignment....28
Table 6 Project Argus DC-SCI SGPIO Pin Assignment....29
Table 7 Project Argus AST2600 I2C/I3C Mapping Table....30
Table 8 Project Argus DC-SCI USB Pin Assignment....33
Table 9 DC-SCI PCIe Clock Pin Assignment....34
Table 10 DC-SCI PCIE Pin Assignment....35
Table 11 DC-SCI PECI Pin Assignment....35
Table 12 DC-SCI JTAG Pin Assignment....36
Table 13 DC-SCI NC-SI Clock Pin Assignment....36
Table 14 DC-SCI UART Pin Assignment....37
Table 15 DC-SCI PWR_BTN_N Pin Assignment....38
Table 16 DC-SCI Discovery/Sequence Signals Pin Assignment....39
Table 17 Power States and Discovery Sequence....40
Table 18 CPLD GPIO to LTPI Mapping....44
Table 19 SGPIO Register Table....46
Table 20 Button/LED GPIO Mapping....47
Table 21 Power Consumption....59
Table 22 Environmental Regulations....60
Table 23 HPM FRU Requirements....65

1. License

1.1. OPTION B: Open Web Foundation (OWF) CLA

Notes:

The above license does not apply to the Appendix or Appendices. The information in the Appendix or Appendices is for reference only and non-normative in nature.
NOTWITHSTANDING THE FOREGOING LICENSES, THIS SPECIFICATION IS PROVIDED BY OCP "AS IS" AND OCP EXPRESSLY DISCLAIMS ANY WARRANTIES (EXPRESS, IMPLIED, OR OTHERWISE), INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, FITNESS FOR A PARTICULAR PURPOSE, OR TITLE, RELATED TO THE SPECIFICATION. NOTICE IS HEREBY GIVEN, THAT OTHER RIGHTS NOT GRANTED AS SET FORTH ABOVE, INCLUDING WITHOUT LIMITATION, RIGHTS OF THIRD PARTIES WHO DID NOT EXECUTE THE ABOVE LICENSES, MAY BE IMPLICATED BY THE IMPLEMENTATION OF OR COMPLIANCE WITH THIS SPECIFICATION. OCP IS NOT RESPONSIBLE FOR IDENTIFYING RIGHTS FOR WHICH A LICENSE MAY BE REQUIRED IN ORDER TO IMPLEMENT THIS SPECIFICATION. THE ENTIRE RISK AS TO IMPLEMENTING OR OTHERWISE USING THE SPECIFICATION IS ASSUMED BY YOU. IN NO EVENT WILL OCP BE LIABLE TO YOU FOR ANY MONETARY DAMAGES WITH RESPECT TO ANY CLAIMS RELATED TO, OR ARISING OUT OF YOUR USE OF THIS SPECIFICATION, INCLUDING BUT NOT LIMITED TO ANY LIABILITY FOR LOST PROFITS OR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT, SPECIAL OR PUNITIVE DAMAGES OF ANY CHARACTER FROM ANY CAUSES OF ACTION OF ANY KIND WITH RESPECT TO THIS SPECIFICATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, AND EVEN IF OCP HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

1.2 Acknowledgements

The Contributors of this Specification would like to acknowledge the following companies for their feedback:

Cloudflare
Lenovo

2. Compliance with OCP Tenets

2.1. Openness

Project Argus is an open design and follows the DC-SCM 2.0 base specification. A detailed design specification is provided including reference design files needed to allow recreation of the design.

2.2. Efficiency

Project Argus DC-SCM 2.0 is designed to be a cost effective and energy efficient design consuming under 20W.

2.3. Impact

Project Argus DC-SCM 2.0 provides a DC-SCM reference design with hardware and firmware implementation details to enable fast deployment and interoperability across a multitude of HPM implementations by complying with the DC-SCI interface.

2.4. Scale

Project Argus DC-SCM 2.0 is designed to optimize TCO for large scale implementation by using a common server management module across large deployments. It enables the design and deployment of the HPM and DC-SCM with increased efficiency for time to market.

2.5. Sustainability

Project Argus DC-SCM 2.0 is a modular design that is specified to work with a multitude of HPM implementations by complying with the DC-SCI interface. By following the DC-SCI pinout and definition, the common server management, security, and control features can be used across multiple platforms of the same generation and across platforms of different generations. Project Argus DC-SCM 2.0 enables standardizing common HWRoT, boot, monitoring, control, and remote debugging for these diverse platforms.

3. Version Table

Date	Version #	Author	Description
5/15/2023	1.0	Lenovo, Cloudflare	Initial Release

4. Scope

This document defines the technical specification for Project Argus which is a DC-SCM 2.0 compliant module based on the OCP DC-SCM Rev2.0 Ver1.0 Base Specification.

The requirements and objectives for the specification are:

- A collection of specifications defining Project Argus DC-SCM 2.0, which would enable interoperability of a multitude of HPM implementations with a spec compliant DC-SCI interface.
- A collection of specifications of ingredients associated with direct interfacing to Project Argus DC-SCM 2.0 in support of enabling the above objective.

The scope of the Specification shall be limited to the following:

- DC-SCM form-factor details including mechanical outlines of the faceplate, mechanics of locking mechanism, and mount-points.
- Definition of interfaces from the DC-SCM to HPM including but not limited to interface pin-out, electrical signaling, and sequencing.
- Definition of I/O connectors on the DC-SCM including but not limited to type of connector, electrical signaling, and placement.
- Definition of firmware requirements and operation for purposes of discovery and management.
- Requirements pertaining to the use of HWRoT solution for firmware attestations.
- Additional details and documents to improve interoperability of DC-SCM designs including but limited to schematic reference design, bill of materials, stackup, block diagrams and minimum bootable device tree requirements.

Without limiting the scope, the following subject matter is specifically out of scope under this Specification:

- Specification, definition, and design of chassis
- Cables, peripherals, peripheral form-factors, peripheral subsystems, HPM, non-DC-SCM devices part of a chassis
- Details pertaining to specific CPU and memory implementations
- Proprietary implementation details pertaining to AST2600 Integrated Remote Management Processor of ASPEED Technology Inc.
- Proprietary implementation details pertaining to AST1060 HWRoT Processor of ASPEED Technology Inc.
- Proprietary LTPI implementation details pertaining to Lattice MachXO3D CPLD of Lattice Semiconductor

5. Overview

Project Argus is an implementation based on the OCP DC-SCM Rev2.0 Ver1.0 Base Specification. Project Argus DC-SCM 2.0 allows connection to different single node configuration HPM platforms providing a common server management and security solution across different platforms. At the heart of the module is the ASPEED AST2600 BMC SoC, which when loaded with a compatible OpenBMC firmware, provides a rich set of common features necessary for remote server management. Project Argus DC-SCM 2.0 uses ASPEED AST1060 as the HWRoT solution providing secure firmware authentication, firmware recovery, and firmware update capability. Project Argus DC-SCM 2.0 uses Lattice MachXO3D CPLD with secure boot and dual boot ability as the DC-SCM CPLD to support a variety of IO interfaces including LTPI, SGPIO, UART and GPIOs. Project Argus DC-SCM 2.0 is implemented in the horizontal External Form Factor (EFF) design.

6. Rack Compatibility

Project Argus DC-SCM 2.0 module is mechanically compatible within any system that has a DC-SCM 2.0 horizontal EFF slot and is not rack dependent.

7. Physical Specifications

7.1 Block Diagram

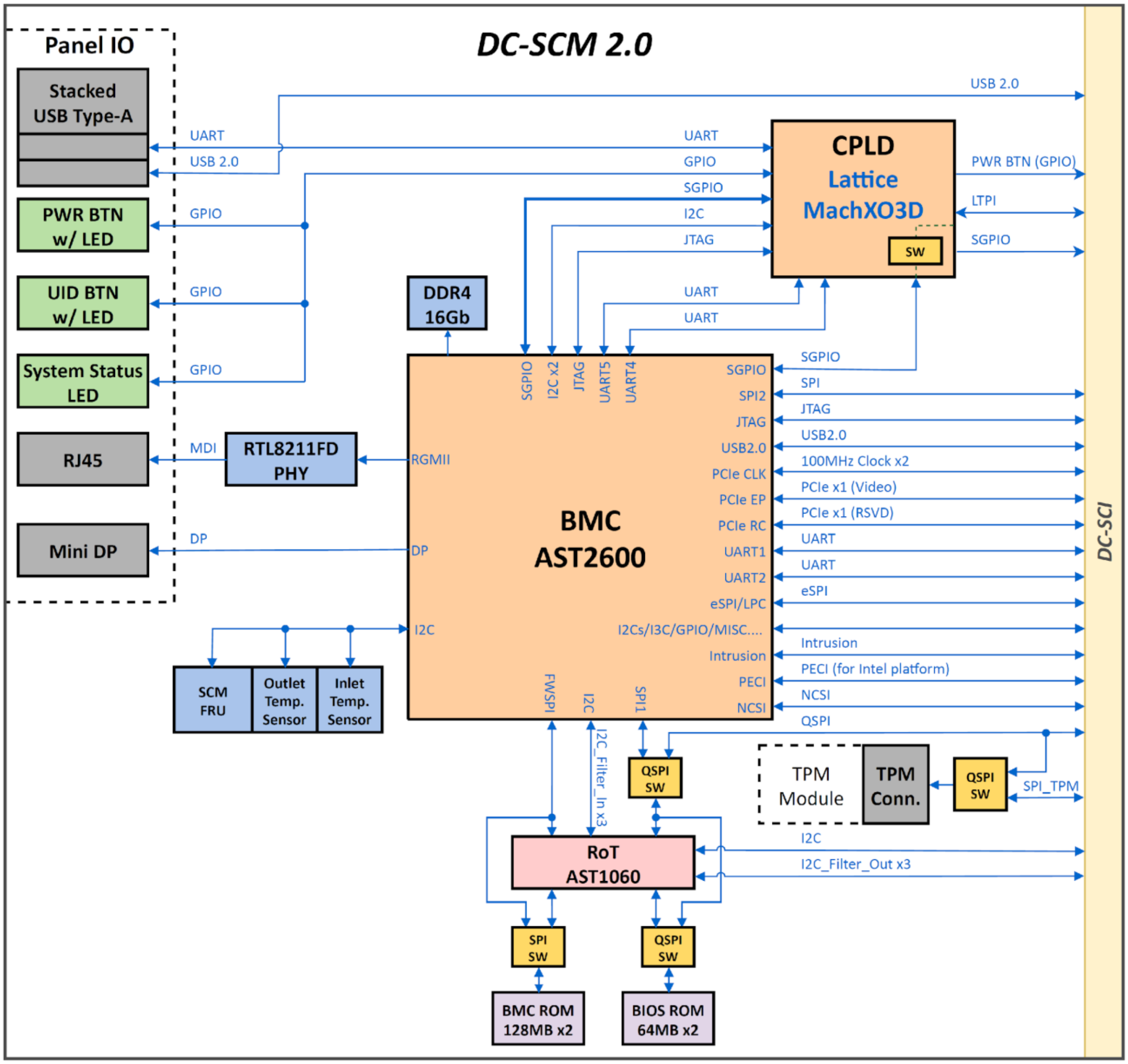
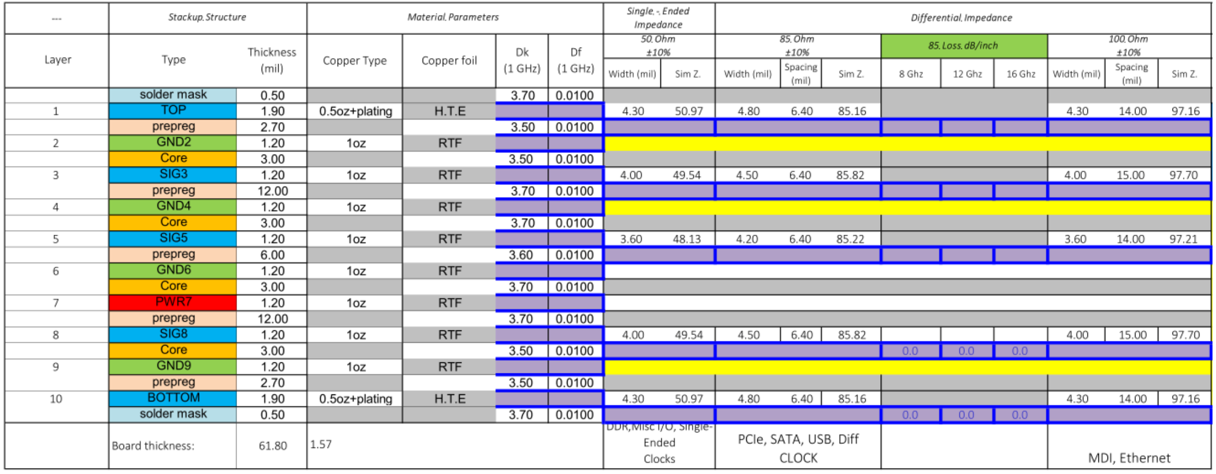


Figure 1 Block Diagram

7.2 PCB Overview

7.2.1 Board Stack-up



---	Stackup.Structure		Material.Parameters				Single.-.Ended Impedance		Differential.Impedance								
Layer	Type	Thickness (mil)	Copper Type	Copper foil	Dk (1 GHz)	Df (1 GHz)	50.Ohm ±10%		85.Ohm ±10%			85.Loss.dB/inch			100.Ohm ±10%		
							Width (mil)	Sim Z.	Width (mil)	Spacing (mil)	Sim Z.	8 Ghz	12 Ghz	16 Ghz	Width (mil)	Spacing (mil)	Sim Z.
	solder mask	0.50			3.70	0.0100											
1	TOP	1.90	0.5oz+plating	H.T.E			4.30	50.97	4.80	6.40	85.16				4.30	14.00	97.16
	prepreg	2.70			3.50	0.0100											
2	GND2	1.20	1oz	RTF													
	Core	3.00			3.50	0.0100											
3	SIG3	1.20	1oz	RTF			4.00	49.54	4.50	6.40	85.82				4.00	15.00	97.70
	prepreg	12.00			3.70	0.0100											
4	GND4	1.20	1oz	RTF													
	Core	3.00			3.70	0.0100											
5	SIG5	1.20	1oz	RTF			3.60	48.13	4.20	6.40	85.22				3.60	14.00	97.21
	prepreg	6.00			3.60	0.0100											
6	GND6	1.20	1oz	RTF													
	Core	3.00			3.70	0.0100											
7	PWR7	1.20	1oz	RTF													
	prepreg	12.00			3.70	0.0100											
8	SIG8	1.20	1oz	RTF			4.00	49.54	4.50	6.40	85.82				4.00	15.00	97.70
	Core	3.00			3.50	0.0100						0.0	0.0	0.0			
9	GND9	1.20	1oz	RTF													
	prepreg	2.70			3.50	0.0100											
10	BOTTOM	1.90	0.5oz+plating	H.T.E			4.30	50.97	4.80	6.40	85.16				4.30	14.00	97.16
	solder mask	0.50			3.70	0.0100						0.0	0.0	0.0			
	Board thickness:	61.80	1.57				DDR,Misc I/O, Single-Ended Clocks		PCIe, SATA, USB, Diff CLOCK						MDI, Ethernet		

Figure 2 Board Stackup

7.2.2 Board Placement Top Side

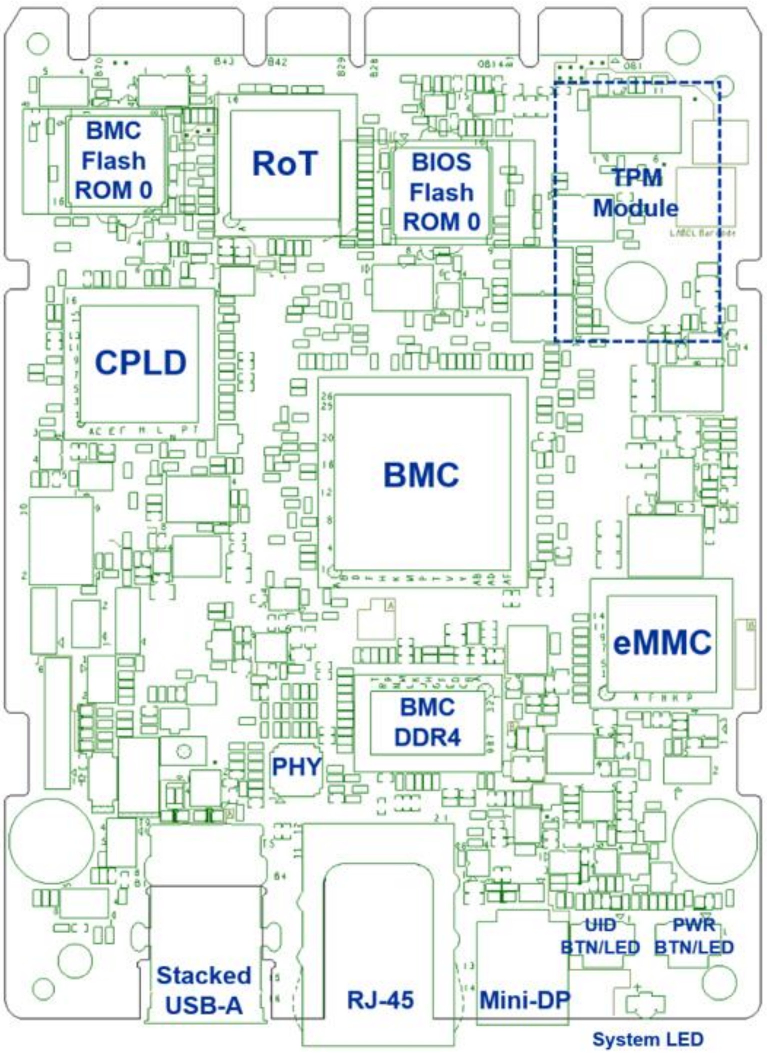


Figure 3 Board Placement Top Side

7.2.3 Board Placement Bottom Side

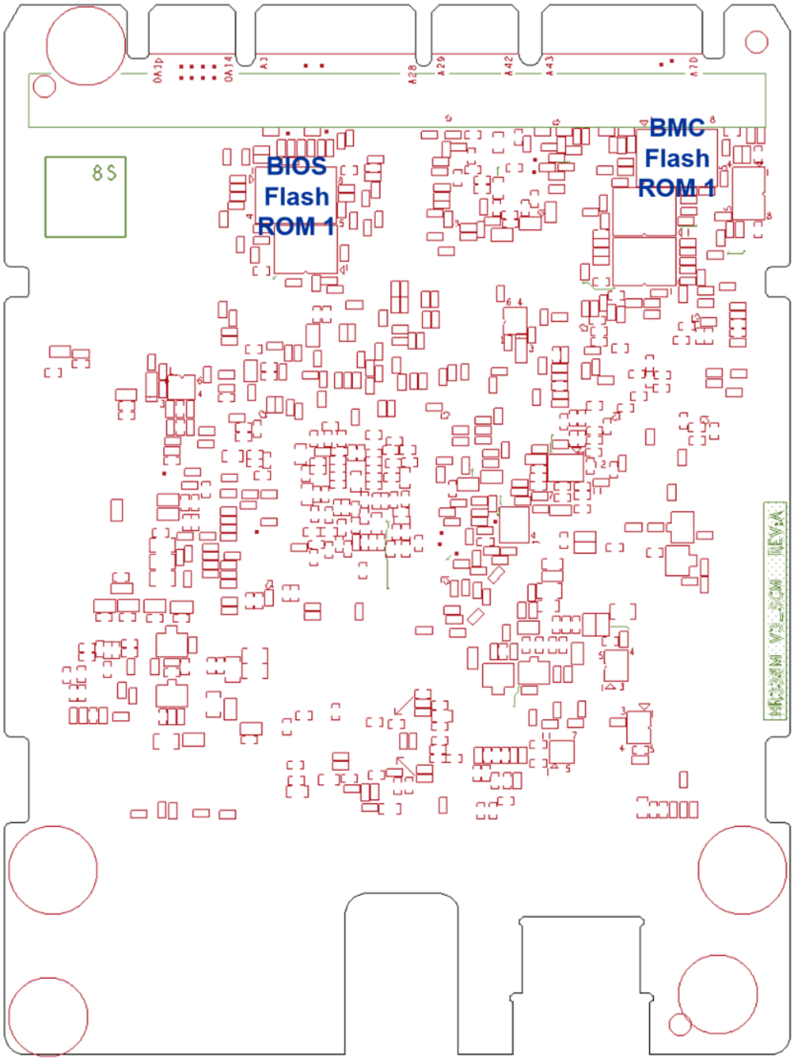


Figure 4 Board Placement Bottom Side

7.2.4 Board Mechanical

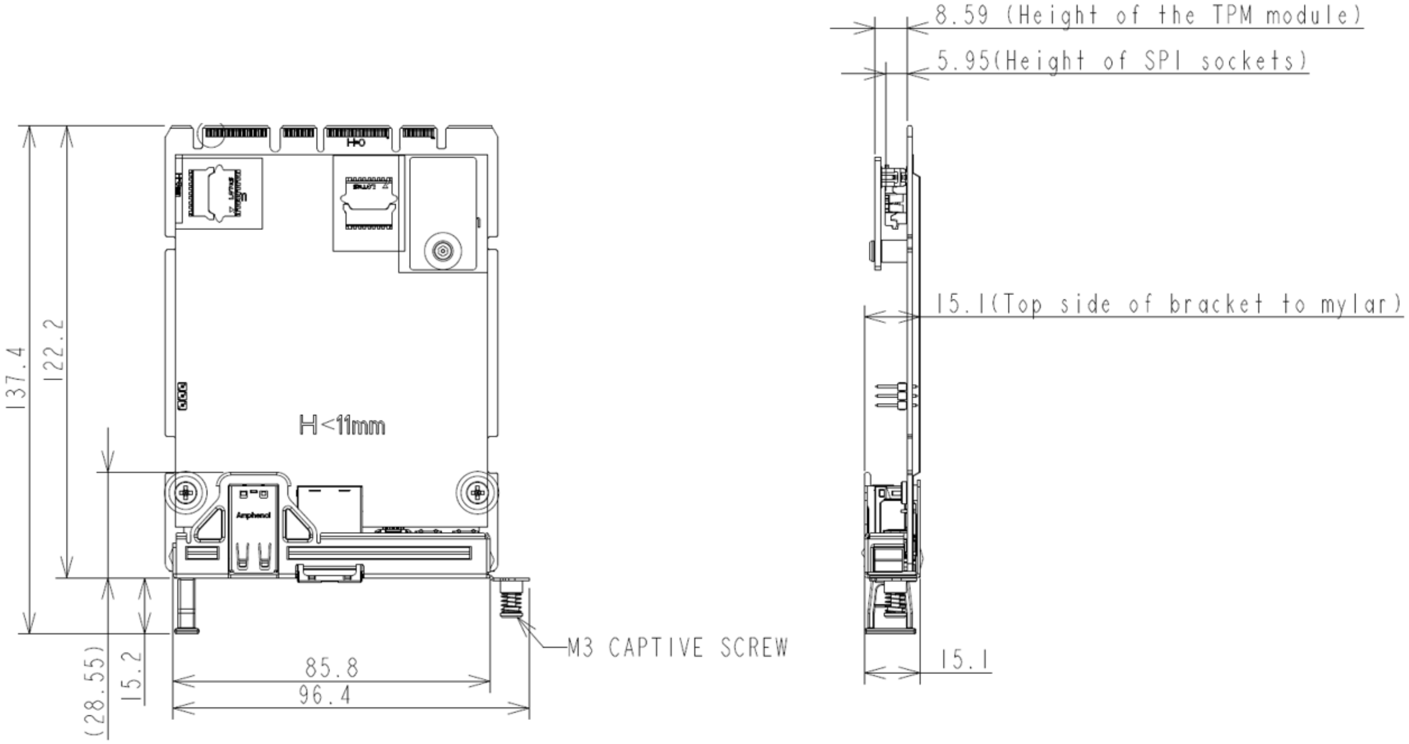

8.59 (Height of the TPM module)
5.95(Height of SPI sockets)
137.4
122.2
H<11mm
Amphenol
15.1(Top side of bracket to mylar)
M3 CAPTIVE SCREW
(28.55)
15.2
85.8
96.4
15.1

Figure 5 Board Mechanical

8. Thermal Design Requirements

8.1 Thermal Design Conditions

Project Argus DC-SCM 2.0 module and its components are expected to operate without any thermal issues and meet thermal reliability requirements in the following environmental conditions.

- Ambient temperature: 5°C to 40°C
- Card inlet temperature: 50°C

8.2 Sensor Locations on Board

There are two ambient temperature sensors on the module. When the DC-SCM is installed at the rear of the chassis, Temperature Sensor #1 measures the inlet temperature of the module and Temperature Sensor #2 measures the outlet temperature of the module. BMC firmware accesses these temperature sensors via I2C bus15. See the figure below for the approximate sensor locations on the board.

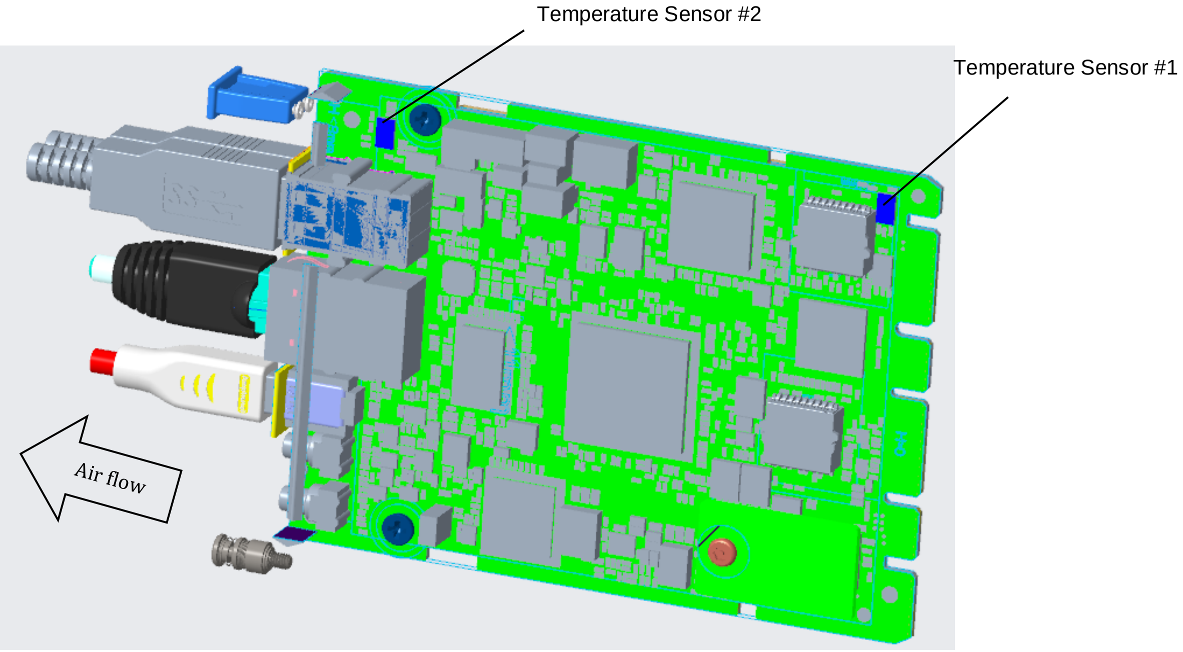


Figure 6 Sensor Locations on the Board

9. I/O System

9.1 DC-SCI Card Edge Connector Requirement

The DC-SCI card edge connector interface is compliant to the SFF-TA-1002 specification with respect to the 4C+ connector size which complies with the OCP DC-SCM Rev2.0 Ver1.0 Base Specification. Mechanical details of the edge finger requirements are shown in the figure below.

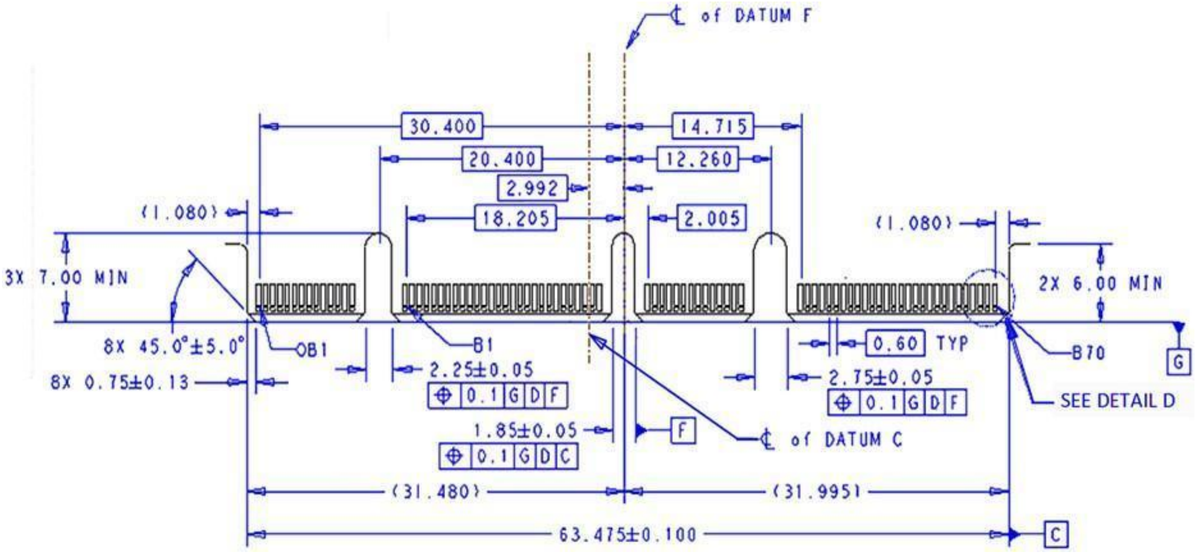


Figure 7 Card Edge Connector Dimensions – Top Side (“B” Pins)

9.2 Gold Finger Plating Requirement

The minimum gold finger plating shall be 30µinches of gold over 50µinches of nickel which complies with the OCP DC-SCM Rev2.0 Ver1.0 Base Specification.

9.3 HPM Connector Requirement

Project Argus DC-SCM 2.0 module is connected coplanar to the HPM through a straddle mount connector and fastened by two M2 screws. The dimensions of the straddle mount connector are shown in the figure below.

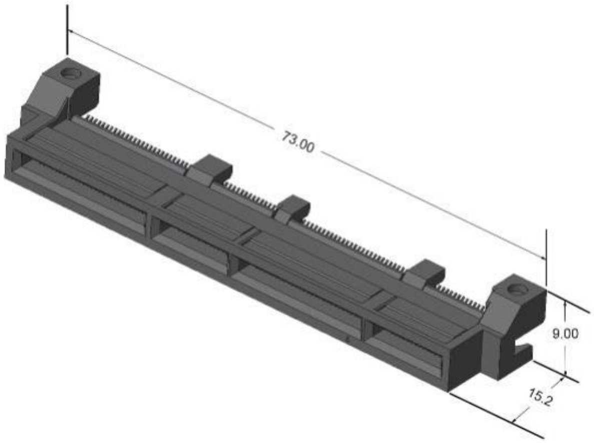


Figure 8 Straddle Mount Connector Dimensions (mm)

9.4 DC-SCI Pin Definition

Project Argus DC-SCI pinout fully complies with the OCP DC-SCI Rev2.0 Ver1.0 Pin Definition. An overview of the interfaces supported by Project Argus DC-SCI connector pinout is defined in the table below.

Function
12V Aux Power
Power Sequencing & Presence Detection
JTAG
LTPI (LVDS)
BMC PCIe x1 End Point
BMC PCIe x1 Root Complex
eSPI (Single Node/CPU P0)
QSPI (Single Node/CPU P0)
SPI
PECI
BMC USB 2.0 Host
BMC USB 2.0 Endpoint
NC-SI

2 x I3C 1.0V
6 x I2C/I3C 1.8V
10 x I2C 3.3V
1 x GPI
TPM SPI
UART0
UART1

Table 1 DC-SCI Pinout Overview

The detailed pin assignments of the DC-SCI connector are captured in the tables below.

Side A	Single Node Primary / Alternative Function (if Applicable)	Voltage Single/Dual	Direction DC-SCM View	**Project Argus DC-SCM 2.0**
OA1	GND			GND
OA2	**PCIE_HPMROOT_SCM_HPM_0_DN** / USB3_SCMHOST2_SCM_HPM_DN		output / output	NC_PCIE_HPMROOT_SCM_HPM_0_DN
OA3	**PCIE_HPMROOT_SCM_HPM_0_DP** / USB3_SCMHOST2_SCM_HPM_DP		output / output	NC_PCIE_HPMROOT_SCM_HPM_0_DP
OA4	GND			GND
OA5	**PCIE_HPMROOT_SCM_HPM_1_DN** / LTPI2_SCM_HPM_CLK_DN / DISPLAYPORT_SCM_HPM_LANE0_DN	PCIe / LTPI / DP	output/ output/ output	NC_PCIE_HPMROOT_SCM_HPM_1_DN
OA6	**PCIE_HPMROOT_SCM_HPM_1_DP** / LTPI2_SCM_HPM_CLK_DP / DISPLAYPORT_SCM_HPM_LANE0_DP	PCIe / LTPI / DP	output/ output/ output	NC_PCIE_HPMROOT_SCM_HPM_1_DP
OA7	GND			GND
OA8	**PCIE_HPMROOT_SCM_HPM_2_DN** / SGMII_SCM_HPM_DN		output / output	NC_PCIE_HPMROOT_SCM_HPM_2_DN
OA9	**PCIE_HPMROOT_SCM_HPM_2_DP** / SGMII_SCM_HPM_DP		output / output	NC_PCIE_HPMROOT_SCM_HPM_2_DP
OA10	GND			GND
OA11	**PCIE_HPMROOT_SCM_HPM_3_DN** / LTPI2_SCM_HPM_DATA_DN / DISPLAYPORT_SCM_HPM_LANE1_DN	PCIe / LTPI / DP	output / output/ output	NC_PCIE_HPMROOT_SCM_HPM_3_DN
OA12	**PCIE_HPMROOT_SCM_HPM_3_DP** / LTPI2_SCM_HPM_DATA_DP / DISPLAYPORT_SCM_HPM_LANE1_DP	PCIe / LTPI / DP	output / output/ output	NC_PCIE_HPMROOT_SCM_HPM_3_DP

OA13	GND			GND
OA14	**PECI_HPM_SCM** / GPIO	0.85-1.21	inout	PECI_BMC
A1	P12V_AUX		input	P12V_SCM_AUX
A2	P12V_AUX		input	P12V_SCM_AUX
A3	P12V_AUX		input	P12V_SCM_AUX
A4	P12V_AUX		input	P12V_SCM_AUX
A5	GND			GND
A6	GND			GND
A7	PRSNT1_HPM_SCM_N	0	input	PRSNT1_N
A8	JTAG_SCMCNTRL_TCK	3.3	output	HPM_JTAG_TCK
A9	JTAG_SCMCNTRL_TDI	3.3	input	HPM_JTAG _TDI
A10	JTAG_SCMCNTRL_TDO	3.3	output	HPM_JTAG _TDO
A11	JTAG_SCMCNTRL_TMS	3.3	output	HPM_JTAG _TMS
A12	JTAG_SCMCNTRL_TRST_N	3.3	output	HPM_JTAG _TRST_N
A13	SCM_HPM_STBY_RST_N	3.3	output	PFR_HPM_STBY_RST_N
A14	SCM_HPM_STBY_EN	3.3	output	HPM_STBY_EN
A15	I2C_3V3_0_SCL	3.3	inout	DCSCI_BMC_I2C_R_SCL11
A16	I2C_3V3_0_SDA	3.3	inout	DCSCI_BMC_I2C_R_SDA11
A17	I2C_3V3_1_SCL	3.3	inout	DCSCI_I2C_3V3_SCL7_ROT
A18	I2C_3V3_1_SDA	3.3	inout	DCSCI_I2C_3V3_SDA7_ROT
A19	GND			GND
A20	LTPI_SCM_HPM_DATA_DN		output	LTPI_SCM_HPM_DATA_DN
A21	LTPI_SCM_HPM_DATA_DP		output	LTPI_SCM_HPM_DATA_DP
A22	GND			GND
A23	LTPI_SCM_HPM_CLK_DN		output	LTPI_SCM_HPM_CLK_DN
A24	LTPI_SCM_HPM_CLK_DP		output	LTPI_SCM_HPM_CLK_DP
A25	GND			GND
A26	I2C_3V3_2_SCL	3.3	inout	DCSCI_I2C_3V3_SCL9_ROT
A27	I2C_3V3_2_SDA	3.3	inout	DCSCI_I2C_3V3_SDA9_ROT
A28	PCIE_HPM_SCM_PERST_N	3.3	input	PCIE_HPM_SCM_PERST_N
A29	GND			GND
A30	PCIE_HPMROOT_SCM_HPM_4_DN		output	PCIE_HPMROOT_SCM_HPM_RX_C_DN
A31	PCIE_HPMROOT_SCM_HPM_4_DP		output	PCIE_HPMROOT_SCM_HPM_RX_C_DP
A32	GND			GND
A33	**PCIE_SCMROOT_SCM_HPM_DN** / USB3_SCMHOST1_SCM_HPM_DN		output / output	PCIE_SCMROOT_SCM_HPM_TX_C_DN
A34	**PCIE_SCMROOT_SCM_HPM_DP** / USB3_SCMHOST1_SCM_HPM_DP		output / output	PCIE_SCMROOT_SCM_HPM_TX_C_DP
A35	GND			GND
A36	PCIE_HPM_SCM_CLK_100M_0_DN		input	PCIE_HPM_SCM_CLK_100M_0_DN
A37	PCIE_HPM_SCM_CLK_100M_0_DP		input	PCIE_HPM_SCM_CLK_100M_0_DP
A38	GND			GND
A39	**I2C_I3C_1V0_18_SCL** / FSI_1V2_0_SCL	1.0/1.2	inout	DCSCI_I3C_1V0_SCL1
A40	**I2C_I3C_1V0_18_SDA** / FSI_1V2_0_SDA	1.0/1.2	inout	DCSCI_I3C_1V0_SDA1

A41	**I2C_I3C_1V0_19_SCL** / FSI_1V2_1_SCL	1.0/1.2	inout	DCSCI_I3C_1V0_SCL2
A42	**I2C_I3C_1V0_19_SDA** / FSI_1V2_1_SDA	1.0/1.2	inout	DCSCI_I3C_1V0_SDA2
A43	I2C_3V3_3_SCL	3.3 (Single) 1.8 (Dual)	inout	DCSCI_BMC_I2C_R_SCL12
A44	I2C_3V3_3_SDA	3.3 (Single) 1.8 (Dual)	inout	DCSCI_BMC_I2C_R_SDA12
A45	I2C_3V3_4_SCL	3.3 (Single) 1.8 (Dual)	inout	DCSCI_BMC_I2C_R_SCL10
A46	I2C_3V3_4_SDA	3.3 (Single) 1.8 (Dual)	inout	DCSCI_BMC_I2C_R_SDA10
A47	I2C_3V3_5_SCL	3.3 (Single) 1.8 (Dual)	inout	DCSCI_BMC_I2C_R_SCL5
A48	I2C_3V3_5_SDA	3.3 (Single) 1.8 (Dual)	inout	DCSCI_BMC_I2C_R_SDA5
A49	I2C_3V3_6_SCL	3.3 (Single) 1.8 (Dual)	inout	DCSCI_I2C_3V3_SCL6_ROT
A50	I2C_3V3_6_SDA	3.3 (Single) 1.8 (Dual)	inout	DCSCI_I2C_3V3_SDA6_ROT
A51	I2C_I3C_1V8_16_SCL	1.8	inout	DCSCI_BMC_I2C_R_SCL3_1V8
A52	I2C_I3C_1V8_16_SDA	1.8	inout	DCSCI_BMC_I2C_R_SDA3_1V8
A53	GND			GND
A54	**SPI_HPMCNTRL_TPM_CLK** / I2C_I3C_1V8_10_SCL	1.8	input / inout	SPI_TPM_CLK
A55	**SPI_HPMCNTRL_TPM_CS_N** / I2C_I3C_1V8_10_SDA / QSPI_HPMCNTRL_TPM_CS_N	1.8	input / inout / input	SPI_TPM_CS_N
A56	**SPI_HPMCNTRL_TPM_MOSI** / I2C_I3C_1V8_11_SCL	1.8	input / inout	SPI_TPM_MOSI
A57	**SPI_HPMCNTRL_TPM_MISO** / I2C_I3C_1V8_11_SDA	1.8	output / inout	SPI_TPM_MISO
A58	I2C_I3C_1V8_12_SCL	1.8	inout	DCSCI_I2C_SCL_ROT_1V8
A59	I2C_I3C_1V8_12_SDA	1.8	inout	DCSCI_I2C_SDA_ROT_1V8
A60	GPI / **SPI_SCMCNTRL_IRQ0_N**	1.8	input / input	SPI_HPM_SCM_IRQ0_N
A61	I2C_I3C_1V8_13_SCL	1.8	inout	DCSCI_I2C8_SCL_1V8
A62	I2C_I3C_1V8_13_SDA	1.8	inout	DCSCI_I2C8_SDA_1V8
A63	**UART0_HPM_SCM_DATA** / GPIO	3.3	input / inout	UART0_HPM_SCM_DATA
A64	GND			GND
A65	PCIE_HPMROOT_SCM_HPM_5_DN		output	NC_PCIE_HPMROOT_SCM_HPM_5_DN
A66	PCIE_HPMROOT_SCM_HPM_5_DP		output	NC_PCIE_HPMROOT_SCM_HPM_5_DP
A67	GND			GND

A68	**PCIE_HPM_SCM_CLK_100M_1_S0_DN** / PCIE_HPM_SCM_CLK_100M_1_S5_DN		input / input	PCIE_HPM_SCM_CLK_100M_1_S0_DN
A69	**PCIE_HPM_SCM_CLK_100M_1_S0_DP** / PCIE_HPM_SCM_CLK_100M_1_S5_DP		input / input	PCIE_HPM_SCM_CLK_100M_1_S0_DP
A70	GND			GND

Table 2 Side A Pinout

Side B	Single Node Primary / Alternative Function (if Applicable)	Voltage Single/Dual	Direction DC-SCM View	**Project Argus DC-SCM 2.0**
OB1	GND			GND
OB2	**PCIE_HPMROOT_HPM_SCM_0_DN** / USB3_SCMHOST2_HPM_SCM_DN		input / input	NC_PCIE_HPMROOT_HPM_SCM_0_DN
OB3	**PCIE_HPMROOT_HPM_SCM_0_DP** / USB3_SCMHOST2_HPM_SCM_DP		input / input	NC_PCIE_HPMROOT_HPM_SCM_0_DP
OB4	GND			GND
OB5	**PCIE_HPMROOT_HPM_SCM_1_DN** / LTPI2_HPM_SCM_CLK_DN / DISPLAYPORT_AUX_DN	PCIe / LTPI / DP	input / input / inout	NC_PCIE_HPMROOT_HPM_SCM_1_DN
OB6	**PCIE_HPMROOT_HPM_SCM_1_DP** / LTPI2_HPM_SCM_CLK_DP / DISPLAYPORT_AUX_DP	PCIe / LTPI / DP	input / input / inout	NC_PCIE_HPMROOT_HPM_SCM_1_DP
OB7	GND			GND
OB8	**PCIE_HPMROOT_HPM_SCM_2_DN** / SGMII_HPM_SCM_DN		input / input	NC_PCIE_HPMROOT_HPM_SCM_2_DN
OB9	**PCIE_HPMROOT_HPM_SCM_2_DP** / SGMII_HPM_SCM_DP		input / input	NC_PCIE_HPMROOT_HPM_SCM_2_DP
OB10	GND			GND
OB11	**PCIE_HPMROOT_HPM_SCM_3_DN** / LTPI2_HPM_SCM_DATA_DN / USB2_SCMHOST3_DN	PCIe / LTPI / USB2	input / input / inout	NC_PCIE_HPMROOT_HPM_SCM_3_DN
OB12	**PCIE_HPMROOT_HPM_SCM_3_DP** / LTPI2_HPM_SCM_DATA_DP / USB2_SCMHOST3_DP	PCIe / LTPI / USB2	input / input / inout	NC_PCIE_HPMROOT_HPM_SCM_3_DP
OB13	GND			GND
OB14	PECI_VREF_HPM_SCM / GPI	0.85-1.21	input	PVCCIO_PECI
B1	ESPI_HPMCNTRL_CLK	1.8	input	ESPI_HPMCNTRL_CLK
B2	ESPI_HPMCNTRL_CS0_N	1.8	input	ESPI_HPMCNTRL_CS0_N
B3	ESPI_HPMCNTRL_RESET_N	1.8	input	ESPI_HPMCNTRL_RESET_N

B4	ESPI_HPMCNTRL_IO_0	1.8	inout	ESPI_HPMCNTRL_IO_0
B5	ESPI_HPMCNTRL_IO_1	1.8	inout	ESPI_HPMCNTRL_IO_1
B6	ESPI_HPMCNTRL_IO_2	1.8	inout	ESPI_HPMCNTRL_IO_2
B7	ESPI_HPMCNTRL_IO_3	1.8	inout	ESPI_HPMCNTRL_IO_3
B8	ESPI_HPMCNTRL_ALERT0_N	1.8	output	ESPI_HPMCNTRL_ALERT0_N
B9	I2C_I3C_1V8_17_SCL / ESPI0_HPMCNTRL_CS1_N	1.8	inout / input	DCSCI_BMC_I2C_R_SCL4_1V8
B10	I2C_I3C_1V8_17_SDA / ESPI0_HPMCNTRL_ALERT1_N	1.8	inout / output	DCSCI_BMC_I2C_R_SDA4_1V8
B11	GND			GND
B12	QSPI_HPMCNTRL_CLK	1.8	input	SYS_QSPI_CLK_1V8
B13	QSPI_HPMCNTRL_CS0_N	1.8	input	SYS_QSPI_CS0_1V8_N
B14	QSPI_HPMCNTRL_IO_0	1.8	inout	SYS_QSPI_D0_1V8
B15	QSPI_HPMCNTRL_IO_1	1.8	inout	SYS_QSPI_D1_1V8
B16	QSPI_HPMCNTRL_IO_2	1.8	inout	SYS_QSPI_D2_1V8
B17	QSPI_HPMCNTRL_IO_3	1.8	inout	SYS_QSPI_D3_1V8
B18	QSPI_HPMCNTRL_CS1_N / GPI	1.8	input / input	**SYS_QSPI_CS1_1V8_N**
B19	GND			GND
B20	LTPI_HPM_SCM_DATA_DN		input	LTPI_HPM_SCM_DATA_DN
B21	LTPI_HPM_SCM_DATA_DP		input	LTPI_HPM_SCM_DATA_DP
B22	GND			GND
B23	LTPI_HPM_SCM_CLK_DN		input	LTPI_HPM_SCM_CLK_DN
B24	LTPI_HPM_SCM_CLK_DP		input	LTPI_HPM_SCM_CLK_DP
B25	GND			GND
B26	HPM_SCM_STBY_RDY	3.3	input	HPM_STBY_RDY
B27	HPM_SCM_INTRUSION_N	3.3/BAT	input	FM_INTRUDER_BMC_N
B28	P3V0_HPM_SCM_BAT	3.0 BAT	input	P3V_BAT
B29	GND			GND
B30	PCIE_HPMROOT_HPM_SCM_4_DN		input	PCIE_HPMROOT_HPM_SCM_TX_DN
B31	PCIE_HPMROOT_HPM_SCM_4_DP		input	PCIE_HPMROOT_HPM_SCM_TX_DP
B32	GND			GND
B33	**PCIE_SCMROOT_HPM_SCM_DN** / USB3_SCMHOST1_HPM_SCM_DN		input / input	PCIE_SCMROOT_HPM_SCM_RX_DN
B34	**PCIE_SCMROOT_HPM_SCM_DP** / USB3_SCMHOST1_HPM_SCM_DP		input / input	PCIE_SCMROOT_HPM_SCM_RX_DP
B35	GND			GND
B36	USB2_SCMHOST1_DN / **USB2_HPMHOST1_DN** / GPIO	3.3	inout / inout	USB2_HPMHOST1_DN
B37	USB2_SCMHOST1_DP / **USB2_HPMHOST1_DP** / GPIO	3.3	inout / inout	USB2_HPMHOST1_DP
B38	GND			GND
B39	I2C_I3C_1V8_14_SCL	1.8	inout	DCSCI_ROTBMC_I3C_SCL1_1V8
B40	I2C_I3C_1V8_14_SDA	1.8	inout	DCSCI_ROTBMC_I3C_SDA1_1V8
B41	I2C_I3C_1V8_15_SCL	1.8	inout	DCSCI_BMC_I2C_R_SCL2_1V8
B42	I2C_I3C_1V8_15_SDA	1.8	inout	DCSCI_BMC_I2C_R_SDA2_1V8

B43	**NCSI_HPM_SCM_CLK** / GPIO	3.3	input	NCSI_CLK
B44	**NCSI_HPM_SCM_CRS_DV** / GPIO	3.3	input	NCSI _CRS_DV
B45	**NCSI_SCM_HPM_TX_EN** / GPIO	3.3	output	NCSI_TXEN
B46	**NCSI_SCM_HPM_D0** / GPIO	3.3	output	NCSI_TXD0
B47	**NCSI_SCM_HPM_D1** / GPIO	3.3	output	NCSI_TXD1
B48	**NCSI_HPM_SCM_D0** / GPIO	3.3	input	NCSI_RXD0
B49	**NCSI_HPM_SCM_D1** / GPIO	3.3	input	NCSI_RXD1
B50	VCC_SCM_HPM_FRU	3.3	output	VCC_SCM_HPM_FRU
B51	**UART0_SCM_HPM_DATA** / PCIE_SCM_HPM_PERST_N/ GPO/ NCSI2_SCM_HPM_TX_EN	3.3	output / output / output	UART0_SCM_HPM_DATA
B52	I2C_3V3_7_SCL / **SGPIO_CLK** / NCSI2_HPM_SCM_CLK	3.3	inout / output / output	SGPIO_SCM_HPM_CLK
B53	I2C_3V3_7_SDA / **SGPIO_LD** / NCSI2_HPM_SCM_CRS_DV /	3.3	inout / output / output	SGPIO_SCM_HPM_LD
B54	I2C_3V3_8_SCL / **SGPIO_DATAOUT** / NCSI2_SCM_HPM_D0	3.3	inout / output / inout	SGPIO_SCM_HPM_DATAOUT
B55	I2C_3V3_8_SDA / **SGPIO_DATAIN** / NCSI2_SCM_HPM_D1	3.3	inout / input / inout	SGPIO_SCM_HPM_DATAIN
B56	I2C_3V3_9_SCL / **UART1_SCM_HPM_DATA** / NCSI2_HPM_SCM_D0	3.3	inout / output / inout	UART2_TX_SCM_HPM_DATA
B57	I2C_3V3_9_SDA / **UART1_HPM_SCM_DATA** / NCSI2_HPM_SCM_D1	3.3	inout / input / inout	UART2_RX_HPM_SCM_DATA
B58	PRSNT0_SCM_HPM_N	0	output	PRSNT0_N
B59	SPI_SCMCNTRL_CS1_N / **GPIO**	3.3	output / inout	PWR_BTN_N
B60	SPI_SCMCNTRL_CLK	3.3	output	SPI_SCMCNTRL_CLK
B61	SPI_SCMCNTRL_MISO	3.3	input	SPI_SCMCNTRL_MISO
B62	SPI_SCMCNTRL_MOSI	3.3	output	SPI_SCMCNTRL_MOSI
B63	SPI_SCMCNTRL_CS0_N	3.3	output	SPI_SCMCNTRL_CS0_N
B64	GND			GND
B65	PCIE_HPMROOT_HPM_SCM_5_DN		input	NC_PCIE_HPMROOT_HPM_SCM_5_DN
B66	PCIE_HPMROOT_HPM_SCM_5_DP		input	NC_PCIE_HPMROOT_HPM_SCM_5_DP
B67	GND			GND
B68	USB2_SCMHOST2_DN / **USB2_HPMHOST2_DN** / GPIO	3.3	inout / inout	USB2_HPMHOST2_DN
B69	USB2_SCMHOST2_DP / **USB2_HPMHOST2_DP**/ GPIO	3.3	inout / inout	USB2_HPMHOST2_DP
B70	GND			GND

Table 3 Side B Pinout

9.5 Project Argus DC-SCI Signal Descriptions and Examples

9.5.1 LVDS Tunneling Protocol and Interface (LTPI)

Project Argus DC-SCM 2.0 implementation of LTPI fully adheres to the electrical specification of LTPI defined in OCP DC-SCM Rev2.0 Ver1.0 Base Specification as well as OCP DC-SCM 2.0 LVDS Tunneling Protocol & Interface Specification . The LTPI uses a total of 8 x CPLD LVDS differential I/O pins for connecting the DC-SCM CPLD with the HPM CPLD.

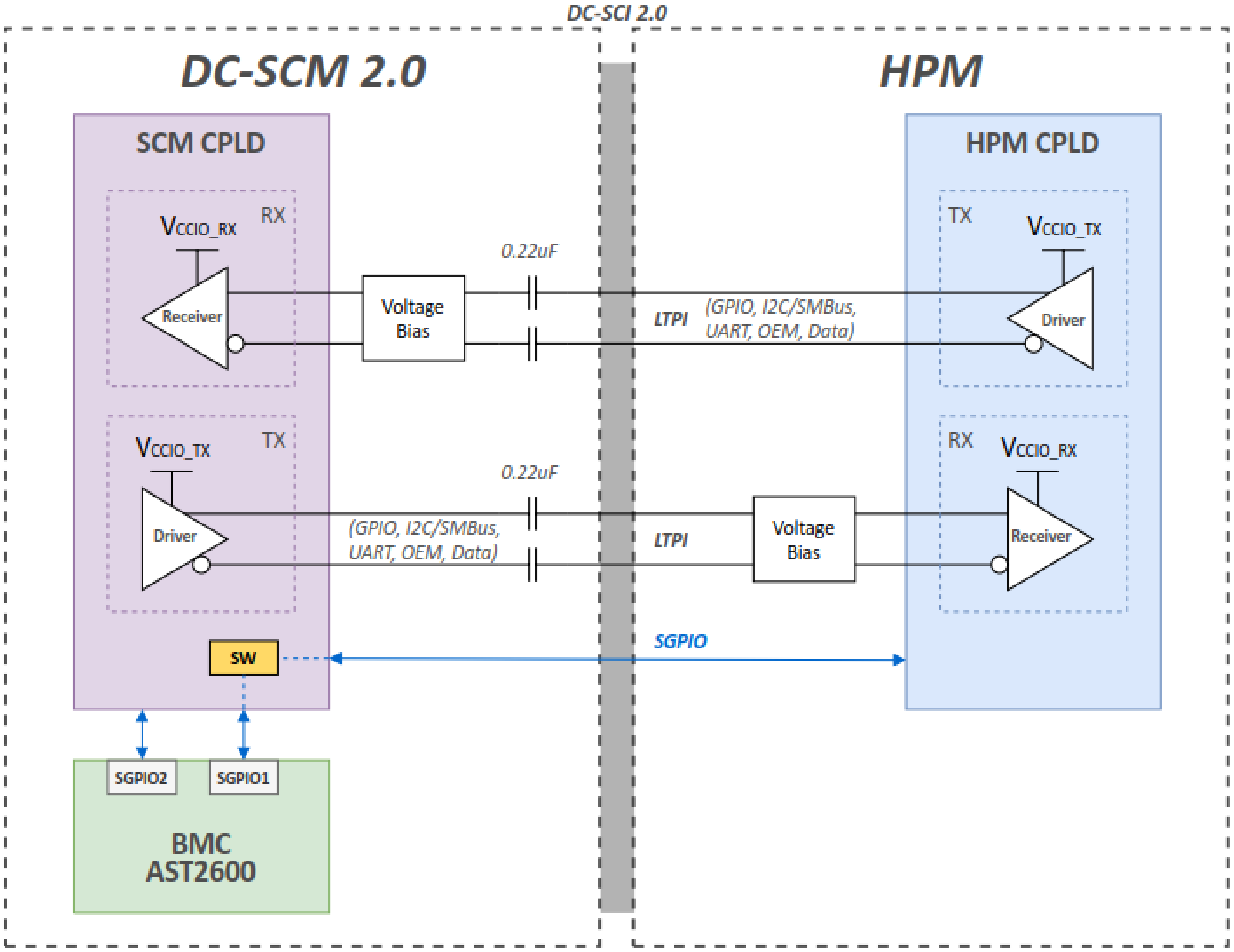


Figure 9 DC-SCI LVDS Differential Channels between DC-SCM and HPM

There are a total of 4 x LVDS unidirectional links defined for HPM-to-SCM and SCM-to-HPM communication. The links in each direction are defined by 2 x LVDS-based channels i.e. DATA and CLOCK. The description of the LTPI I/O pins and the direction of LVDS links from DC-SCM CPLD and HPM CPLD are listed in the tables below. Refer to section 9.8.2 for more information on the LTPI architecture.

Function	HPM CPLD LVDS I/O	SCM CPLD LVDS I/O
LTPI_HPM_SCM_DATA_DN	TX Data Negative	RX Data Negative
LTPI_HPM_SCM_DATA_DP	TX Data Positive	RX Data Positive
LTPI_HPM_SCM_CLK_ DN	TX Clock Negative	RX Clock Negative
LTPI_HPM_SCM_CLK_ DP	TX Clock Positive	RX Clock Positive
LTPI_SCM_HPM_DATA_DN	RX Data Negative	TX Data Negative
LTPI_SCM_HPM_DATA_DP	RX Data Positive	TX Data Positive
LTPI_SCM_HPM_CLK_DN	RX Clock Negative	TX Clock Negative
LTPI_SCM_HPM_CLK_DP	RX Clock Positive	TX Clock Positive

Table 4 LTPI Signal Descriptions

DC-SCM Side	DC-SCI Pin #	DC-SCI	HPM Side
CPLD	A20/21	LTPI_DATA RX	CPLD
CPLD	A23/24	LTPI_ CLK RX	CPLD
CPLD	B20/21	LTPI_DATA TX	CPLD
CPLD	B23/24	LTPI_ CLK TX	CPLD

Table 5 DC-SCI LTPI Pin Assignment

9.5.2 SGPIO

Project Argus DC-SCI supports 1 x Serial GPIO (SGPIO) interface between the DC-SCM and the HPM. The purpose of the SGPIO interface is to provide a low pin count interface for transmitting status and control signals. Project Argus DC-SCM 2.0 utilizes the defined pins below for the alternative SGPIO function per the OCP DC-SCI Rev2.0 Ver1.0 Pin Definition..

DC-SCM Side	DC-SCI Pin #	DC-SCI	HPM Side
AST2600	B52	SGPIO_SCM_HPM_CLK	CPLD
AST2600	B53	SGPIO_SCM_HPM_LD	CPLD
AST2600	B55	SGPIO_SCM_HPM_DATAIN	CPLD
AST2600	B54	SGPIO_SCM_HPM_DATAOUT	CPLD

Table 6 Project Argus DC-SCI SGPIO Pin Assignment

9.5.3 I2C/I3C

Project Argus DC-SCI supports a total of 16 x I2C ports and 4 x I3C ports from the DC-SCM to the HPM. The I2C/I3C bus mapping is shown in the table below.

AST2600	AST2600 pin	HWRoT/CPLD	DC-SCI	HPM
I3C_1	AF23/AF24	X	A39/A40	CPU0_DIMM_ABCDEF
I3C_2	AF22/AE22	X	A41/A42	CPU0_DIMM_GHIJKL
I3C_3	AF25/AF26	X	X	X
I3C_4	AE25/AF24	X	X	X
HVI3C3	B20/A20	X	B39/B40	From BMC/HWRoT to CPU via I3C MUX, reserved for CPU attestation on Intel platform.
SMB_2	E19/D20	X	B41/B42	**For 1.8V I2C devices**
SMB_3	C19/A19	X	A51/A52	**For 1.8V I2C devices**
SMB_4	C20/D19	X	B9/B10	**For 1.8V I2C devices**
SMB_5	A11/C11	X	A47/A48	**For 3.3V I2C devices** **Example:** HPM CPLD
SMB_6	D12/E13	HWRoT	A49/A50	**Example:** Power supply, PDB
SMB_7	D11/E11	HWRoT	A17/A18	**Example:** Drive backplane
SMB_8	F13/E12	X	A61/A62	**For 1.8V I2C devices**
SMB_9	D15/A14	HWRoT	A26/A27	**Example:** Digital VRs
SMB_10	E15/A13	X	A45/A46	**Example:** APML
SMB_11	M24/M25	X	A15/A16	**For 3.3V I2C devices, HPM FRU**

SMB_12	L26/K24	X	A43/A44	For 3.3V I2C devices
SMB_15	D18/B17	CPLD	X	X
SMB_16	C17/E18	HWRoT	X	X

Table 7 Project Argus AST2600 I2C/I3C Mapping Table

Project Argus DC-SCM 2.0 I2C/I3C block diagram is shown in the figure below.

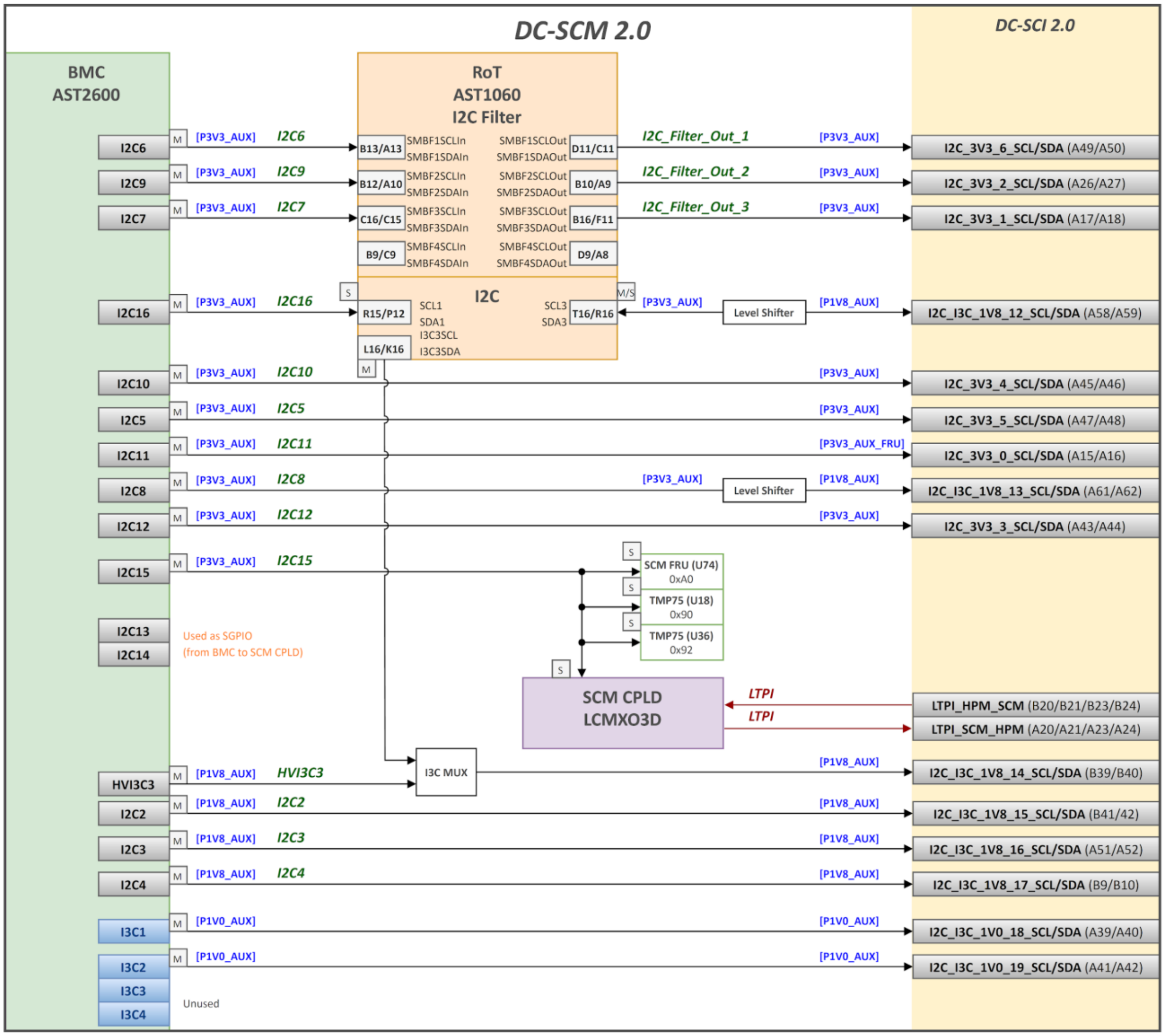


Figure 10 Project Argus I2C/I3C Block Diagram

9.5.4 eSPI

Project Argus supports single node configurations with 1 x HPM to DC-SCM eSPI bus defined. CS0#/ALERT0# should be used for the BMC. Even though known hosts vary in their need for utilizing eSPI in S5, they are tolerant to S5 bias.

There is no LPC bus support in Project Argus. Host to BMC interface details when eSPI is unavailable are outside the scope of this specification.

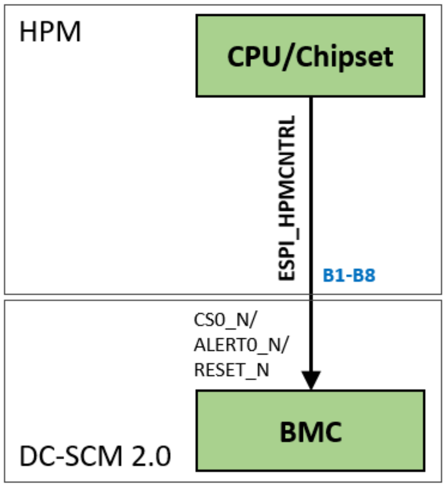


Figure 11 eSPI Block Diagram

9.5.5 QSPI and SPI

Project Argus supports single-node configuration and the DC-SCI Pin definition supports 1 x QSPI and 1 x SPI interface:

- QSPI (SYS_QSPI_x):
  HPM is the initiator. This enables HPM communication with the BIOS flash devices and TPM on the DC-SCM. Only one QSPI bus is defined for a single-node design.
- SPI_SCMCNTRL (SPI_SCMCNTRL_x):
  DC-SCM is the initiator. This enables DC-SCM communication with expansion devices on the HPM such as the HPM CPLD. Note that only one SPI_HPM_SCM_IRQ0_N discrete signal is defined like in DC-SCM 1.0. Additional shared or non-shared interrupts must be tunneled via LTPI.

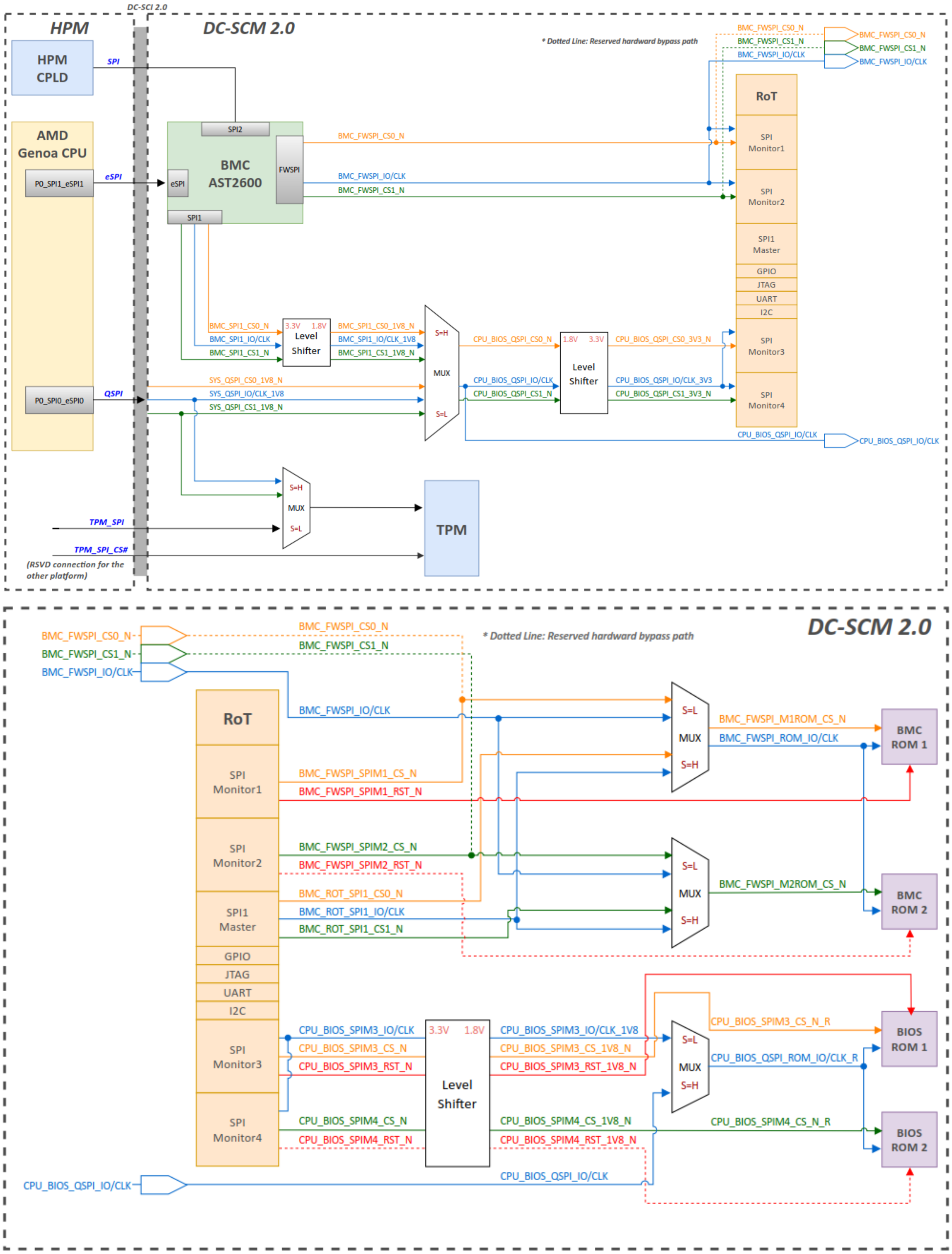


Figure 12 Project Argus SPI Topology between DC-SCM and HPM

9.5.6 USB

Project Argus DC-SCM 2.0 supports a USB 2.0 port that is located on the front faceplate. The USB signal (USB2_HPMHOST1_x) comes directly from the host CPU through the DC-SCI connector.

Project Argus DC-SCI supports a second USB bus (USB2_HPMHOST2_x) that is connected between the host CPU and the BMC. This USB bus is used as the BMC managed USB host controller connectivity to the HPM for a high-speed management interface to various subsystems and extended peripherals.

DC-SCM Side	DC-SCI Pin #	DC-SCI	HPM Side
AST2600: USB2A	B68/B69	USB2_HPMHOST2_DN/ USB2_HPMHOST2_DP	USB Host
Front USB 2.0	B36/B37	USB2_HPMHOST1_DN/ USB2_HPMHOST1_DP	USB Host

Table 8 Project Argus DC-SCI USB Pin Assignment

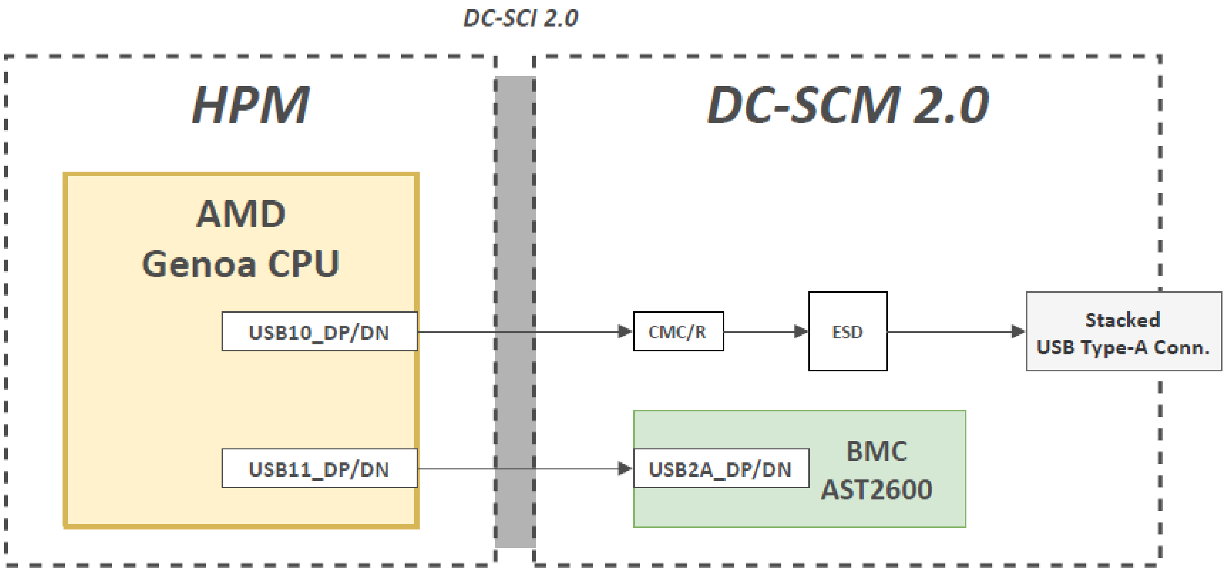


Figure 13 Project Argus USB Block Diagram

9.5.7 PCIE/Clock

Project Argus DC-SCI supports 2 x HPM provided PCIe clocks. On the reference design, both PCIe clocks are connected to the BMC. Alternatively, PCIE_HPM_SCM_CLK_100M_0 can be used to feed the PCIe x4 endpoint and PCIE_HPM_SCM_CLK_100M_1_S0 can be fanned out through a clock buffer and feed other (slower) PCIe devices.

Project Argus DC-SCI supports 7 x PCIe interfaces, each can support up to PCIe Gen 5 speed.

- PCIe x1 interface over pins A30 - B31 are connected to the BMC enabling host to BMC communication.
- PCIe x1 interface over pins A65 - B66 are not connected on the reference design but could be connected to a USB host controller or other PCIe x1 device.
- PCIe x1 interface over pins A33 - B34 are connected to BMC PCIE root complex port.
- PCIe x4 interface over pins OA2 - OB12 are not connected on the reference design but could be connected to PCIe x4 device or subdivided as 1 x4, 2 x2 lanes, 4 x1, or x2/x1/x1 lanes to connect to multiple endpoint(s).

Project Argus DC-SCI supports a PCIe reset signal from the HPM to the DC-SCM but does not support a PCIe reset signal from the DC-SCM to the HPM.

DC-SCM Side	DC-SCI Pin #	DC-SCI	HPM Side
AST2600	A68/A69	PCIE_HPM_SCM_CLK_100M_1_S0_DN/ PCIE_HPM_SCM_CLK_100M_1_S0_DP	PCIe clock from HPM (Gen5 compatible) **Example**: come from CPU/clock generator /clock buffer
AST2600	A36/A37	PCIE_HPM_SCM_CLK_100M_0_DN/ PCIE_HPM_SCM_CLK_100M_0_DP	PCIe clock from HPM (Gen5 compatible) **Example:** come from CPU/clock generator /clock buffer

Table 9 DC-SCI PCIe Clock Pin Assignment

DC-SCM Side	DC-SCI Pin #	DC-SCI	HPM Side
AST2600	A30/A31 B30/B31	PCIE_HPMROOT_SCM_HPM_RX_C_DN/ PCIE_HPMROOT_SCM_HPM_RX_C_DP/ PCIE_HPMROOT_HPM_SCM_TX_DN/ PCIE_HPMROOT_HPM_SCM_TX_DP	Gen5 Host or CPU
AST2600	A33/A34 B33/B34	PCIE_SCMROOT_SCM_HPM_TX_C_DP/ PCIE_SCMROOT_SCM_HPM_TX_C_DN. PCIE_SCMROOT_HPM_SCM_RX_DP/ PCIE_SCMROOT_HPM_SCM_RX_DN	Gen5 Host or CPU

Gen 5 device or NC	A65/A66 B65/B66	NC_PCIE_HPMROOT_SCM_HPM_5_DN/ NC_PCIE_HPMROOT_SCM_HPM_5_DP/ NC_PCIE_HPMROOT_HPM_SCM_5_DN/ NC_PCIE_HPMROOT_HPM_SCM_5_DP	Gen5 Host or CPU
Gen 5 device or NC	OA2/OA3 OB2/OB3	NC_PCIE_HPMROOT_SCM_HPM_0_DN/ NC_PCIE_HPMROOT_SCM_HPM_0_DP/ NC_PCIE_HPMROOT_HPM_SCM_0_DN/ NC_PCIE_HPMROOT_HPM_SCM_0_DP	Gen5 Host or CPU
Gen 5 device or NC	OA5/OA6 OB5/OB6	NC_PCIE_HPMROOT_SCM_HPM_1_DN/ NC_PCIE_HPMROOT_SCM_HPM_1_DP/ NC_PCIE_HPMROOT_HPM_SCM_1_DN/ NC_PCIE_HPMROOT_HPM_SCM_1_DP	Gen5 Host or CPU
Gen 5 device or NC	OA8/OA9 OB8/OB9	NC_PCIE_HPMROOT_SCM_HPM_2_DN/ NC_PCIE_HPMROOT_SCM_HPM_2_DP/ NC_PCIE_HPMROOT_HPM_SCM_2_DN/ NC_PCIE_HPMROOT_HPM_SCM_2_DP	Gen5 Host or CPU
Gen 5 device or NC	OA11/OA12 OB11/OB12	NC_PCIE_HPMROOT_SCM_HPM_3_DN/ NC_PCIE_HPMROOT_SCM_HPM_3_DP/ NC_PCIE_HPMROOT_HPM_SCM_3_DN/ NC_PCIE_HPMROOT_HPM_SCM_3_DP	Gen5 Host or CPU

Table 10 DC-SCI PCIE Pin Assignment

9.5.8 PECI

The DC-SCI supports an optional PECI interface (bus + power) for monitoring the health of CPUs. When this interface is not used by the HPM architecture, it should be properly terminated on the HPM. Refer to the CPU vendor and BMC vendor's documentations for detailed PECI electrical IO requirements. Note that the BMC controller PECI interface requires voltage to be supplied by the HPM.

When the PECI interface is not used on both the HPM and DC-SCM, the PECI_HPM_SCM signal may be used as a low voltage (0.85V-1.21V) GPIO biased only in host MAIN in S0 state. Also, PECI_VREF_HPM_SCM may be used as a unidirectional signal from HPM to DC-SCM in the same voltage range. Direction is limited due to the nature of this being a power signal in PECI operation.

DC-SCM Side	DC-SCI Pin #	DC-SCI	HPM Side
AST2600	OA14	PECI_HPM_SCM / GPIO	PECI
AST2600	OB14	PECI_VREF_HPM_SCM / GPI	PECI

Table 11 DC-SCI PECI Pin Assignment

9.5.9 JTAG

Project Argus DC-SCI supports a BMC initiator JTAG interface for use cases like:

- Programming of any HPM programmable devices (FPGA/CPLD or FPGA based PCIe Cards)
- Exposure of XDP or CPU debug capabilities to the BMC

DC-SCM Side	DC-SCI Pin #	DC-SCI	HPM Side
AST2600 (JTAG2)	A8	HPM_JTAG_TCK	JTAG
AST2600 (JTAG2)	A9	HPM_JTAG_TDI	JTAG
AST2600 (JTAG2)	A10	HPM_JTAG_TDO	JTAG
AST2600 (JTAG2)	A11	HPM_JTAG_TMS	JTAG
AST2600 (JTAG2)	A12	HPM_JTAG_TRST_N	JTAG

Table 12 DC-SCI JTAG Pin Assignment

9.5.10 NC-SI

Project Argus DC-SCI supports a RMII/NC-SI interface from the DC-SCM to the HPM. The description of the signals is shown in the table below. To best account for the timing requirements associated with the NC-SI clock, the clock source should be located on the HPM.

DC-SCM Side	DC-SCI Pin #	DC-SCI	HPM Side
AST2600	B43	NCSI_CLK	RMII Reference clock input The clock has a nominal frequency of 50MHz ±100ppm.
AST2600	B44	NCSI_CRS_DV	NC-SI carrier sense receive data valid signal
AST2600	B45	NCSI_TXEN	NC-SI Transmit Enable
AST2600	B46	NCSI_TXD0	BMC transmit to NC-SI interface
AST2600	B47	NCSI_TXD1	BMC transmit to NC-SI interface
AST2600	B48	NCSI_RXD0	BMC receive for NC-SI interface
AST2600	B49	NCSI_RXD1	BMC receive for NC-SI interface

Table 13 DC-SCI NC-SI Clock Pin Assignment

9.5.11 UART

Project Argus DC-SCI supports two sets of UART buses on the DC-SCI. One is connected to the CPU through a level shifter, while the other is connected to the HPM CPLD.

DC-SCM Side	DC-SCI Pin #	DC-SCI	HPM Side
AST2600	A63	UART0_HPM_SCM_DATA	CPU UART through level shifter
AST2600	B51	UART0_SCM_HPM_DATA	CPU UART through level shifter
AST2600	B56	UART2_TX_SCM_HPM_DATA	CPLD
AST2600	B57	UART2_RX_HPM_SCM_DATA	CPLD

Table 14 DC-SCI UART Pin Assignment

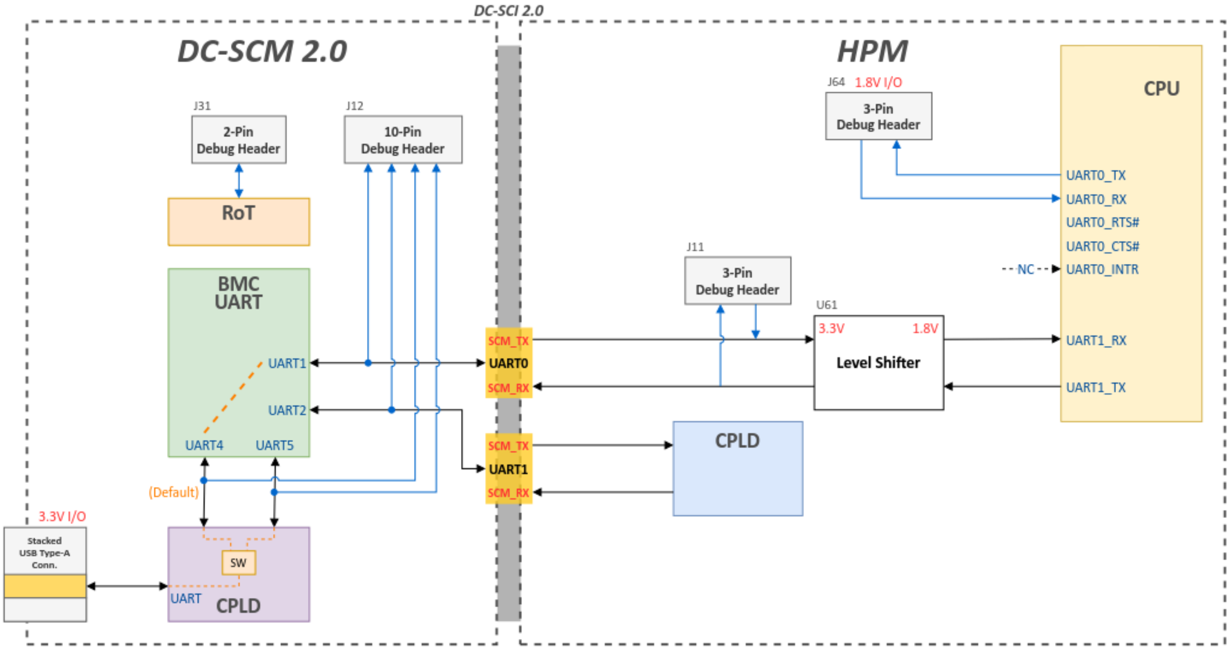


Figure 14 Project Argus UART Block Diagram

9.5.12 HPM Power Button

Project Argus DC-SCI supports a HPM Power Button (PWR_BTN_N) signal from the HPM. The signal is connected to a GPI of the DC-SCM CPLD and can be used in conjunction with the Power Button on Project Argus DC-SCM 2.0 faceplate to control the power of the system**.**

DC-SCM Side	DC-SCI Pin #	DC-SCI	HPM Side
CPLD	B59	PWR_BTN_N	Power Button and CPLD

Table 15 DC-SCI PWR_BTN_N Pin Assignment

9.6 Power States & Boot Sequence

Project Argus DC-SCM 2.0 power states adhere to the OCP DC-SCM Rev2.0 Ver1.0 Base Specification power states. The supported power states are shown below. All signals in the DC-SCI are categorized into each of these states indicating the minimum power state where bias is allowed at the DC-SCI.

The DC-SCM is not specified to support hot insertion or removal. In-rush control for the DC-SCM should be supported on the HPM to protect the circuitry from damages due to faulty connector pins.

Note that error handling of the power state sequence is beyond the scope of this specification. The DC-SCI provides two active low presence pins. The HPM design is recommended to ensure that AUX power to the DC-SCM and HPM circuits are disabled when presence is not detected. A presence enabled eFuse is strongly encouraged on the HPM but can be excluded since Project Argus is mechanically locked with a screw and an internal locking mechanism. The figure below provides an example implementation of a presence enabled eFuse.

Note: Not included in these states are scenarios such as a system level battery hold up or orchestration of the system power when a “high AUX” S5 state is required. That would entail a state where the host is OFF but the system requires more current than PSUs can provide on their AUX power rail. It should be noted that the DC-SCM’s maximum supported power level exceeds many PSU’s AUX rail capabilities and the system design would need to handle that accordingly.

DC-SCM Side	DC-SCI Pin #	DC-SCI	HPM Side
SCM Board	A7	PRSNT1_N	GND
SCM Board	B58	PRSNT0_N	eFuse, CPLD, PCH
CPLD	A14	HPM_STBY_EN	CPLD
CPLD	B26	HPM_STBY_RDY	CPLD
CPLD	A13	PFR_HPM_STBY_RST_N	CPLD

Table 16 DC-SCI Discovery/Sequence Signals Pin Assignment

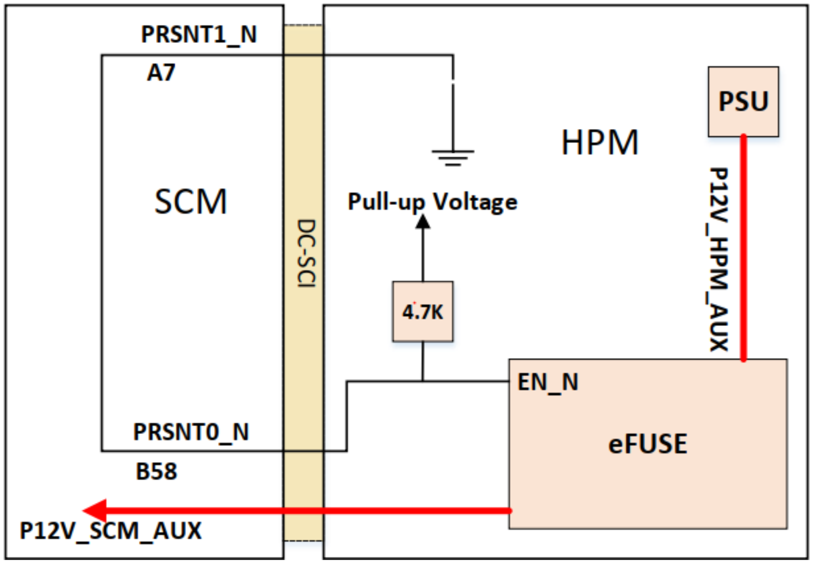


Figure 15 Presence Detection and Power Protection Example

Power State	Description
G3	No PSU Input power. Only bias power is from the coin cell battery.
Pre-STBY	1: On HPM, PSU(s) through PDB deliver P12V_AUX output power to the input of HPM eFuse. 2: If DC-SCM is fully seated, HPM eFuse becomes enabled (if present – see example above), providing power to the DC-SCM. 3: DC-SCM AUX VRs regulate and power BMC AUX rails, HWRoT AUX rails and VCC_SCM_HPM_FRU. 4: HWRoT authenticates its own image and boots. (See Section 16.2.2) 5: HWRoT authenticates BMC image, de-asserts BMC_PFR_SRST_N and allows DC-SCM BMC to boot. (See Section 16.2.3) 6: HWRoT authenticates UEFI image, de-asserts PFR_HPM_STBY_RST_N. (See Section 16.2.4) 7: DC-SCM BMC boots to a point to read the I2C HPM FRU (required) & performs HPM crypto authentication (optional). Note if HPM FRU is unrecognized, BMC will boot into a minimum bootable device tree config and the boot sequence is halted.
STBY	8: Upon compatibility check pass, DC-SCM asserts HPM_STBY_EN to enable HPM AUX circuits.
Pre-S5	9: HPM asserts HPM_STBY_RDY when all HPM AUX Rails are within regulation. 10: DC-SCM CPLD releases HPM_STBY_RST_N.
S5	11: S5 classified interfaces may engage. HPMs and DC-SCM must use PFR_HPM_STBY_RST_N as the qualifier for engaging S5 allowed DC-SCI signals. 12: HPM CPLD/FPGA enable the host CPU/Chipset (i.e. de-assert RSM_RST_N or assert AUXPWROK) to officially enter S5. Host is OFF. 13: Host WAKE request sources vary. Host power on request is typically blocked until a BMC grant so that BMC boot and security services and attestations are performed before PFR_HPM_STBY_RST_N is released.
S0	14: BMC grants power to HPM CPLD. HPM CPLD sequences the host into a full ON S0 state.

Table 17 Power States and Discovery Sequence

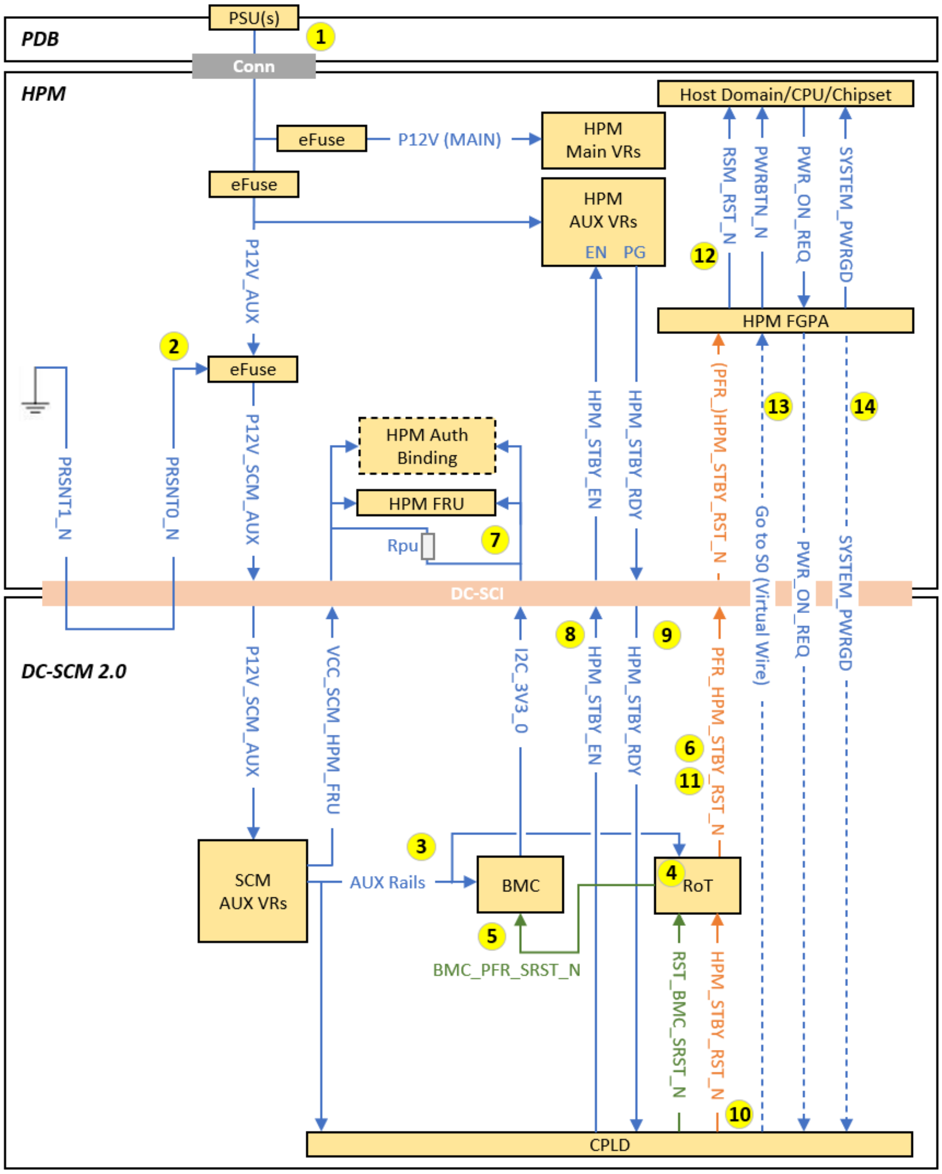


Figure 16 Discovery Sequence

9.6.1 Virtual Reseat

Project Argus DC-SCM 2.0 supports virtual reseat function. Virtual reseat is accomplished by de-asserting HPM_STBY_EN, which would return the system to Pre-STBY power state with all power rails on HPM to be removed completely or drain down to <5% of their nominal values for as long as the HPM_STBY_EN remains de-asserted. When HPM_STBY_EN is asserted, system moves to STBY power state and the HPM power rails are automatically restored.

9.7 Platform Root of Trust (PRoT)

Project Argus DC-SCM 2.0 functions as the management controller, as such, platform firmwares are stored on the module. Platform firmware resilience and security should be hardened which would add to physical security features like screws and internal lock mechanism. This is accomplished by a Platform Root of Trust that serves as the trust store of cryptographic keys which is used to authenticate firmware images including UEFI and BMC for secure boot process. In addition, the Platform Root of Trust should also protect platform firmwares from malicious attacks and suspicious activity, detect platform firmware data corruption, and recover from failed firmware updates, in accordance with recommendation published in National Institutes of Standards and Technology (NIST) Special Publication 800-193: Platform Firmware Resiliency Guidelines.

Project Argus DC-SCM 2.0 adopts the AST1060 HWRoT developed by ASPEED Technology Inc. as the Platform Root of Trust solution for the design. The root of trust is implemented in hardware, therefore immutable and inherently immune from malware attacks. AST1060 also complies to OCP Hardware Secure Boot Specification.

The AST1060 Hardware Root of Trust (HWRoT) features includes:

- Cryptographic engine to authenticate firmware signatures for the purpose of secure boot
- Support for AES 256 for secure boot image encryption
- Support for SHA384 for secure boot image measurement
- Support for ECDSA384 for secure boot image digest encryption
- Support for RSA4096 for secure boot key encryption
- 4 sets of QSPI with real time monitoring and filtering ability
- 4 sets of SMBUS interface with real time monitoring and filtering ability.
- Control interface to sequence secure boot process

Details on AST1060 HWRoT can be obtained from the vendor’s datasheet.

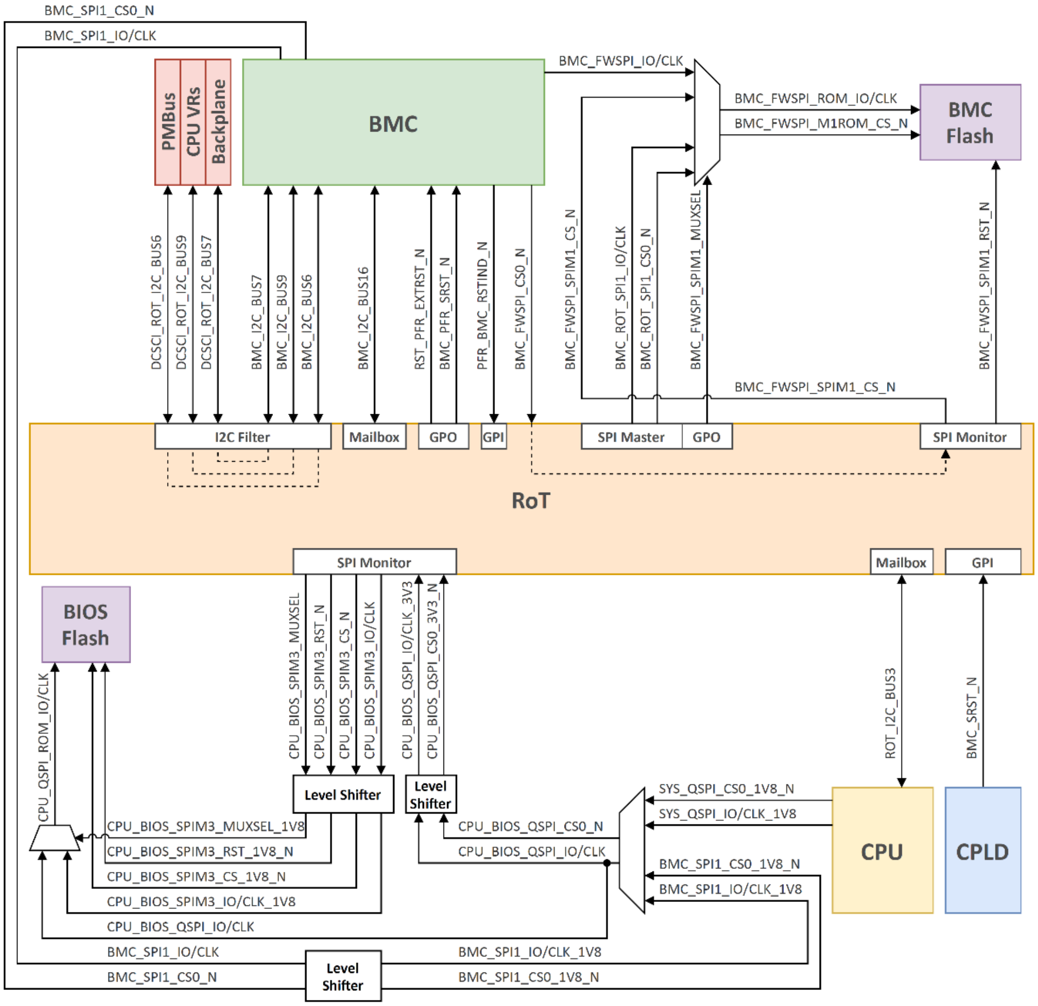


Figure 17 AST1060 Block Diagram

9.8 DC-SCM CPLD

Project Argus DC-SCM 2.0 uses Lattice MachXO3D as the DC-SCM CPLD and is critical in enabling a variety of key features of the module.

9.8.1 Secure Boot and Dual Boot

Even though DC-SCM CPLD binary is not authenticated by Platform Root of Trust described in section 9.7, Lattice MachXO3D supports secure boot and on-device dual boot flash maintaining high security posture with the ability to protect non-volatile memory, detect malicious code, and recover in case of corruption.

9.8.2 LTPI

DC-SCM LTPI architecture complies with the OCP DC-SCM 2.0 LVDS Tunneling Protocol & Interface Specification. More information is available on Lattice DC-SCM LVDS Tunneling Protocol and Interface IP Core - User Guide.

Project Argus DC-SCM 2.0 uses the LTPI bus to tunnel the following interfaces:

- Low Latency (LL) GPIO
- Normal Latency (NL) GPIO

No.	CPLD GPIO	CPLD Pin	Net Name	Direction	GPIO Type
0	PB44B	T13	FM_CPLD_BMC_PWRDN_N	O	LL
1			Reserved		LL
2			Reserved		LL
3			Internal register		LL
4			Internal register		LL
5			Reserved		LL
6	PB41B	T14	FM_PWRBRK_N	I	LL
7			Reserved		LL
8	PT9A	C4	FM_CPLD_HEARTBEAT_N	O	LL
9	PT12B	B4	FM_BMC_READY_N	I	LL
10	PT20B	C7	PCIE_HPM_SCM_PERST_N	I	LL
11	PT23B	A8	BMC_PFR_SRST_N	I	LL
12	PT24A	D8	RST_BMC_RSTBTN_OUT_R_N	I	LL
13	PT24B	E9	RST_RSMRST_N	O	LL
14	PT44A	B14	PCIE_HPM_SCM_CPLD_PERST_N	O	LL
15	PT44B	A15	RST_BMC_SRST_N	O	LL
0			Reserved		NL
1			Internal register		NL
2			Internal register		NL
3			Reserved		NL
4	PL12B	G3	IRQ_BMC_SMI_N	I	NL
5			Reserved		NL
6	PL27B	M1	HPM_STBY_RDY	I	NL
7	PL27A	L2	HPM_STBY_EN	O	NL
8	PB43A	R11	FM_THROTTLE_IN_N	O	NL
9	PL18D	K6	IRQ_TPM_SPI_N	O	NL
10			Internal register		NL
11			Reserved		NL
12	PR28D	P16	USB_EX1_OC_PLD_R_N	O	NL
13	PB33B	R10	FM_BMC_ENABLE	I	NL
14	PL25B	L3	HPM_STBY_RST_N	O	NL
15	PB18A	R7	FM_SPD_SWITCH_CTRL_N	I	NL
16			Reserved		NL
17	PB10B	R6	FM_BMC_PWRBTN_OUT_R_N	I	NL
18	PB5B	T4	SYS_PWROK_BMC	O	NL
19			Internal register		NL
20	PR3A	D16	BMC_RST_BTN_N	I	NL
21	PR3B	E14	RST_BTN_N	I	NL
22	PR14C	G11	CPLD_BIOS_ROM_SEL	O	NL
23	PR20C	J11	CPLD_ID_LED_N	O	NL

Table 18 CPLD GPIO to LTPI Mapping

9.8.3 SGPIO

DC-SCM CPLD includes 2 x SGPIO bus that connects to the BMC in addition to the SGPIO_SCM_HPM_x connection to the DC-SCI connector. SGPIO_SCM_CPLDIN_HPM_x bus tunnels SGPIO transactions from the SGPIO_SCM_HPM_x bus through the CPLD to the BMC. SGPIO_SCM_CPLD_x bus serializes GPIO transactions between DC-SCM CPLD and BMC for BMC to respond to button inputs and control the LEDs.

No.	CPLD Pin	BMC pin	Net Name	Direction	SGPIO Register Address	Register Bit Offset
0	-	E22	BMC_LED_PWR_RED_N	O	0x10	0
1	-	D23	BMC_LED_PWR_YELLOW_N	O	0x10	1
2	-	AE8	SPI_SCMCNTRL_CS0_R_N	O	0x10	2
3	-	T24	BMC_DBP_PREQ_N	O	0x10	3
4	-	AE14	MUXSEL_BIOS	O	0x10	4
5	-	AD24	A_P3V_BAT_SCALED_EN_N	O	0x10	5
6	-	Y23	FM_BMC_HEARTBEAT_N	O	0x10	6
7	-	D22	ROT_RSTIND_N	I	0x10	7
8	-	AD10	UID_BTN_BMC_N	I	0x10	8
9	-	B10	BMC_EXTRST_N	I	0x10	9
10~15	-		Reserved		0x10	10~15
16~31			Reserved		0x18	0~15
32	C4	-	FM_CPLD_HEARTBEAT_N	O	0x20	0
33	L16	-	P3V3_SCM_AUX_PG	I	0x20	1
34	L12	-	P2V5_SCM_AUX_PG	I	0x20	2
35	K15	-	P1V8_SCM_AUX_PG	I	0x20	3
36	J11	-	CPLD_ID_LED_N	O	0x20	4
37	K14	-	P1V2_SCM_AUX_PG	I	0x20	5
38	J13	-	P1V0_SCM_AUX_PG	I	0x20	6
39	K16	-	PWRGD_P0V6_SCM_AUX	I	0x20	7
40	H11	-	FM_P2V5_SCM_AUX_EN	O	0x20	8
41	J15	-	FM_P1V8_SCM_AUX_EN	O	0x20	9
42	J16	-	CPLD_AUX_EN_CTRL	O	0x20	10
43	H16	-	FM_P1V0_SCM_AUX_EN	O	0x20	11
44	J12	-	CPLD_PFR_DETECT_FAIL	I	0x20	12
45	G16	-	CPLD_USB_PWR_EN	O	0x20	13
46	G11	-	CPLD_BIOS_ROM_SEL	O	0x20	14
47	B3	-	FM_ME_BT_DONE	O	0x20	15
48	F16	-	FM_BMC_3V3_RGM_EN	O	0x28	0
49	E14	-	RST_BTN_N	I	0x28	1
50	P9	-	FM_ME_AUTHN_FAIL	I	0x28	2
51	L10	-	FM_P1V2_SCM_AUX_EN	O	0x28	3
52	N10	-	BIOS0_WP_R_N	O	0x28	4
53	M11	-	BIOS1_WP_R_N	O	0x28	5
54	R10	-	FM_BMC_ENABLE	I	0x28	6
55	T11	-	BMC0_WP_R_N	O	0x28	7
56	P11	-	BMC1_WP_R_N	O	0x28	8
57	L3	-	HPM_STBY_RST_N	O	0x28	9
58	L2	-	HPM_STBY_EN	O	0x28	10

59	M1	-	HPM_STBY_RDY	I	0x28	11
60	G1	-	FM_TPM_MOD_PRSNT_N	I	0x28	12
61	K6	-	IRQ_TPM_SPI_N	I	0x28	13
62	K3	-	RST_TPM_PLD_N	O	0x28	14
63	E1	-	RST_PHY_N	O	0x28	15

Table 19 SGPIO Register Table

9.8.4 I2C

DC-SCM CPLD includes an I2C bus that connects to BMC I2C15 port. This bus is not used but reserved for future telemetry purposes if needed.

9.8.5 JTAG

DC-SCM CPLD includes a JTAG interface that is connected to the BMC to support programming and configuration of the device as well as access to user logic.

9.8.6 UART

In addition to the UART buses over the DC-SCI defined in section 9.5.11, there are two additional UART buses on Project Argus DC-SCM 2.0 connected to the DC-SCM CPLD and debug header**.**

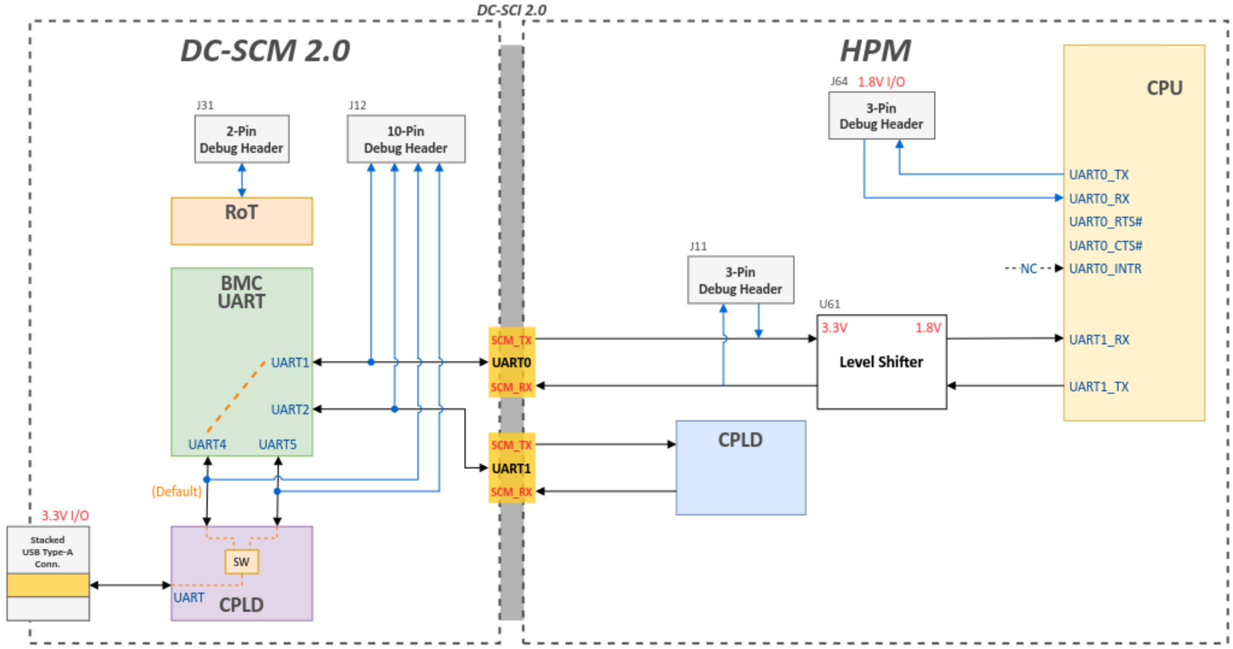


Figure 18 Project Argus UART Block Diagram

Due to space constraints, Project Argus DC-SCM 2.0 uses a USB type-A connector on the IO panel for UART signals which is connected to the CPLD for debug purposes. Within the DC-SCM CPLD is a UART bus switch that allows connection to the CPU UART bus or HPM CPLD UART bus.

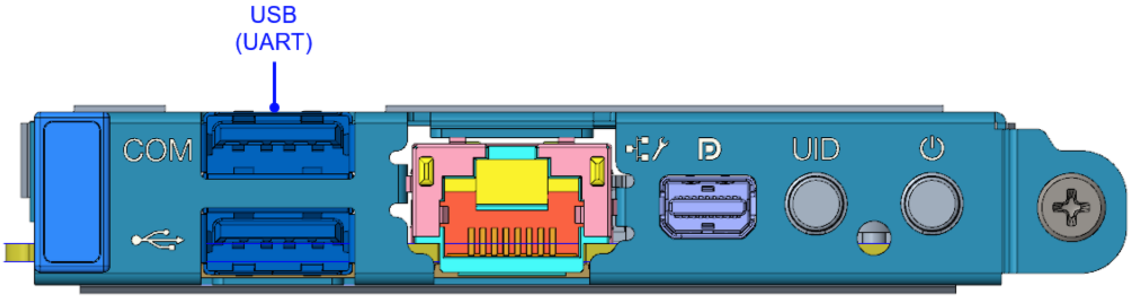


Figure 19 UART Connector on I/O Panel

9.9 Externally Accessible Buttons and LEDs

The table below shows the mapping of the connection of DC-SCM CPLD GPIOs and BMC GPIOs to the following externally accessible buttons and LEDs:

- HPM Power Button through DC-SCI as defined in section 9.5.12
- Power Button and embedded Power LED on the faceplate
- UID Button and embedded UID LED on the faceplate
- System LED on the faceplate

Function	CPLD GPIO	CPLD Pin	BMC GPIO	BMC Pin
Power button	PL21C	K4	GPIU6	AD16
Power LED	PL30D	P2	N/A	N/A
UID button	PT15A	D6	GPIOZ1	AD10
UID LED	PR20C	J11	N/A	N/A
Function	**-**	**-**	**BMC GPIO**	**BMC Pin**
System LED-Red	-	-	GPIOF1	E22
System LED-Yellow	-	-	GPIOF2	D23
Function	**CPLD GPIO**	**CPLD Pin**	**-**	**-**
HPM Power button	PB21A	M6	-	-

Table 20 Button/LED GPIO Mapping

9.10 TPM

SPI_TPM_x: HPM is the initiator. This enables some hosts to have a dedicated TPM SPI bus. Other hosts utilize a dedicated CS on QSPI. In the latter mode, the other SPI pins are not usable except for alternate functions (i.e. I2C_I3C_1V8*). A more universal DC-SCM may provide the appropriate MUX logic for firmware to steer the bus properly during the HPM discovery phase. Please refer to the SPI block diagram in 9.5.5 for more details.

9.11 Intrusion Detection

FM_INTRUDER_BMC_N is an optional 3.3V DC-SCI 2.0 input (unidirectional) signal from the HPM.

On the HPM, FM_INTRUDER_BMC_N should be pulled up to 3.3V RTC battery and connected to the intruder switch (button). On the DC-SCM side, the signal should be routed to the CHASI# pin on BMC or a latchable circuit that is powered by 3.3V RTC. When implemented per described, the expected operation of the switch is that when the chassis cover is closed, the FM_INTRUDER_BMC_N signal will be high indicating no intrusion event. When the chassis cover is opened, the signal will be low indicating that the intrusion event is triggered. Since the circuit is powered by the 3.3V RTC, when system power is not available, intrusion events can still be detected and logged into SRAM.

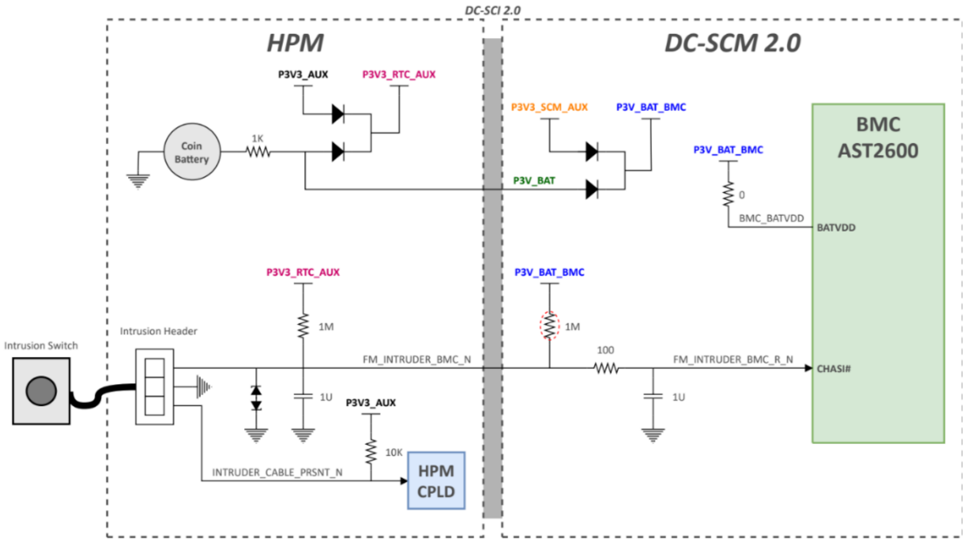


Figure 20 Project Argus Intrusion Detection Block Diagram

10. Rear Side Power, I/O, Expansion Board and Midplane Subsystems

This section is not applicable for this DC-SCM module contribution.

11. Mechanical

11.1 General Overview

Project Argus DC-SCM 2.0 module supports the horizontal External Form Factor design which complies with the OCP DC-SCM Rev2.0 Ver1.0 Base Specification.

- External Form Factor (EFF) – This form factor is intended for use in servers where the DC-SCM is installed in a coplanar fashion at the front/rear of the server with direct interface to the front server bezel or at the rear wall of the server.

Project Argus DC-SCM 2.0 module also supports a removable TPM module that is fixed with a tamper proof screw.

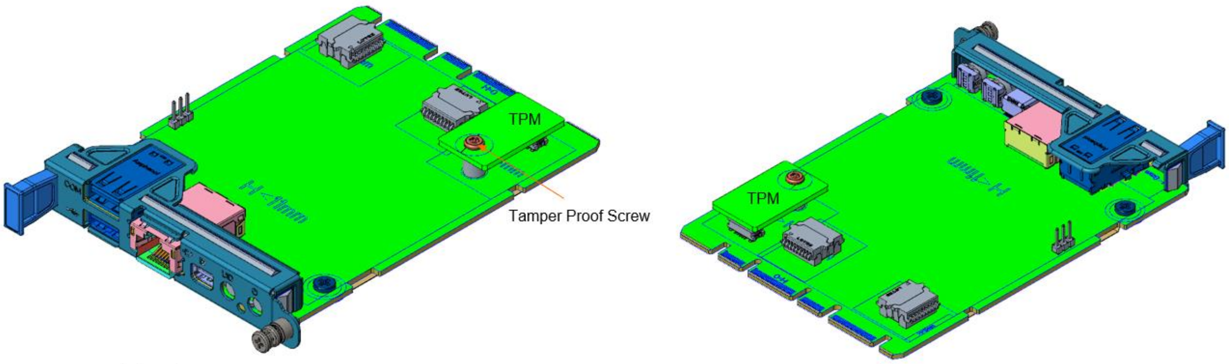


Figure 21 Mechanical Overview

11.2 Board Dimensions and Keep-out Zones

The PCB form factor overall dimensions are shown in the figures below. It has a thickness of 1.57mm. To enable the Internal Lock Mechanism, there are slots on each side to allow the rail features that secure the module in place.

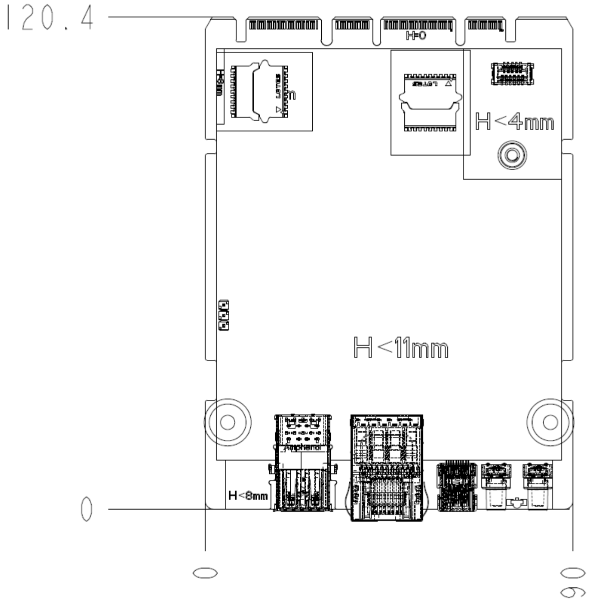


Figure 22 Board Dimensions

The keep-out zones (KOZ) for the top-side, bottom-side, and sides are shown in the figures below.

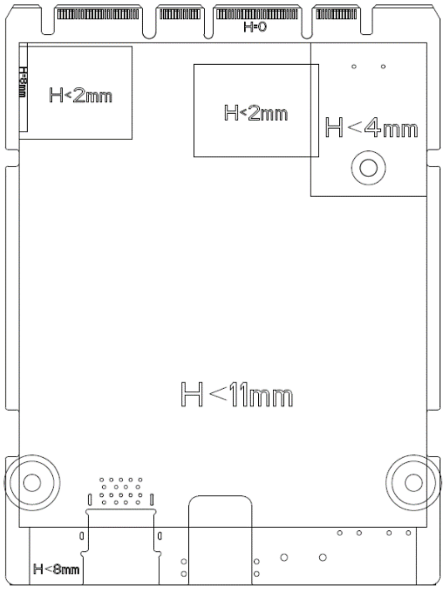


Figure 23 Keep-out Zones – Top-side

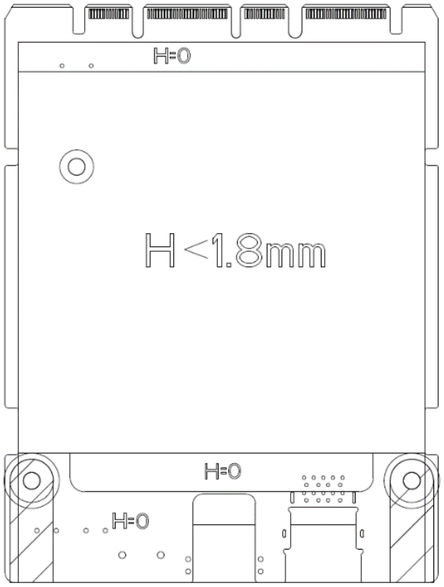


Figure 24 Keep-out Zones – Bottom-side

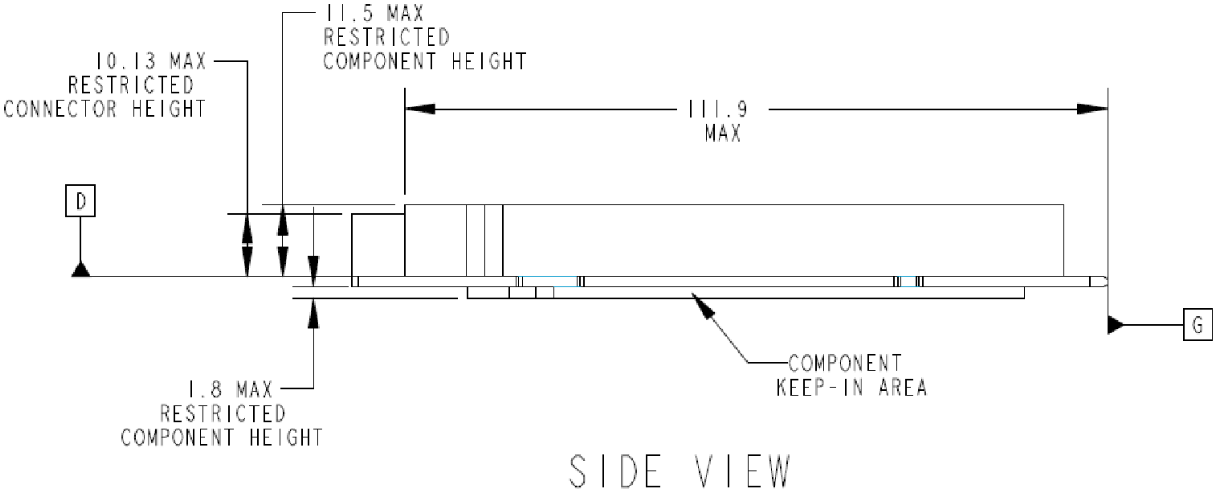


Figure 25 Keep-out Zones – Side

11.3 I/O Faceplate Bracket Subassembly

The I/O faceplate bracket subassembly dimensions are shown in the figure below.

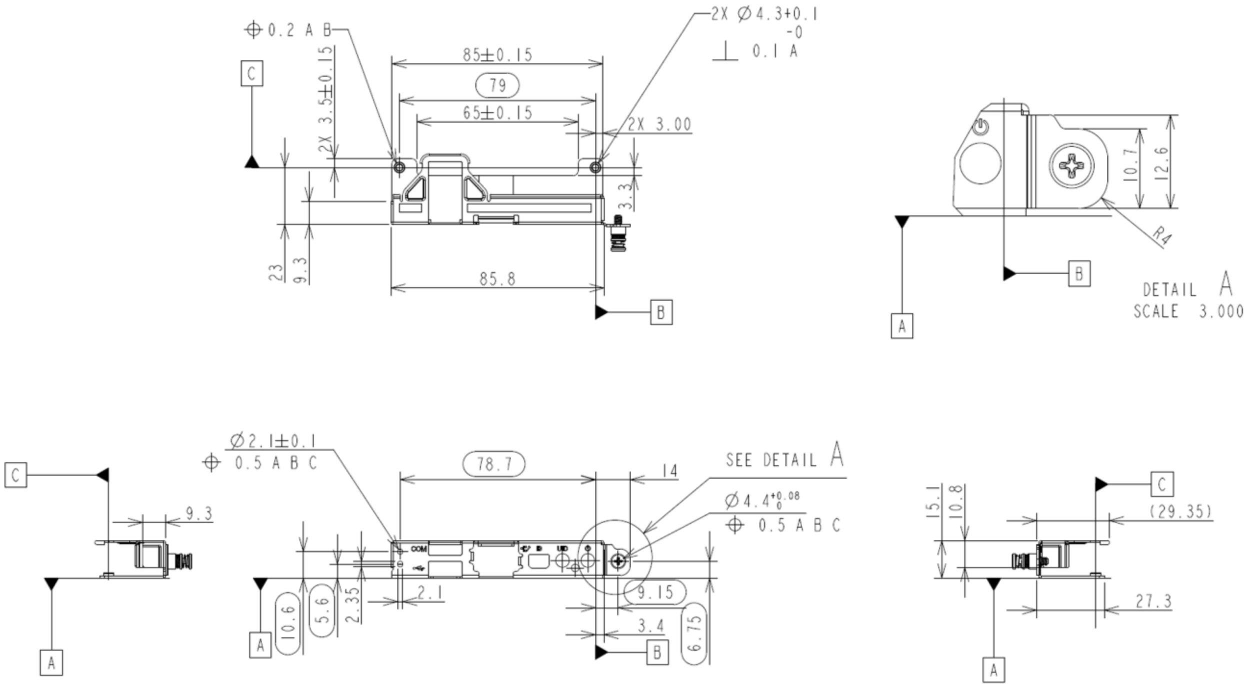


Figure 26 Faceplate Bracket Subassembly

11.4 Module Assembly Overview

The module assembly dimensions are shown in the figure below.

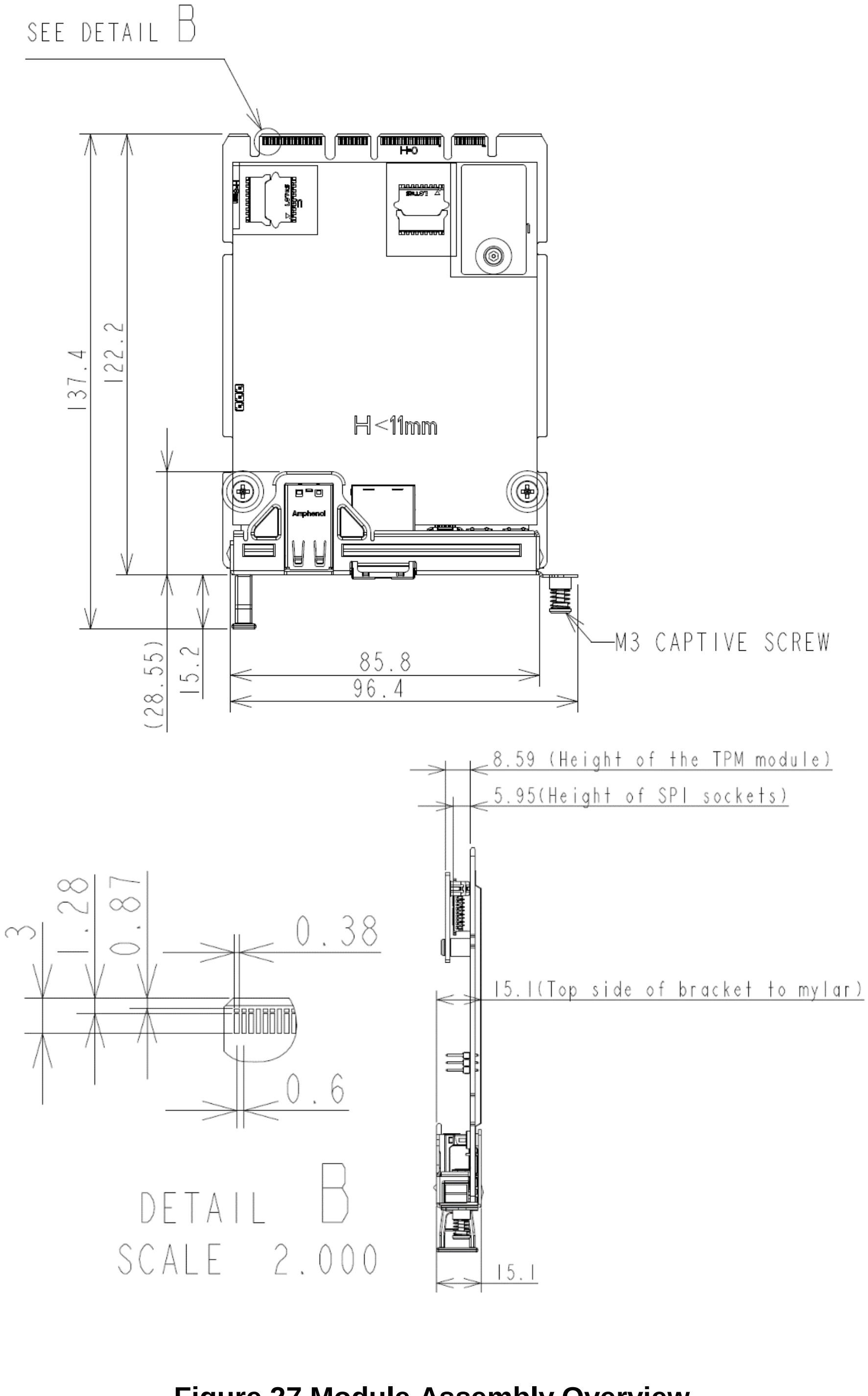
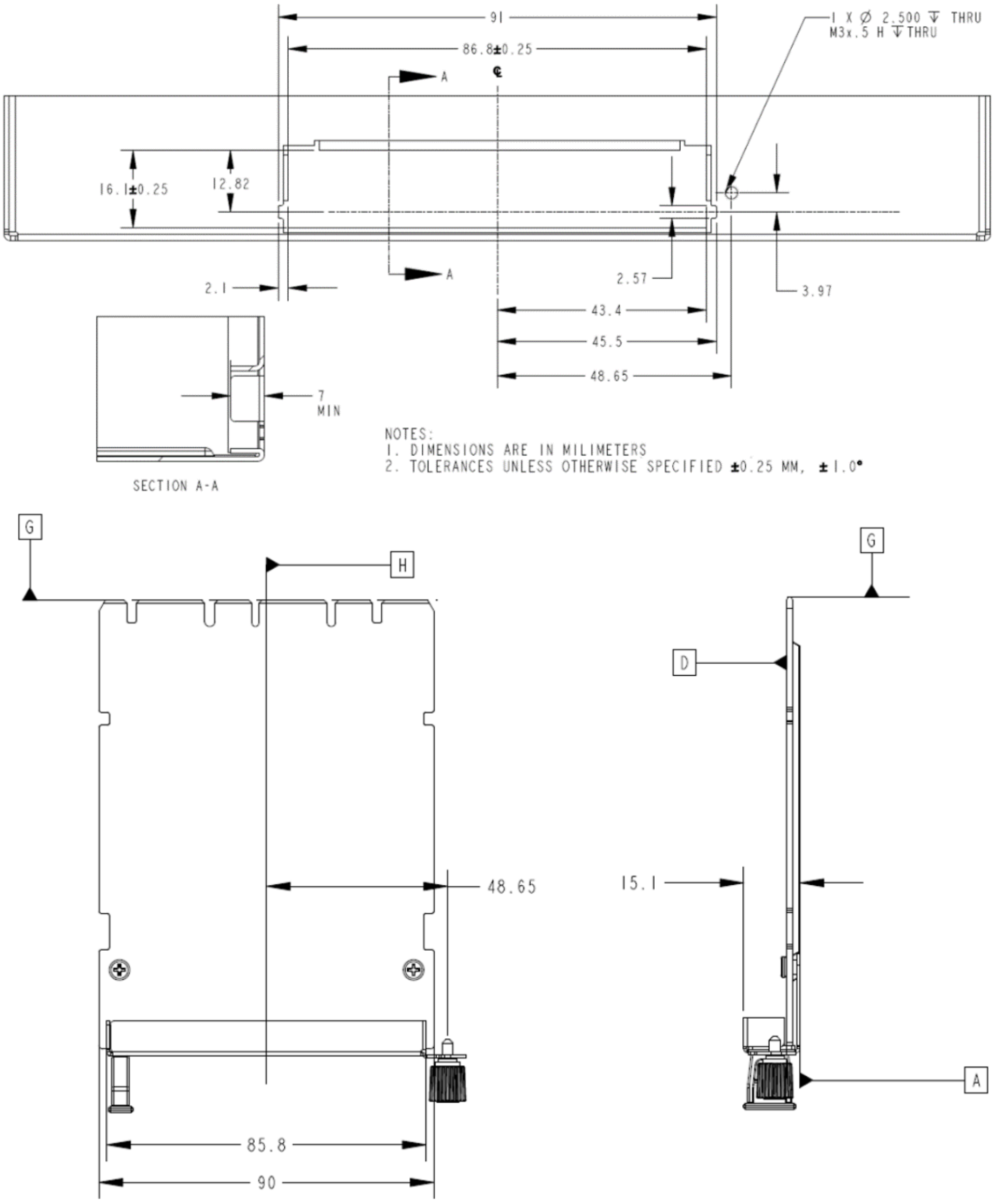


Figure 27 Module Assembly Overview

11.5 Chassis Bay Opening Requirement

Project Argus DC-SCM 2.0 module shall fit within the chassis opening defined in the figure below. Sheet metal flanges on four sides are bent inwards to provide sufficient contact surfaces for EMI solutions providing a conductive path to ground. The height of the chassis cutout is dependent on where the module is positioned relative to the card edge connector on the baseboard.



NOTES:
1. DIMENSIONS ARE IN MILIMETERS
2. TOLERANCES UNLESS OTHERWISE SPECIFIED ±0.25 MM, ±1.0°

Figure 28 Chassis Bay Opening Dimensions

11.6 Front Panel Definition

Project Argus DC-SCM 2.0 front panel includes the following as shown in the figure below.

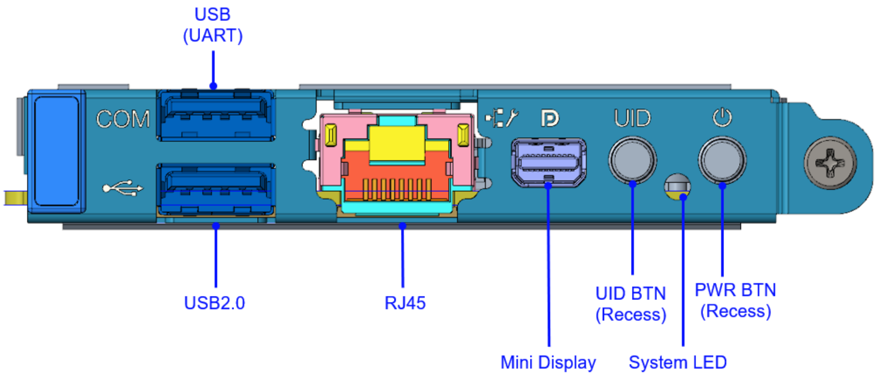


Figure 29 Project Argus Front Panel Definition

11.6.1 Front I/O

The front panel includes the following I/O ports as shown in the figure below.

- Mini Display Port
- RJ45
- USB 2.0
- USB (UART)

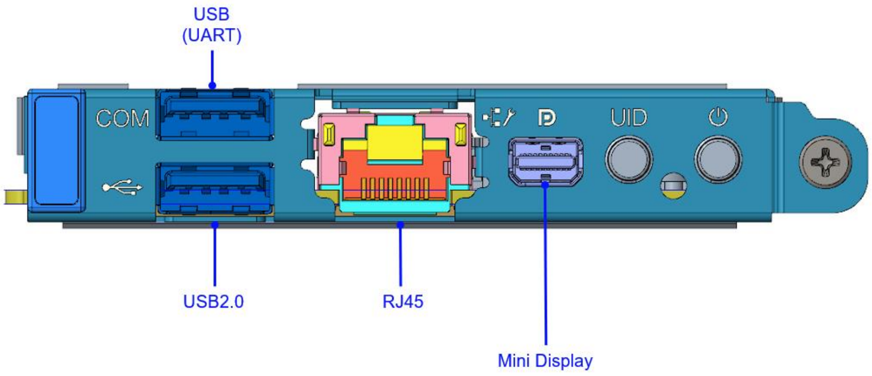


Figure 30 Project Argus Front Panel I/O Ports

11.6.2 Button

The front panel includes the following buttons as shown in the figure below.

- Power Button
- UID Button

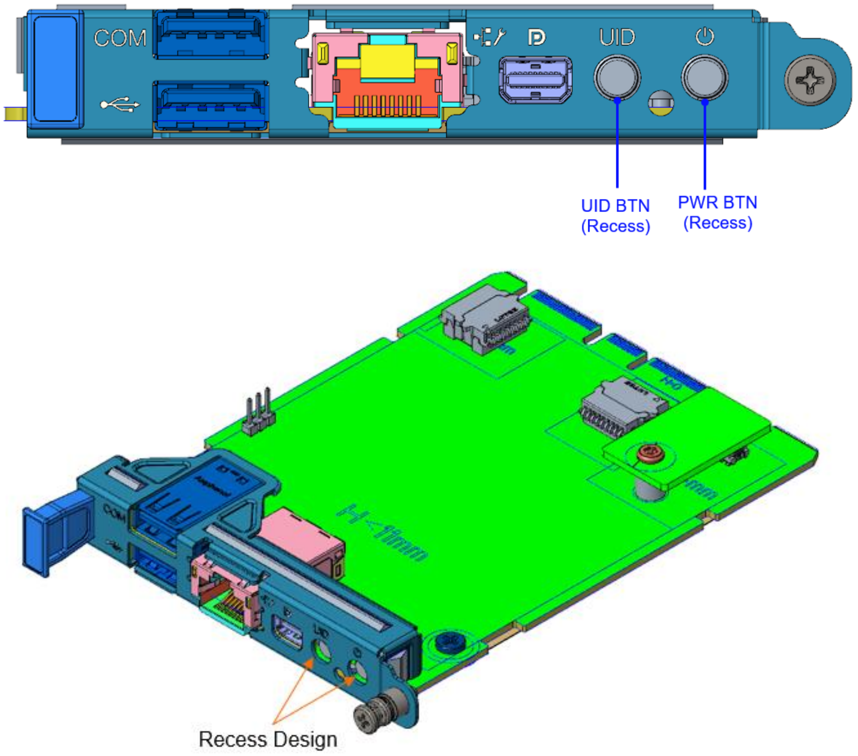


Figure 31 Project Argus Front Panel Buttons

11.6.3 LEDs

The front panel includes the following LEDs as shown in the figure below.

- System LED (Yellow/Red)
- UID LED (Blue - embedded in UID button)
- Power LED (Green - embedded in Power button)

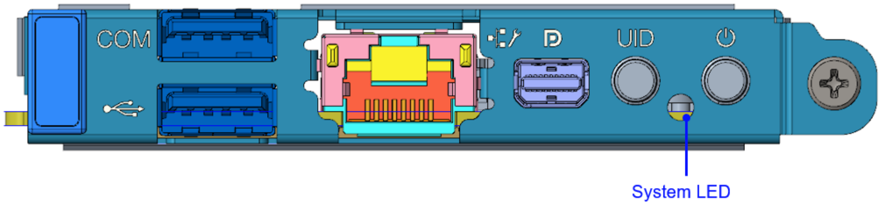


Figure 32 Project Argus Front Panel LED

11.7 Internal Lock Mechanism

Project Argus DC-SCM 2.0 module includes an internal lock mechanism to physically secure the module inside the system enclosure to prevent easy removal of DC-SCM 2.0, either by accident or by intention, from the rear of the chassis without opening the system chassis enclosure to disengage the lock. The internal lock mechanism is implemented using the tray rail as shown in the figure below.

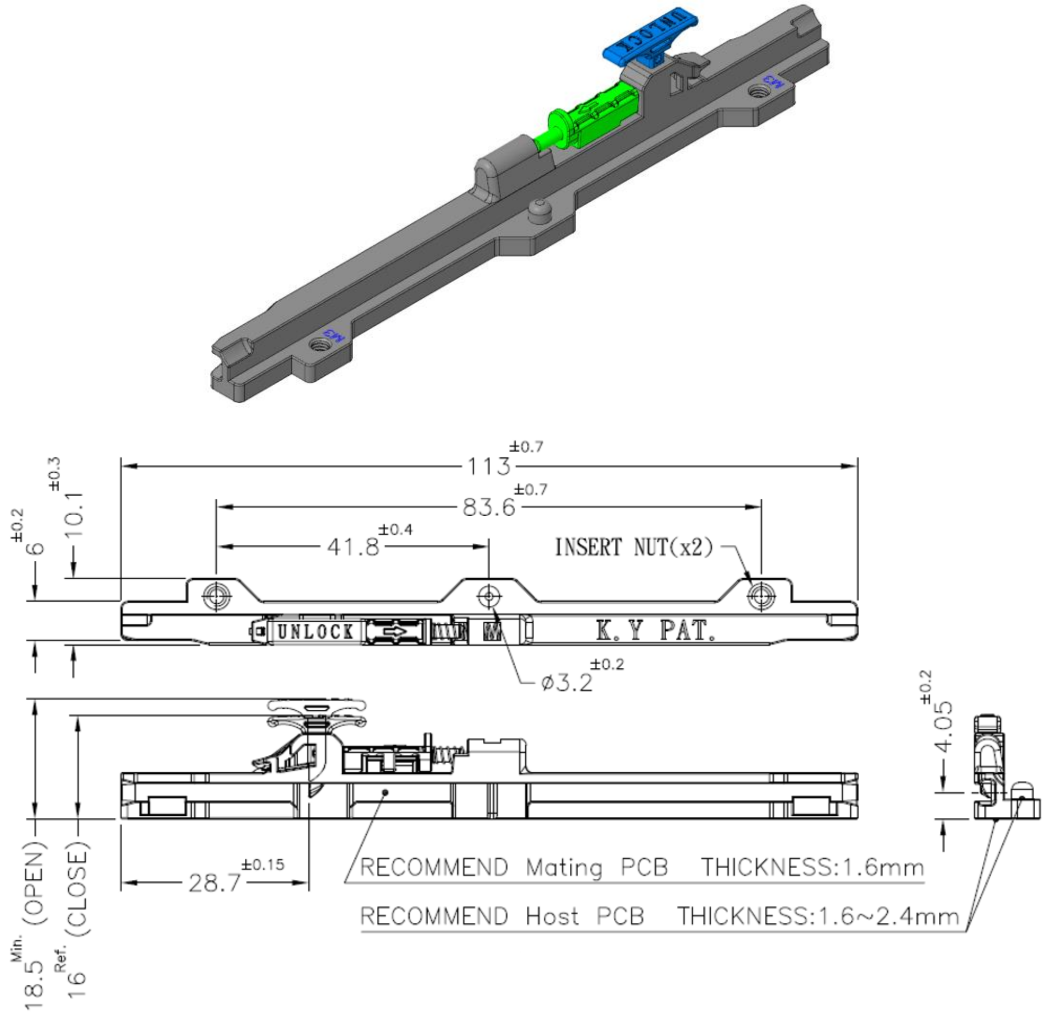


Figure 33 Project Argus Internal Lock Mechanism

The sequence to disassemble the module is shown in the figure below.

1. From the inside of the enclosure, pull up the tab on the rail.
2. From the front side of the module, unfasten the screw on the bracket.

3. Grasp the pullout tab and pull the module removing it from the enclosure.

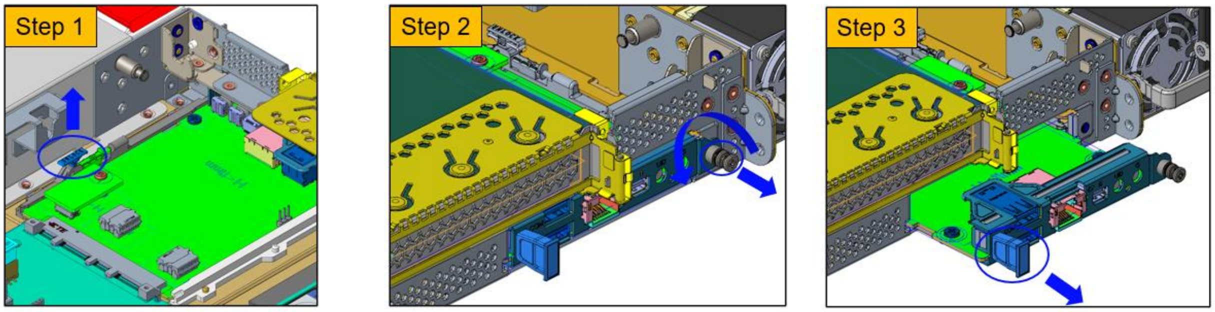


Figure 34 Disassembling the Module from Enclosure

12. Onboard Power System

The power topology for Project Argus DC-SCM 2.0 module is shown in the figure below.

12.1 Power Block Diagram

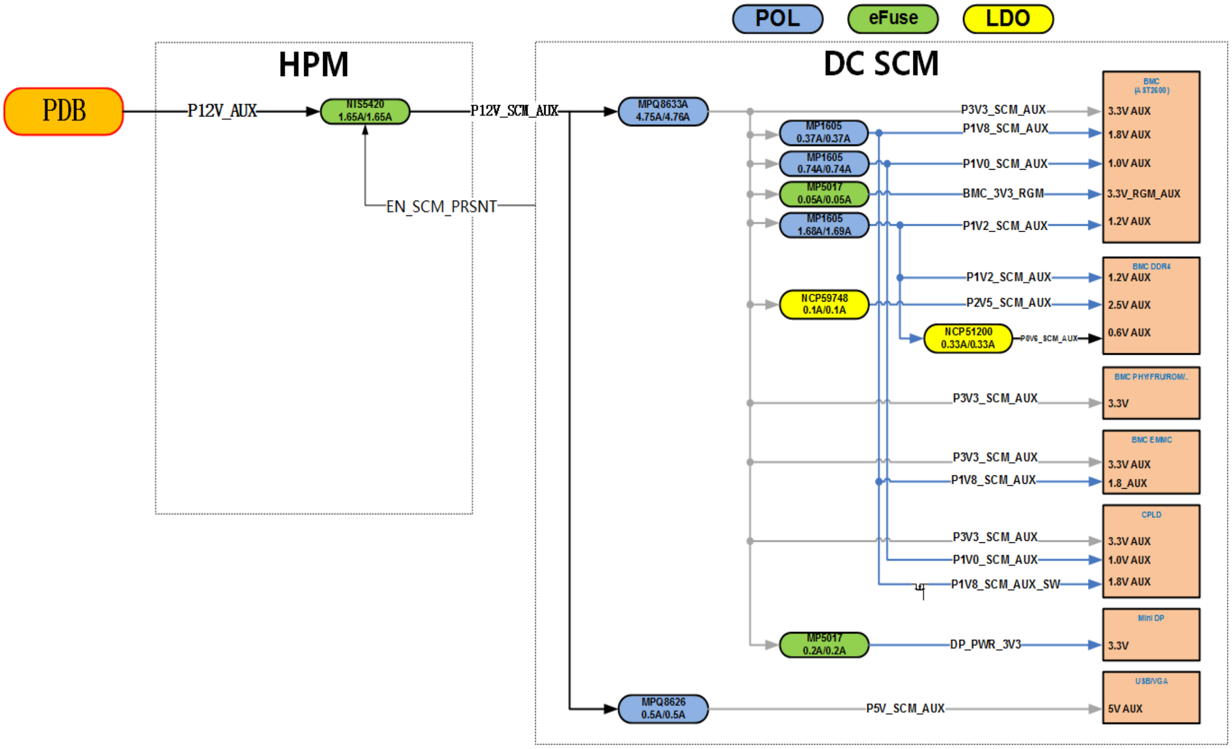


Figure 35 Project Argus Power Delivery Block Diagram

Although the module is not intended to support hot plug or hot removal, an eFuse shall be implemented on the HPM to protect the DC-SCM from any overcurrent events.

12.2 Power Consumption

	Minimum	Nominal	Maximum
Input Voltage	10.8V	12V	13.2V
Input Current*	n/a	n/a	4.4A (1.1A/pin * 4 pins)
Input Power*	n/a	n/a	19.8W

Table 21 Power Consumption

*Input Current is based on 1.1A rating per pin, which includes derating.
*Input Power is based on theoretical calculations

13. Environmental Regulations/Environmental Requirements

Since Project Argus DC-SCM 2.0 module is designed to be used exclusively within a system enclosure, the Environmental Regulations and Requirements are not applicable and are assumed to be completed as part of the overall platform qualification.

Nevertheless, this module includes circuitry on external facing ports to ensure compliance with EMC/EMI regulations and EMS immunity.

Targeted Category	Applicable Specification
Immunity (ESD)	EN 55035 2017, and IEC 61000-4-2 2008 for ESD. EN 55024 may alternatively be reported. Required ±4 kV contact discharge and ±8 kV air discharge Note: EN55024 is scheduled to be superseded by EN55035. Project Argus DC-SCM 2.0 implementers are encouraged to test to EN55035 to avoid recertifying their product when EN55024 is withdrawn
REMI (Radiation test)	Radiation testing for ANSI C63.4/CISPR 32. Required -5dB based on Class A regulatory limits
CEMI (conduction test)	Conduction testing for ANSI C63.4/CISPR 32. Required -5dB based on Class A regulatory limits
Immunity	EN 55035 2017, and IEC 61000-4-6 for CS. Required 3 Vrms, Criteria

(Conducted Immunity, CS)	A
Immunity (Electrical Fast Transient, EFT)	EN 55035 2017, and IEC 61000-4-4 for EFT. Required +/-1 kV, Criteria B on Mains and +/-0.5 kV, Criteria B on I/O
Operating Condition	Operating Altitude: Sea level to 5000 feet Operating relative humidity: 8-85%
Environmental	RoHS Directive 2011/65/EU and Amendment (EU) 2015/863. European Commission Regulation Number 1907/2006 concerning the Registration, Evaluation, Authorization and Restriction of Chemicals (REACH).

Table 22 Environmental Regulations

14. Prescribed Materials

Project Argus DC-SCM 2.0 is ROHS compliant and does not contain any of the restricted hazardous substances. Electrical components include inductors, capacitors, and FETs with at least de-rating of 20%.

15. Software Support (recommended)

N/A

16. System Firmware

16.1 BMC Firmware

For ASPEED AST2600 BMC firmware, the code base is leveraged from OpenBMC, which is an open source Linux distribution for management controllers. See below for repository and key feature list.

BMC Chip: ASPEED AST2600
BMC Firmware: OpenBMC, https://github.com/openbmc/openbmc
BMC Feature list:

- Host management: Power, Cooling, LEDs, Inventory, Events, Watchdog
- IPMI 2.0 compliance
- Code update support for BMC/BIOS

- Web-based user interface
- REST interfaces
- D-Bus based interfaces
- SSH based SOL
- Remote KVM
- User management
- Virtual media
- Chassis intrusion detection
- POST code snooping
- Identify multi-platform motherboard by FRU Product Name

16.1.1 Minimum Bootable Device Tree

The minimum bootable Device Tree (DT) shall be selected if the DT for the DC-SCM vendor is not found or if the HPM FRU is unrecognized during firmware initialization. The minimum device tree shall include the device tree source for the BMC (AST2600) i.e. *aspeed-g6.dtsi*. The partially functional mode of the BMC should have the following:

- IPMI functionality
    - Host Power On
    - Host Power Off
    - Host Power Reset
- SOL
- KVM
- Redfish/bmcweb firmware update
- Fans (Running at 80%)

Refer to the attached Minimum Bootable Device Tree Requirements for more details.

16.2 HWRoT Firmware

For ASPEED AST1060 HWRoT firmware, the code base is based on the ASPEED Zephyr project, which is an open source firmware application for ASPEED PFR. See below for repository and key feature list.

HWRoT Chip: ASPEED AST1060
HWRoT Firmware: ASPEED Zephyr SDK, https://github.com/AspeedTech-BMC/aspeed-zephyr-project
HWRoT Feature List:

- Intel PFR 3.0 compliant HWRoT features
- Firmware authentication

- Firmware recovery
- Secure firmware update
- Field updatable HWRoT firmware
- HWRoT firmware recovery
- HWRoT secure boot
- Checkpoint timer
- SPI filtering
- I2C/SMBus filtering
- SMBus mailbox
- Protect in transit
- UEFI authentication when host reset
- BMC firmware authentication when BMC reset

16.2.1 HWRoT Secure Boot Mode

Project Argus DC-SCM 2.0 secure boot uses a mode offered by AST1060 HWRoT that combines ECDSA encrypted firmware signature and separately RSA encrypted SOC keys. Firmware image is AES-256 encrypted using the ODM/OEM platform key. The SHA-384 hash of the encrypted firmware image is then ECDSA-384 encrypted with the ODM/OEM DSS Private Key to produce the firmware signature. The ODM/OEM platform key is separately RSA-4096 encrypted with SOC private key. The encrypted firmware image, firmware signature and encrypted ODM/OEM platform key are stored in the flash device.

The ODM/OEM DSS Public Key (ECDSA) and SOC Public Key (RSA) are programmed into OTP by the manufacturer. The keys are used to extract other keys, measure the firmware, and compared with the firmware signature during the secure boot process.

16.2.2 HWRoT Secure Boot Process

1. Boot image is loaded into SRAM and the secure boot header is read
2. ODM/OEM DSS Public key is read from OTP
3. Signature is decrypted using ODM/OEM DSS key and resulting digest is measured
4. If the digest matches the image signature, proceed with boot.

16.2.3 BMC Secure Boot Process

1. The HWRoT will validate the signature of the primary BMC firmware.
2. Failure to validate the primary BMC firmware will fallback to the fallback firmware.
3. Failure to validate the fallback firmware will result in a failure to boot the BMC firmware.
4. Upon successfully validating either the primary or fallback image, the image will be loaded and the BMC reset pin (BMC_PFR_SRST_N) will be released by the HWRoT.

16.2.4 UEFI Secure Boot Process

1. The HWRoT will validate the signature of the primary UEFI firmware.
2. Failure to validate the primary UEFI firmware will fallback to the fallback firmware.
3. Failure to validate the fallback firmware will result in a failure to boot the UEFI firmware.
4. Upon successfully validating either the primary or fallback image, the image will be loaded and the HPM reset pin (PFR_HPM_STBY_RST_N) will be released by the HWRoT.

16.3 DC-SCM CPLD firmware

DC-SCM CPLD IP and binary are provided by Lattice Semiconductor. See below for links and key features:

DC-SCM CPLD: Lattice MachXO3D
DC-SCM IP and binary: LTPI-XO3D-UT, https://www.latticesemi.com/en/Products/DesignSoftwareAndIP/IntellectualProperty/IPCore/IPCores05/DC-SCM-LVDS-Tunneling-Protocol-and-Interface-IP-Core
DC-SCM CPLD feature list:

- Compliant with OCP DC-SCM 2.0 LVDS Tunneling Protocol & Interface Specification
- Supports Link initialization, discovery, and negotiation
- Supports Multi-channel Serial Interface and LVDS
- Supports up to five channels aggregation/disaggregation in total
- Supports GPIO aggregation

17. Hardware Management

- Project Argus DC-SCM 2.0 module includes a dedicated RJ45 with 1GbE port for BMC OOB manageability via embedded PHY controller.
- The BMC chip ASPEED AST2600 has 1GB DRAM and 128MB flash for firmware storage.
- Firmware for BMC, BIOS, and CPLD can be online updated.
- Supports monitoring of 12V AUX input and other voltage rails including 5.0V_AUX, 3.3V_AUX and RTC battery voltage.

The following are LEDs used for diagnostic and debug:

- BMC heartbeat LED
- CPLD heartbeat LED
- System health LED

18. Security (only for Platform Boards and Systems)

N/A

19. Interoperability

19.1 HPM FRU Requirements

This table defines the requirement for a MultiRecord Area record on the HPM FRU. This record is for the DC-SCM to read to proceed with the appropriate actions such as the updating of the HPM FPGA or BMC firmware. The table below complies with the OCP DC-SCM Rev2.0 Ver1.0 Base Specification.

Offset	field length	field	Value	
0	1	Record Type ID	0xC1	
1	1	7:7 - End of list 6:4 - Reserved, write as 000b 3:0 - Record Format version		
2	1	Record Length		
3	1	Record Checksum (zero checksum)		
4	1	Header Checksum (zero checksum)		
5	3	Manufacture ID	0x7F 0xA6 0x00	OCP INIA assigned ID 0x00A67F (LSB first)
8	1	OCP DC-SCM 2.0 FRU OEM Record Version	0x00 - Reserved 0x01 - OCP DC-SCM 2.0 card FRU record released with version 1.0	
9	2	DC-SCM Revision 15:8 Major number 7:0 Minor number	0x02 0x00	Revision 2.0
11	1	DC-SCM version 7:4 Major number 3:0 Minor number	0x1 0x0	Version 1.0
12	2	LTPI Revision 15:8 - Major number	0x1 0x0	Version 1.0

		7:0 - Minor number		
14	1	LTPI Version 7:4 - Major number 3:0 - Minor number	0x1 0x0	Version 1.0
15	1	DC-SCM type	0x00 - not any defined type 0x01 - 0xFF Reserved	
16	16	Reserved	Reserved set to 0xFF	
31	32	OEM		Board ID, type, etc.

Table 23 HPM FRU Requirements

20. References

- Open Compute Project. DC-SCM Subgroup. https://www.opencompute.org/projects/dc-scmsub-project
- Open Compute Project. Datacenter Secure Control Module Specification (DC-SCM) Revision 2.0, Version 1.0, July 27th, 2022
- Open Compute Project, Hardware Secure Boot Rev 1.0, Nov 9th, 2020
- PCI-SIG®. PCI Express® Base Specification, Revision 5.0, May 28th, 2019
- PCI-SIG®. PCI Express® Card Electromechanical Specification, Revision 4.0, September 2nd, 2019
- SMBus Management Interface Forum. System Management Bus (SMBus) Specification. Version 3.2, Jan 12th, 2022
- Management Interface Forum, Inc, Version 2.0, August 3rd, 2000
- USB Implementers Forum. Universal Serial Bus Specification, Revision 2.0, April 27th, 2000
- DMTF Standard. DSP0222, Network Controller Sideband Interface (NC-SI) Specification, Version 1.0.0, July 21st, 2009
- Distributed Management Task Force (DMTF), Rev 1.2.0b, August 4th, 2020.
- MIPI alliance Specification for I3C BasicSM, Version 1.1.1, July 2021
- DC-SCM 2.0 LVDS Tunneling Protocol and Interface (LTPI) Specification Revision 1.0, Version 1.0, July 27th, 2022
- ASPEED Technology Inc, AST2600 Integrated Remote Management Processor A3 datasheet, Version 1.3, September 29th, 2022
- ASPEED Technology Inc, AST2600 Application Design Guide, Version 1.00, October 22nd, 2022
- ASPEED Technology Inc, AST1060 PFR processor A2 datasheet, Version 1.2, January 3rd, 2023
- ASPEED Technology Inc, AST1060 Secure Boot User Guide, Version 6.3, October 26th, 2022
- ASPEED Technology Inc, AST1060 Hardware Design Guide, Version 0.6, May 5th, 2023
- National Institutes of Standards and Technology (NIST) Special Publication 800-193: Platform Firmware Resiliency Guidelines, May 2018
- Lattice Semiconductor, DC-SCM LVDS Tunneling Protocol and Interface IP Core - User Guide, Version 1.4, February 3rd, 2023

Appendix A - Checklist for IC approval of this Specification (to be completed by contributor(s) of this Spec)

Complete all the checklist items in the table with links to the section where it is described in this spec or an external document.

Item	Status or Details	Link to detailed explanation
Is this contribution entered into the OCP Contribution Portal?	Yes	If no, please state reason.
Was it approved in the OCP Contribution Portal?	Yes	If no, please state reason.
Is there a Supplier(s) that is building a product based on this Spec? (Supplier must be an OCP Solution Provider)	Yes	Lenovo
Will Supplier(s) have the product available for GENERAL AVAILABILITY within 120 days?	No	The module will be integrated into a platform system which will only become generally available in 400 days (end of Q2 2024).