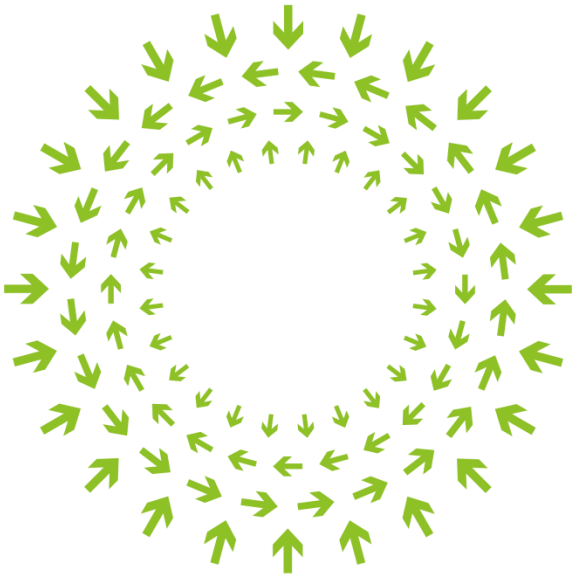


OPEN
Compute Project

Datacenter Secure Control Module Specification

Authors:
Priya Raghu, Senior Hardware Engineer, Microsoft
Mark A. Shaw, Principal Hardware Engineering Manager, Microsoft
Prakash Chauhan, Server Architect, Google
Siamak Tavallaei, Chief Systems Architect, Google
Mike Branch, Server Architect, Google
Mason Possing, Hardware Engineer, Microsoft

Revision History

Version	Date	Notes
0.8	Nov 9th 2020	Initial public review.
0.95	Dec 2nd 2020	Feedback Implemented
1.0	March 11th 2021	Removed ESPI_CS1_N and replaced with RSVD3, Table 22:SPARE[0:1] desc, Fig 22: Updated to initiator/Responder, Table 27: I3C pull-up updated to STBY/MAIN, Sec 6: Platform interop wording edit, Sec 2.2.3- Typo(FFF> HFF), Fig 3,4,5,6 updated, Table 3 updated

Contributions to this Specification are made under the terms and conditions set forth in Open Web Foundation Contributor License Agreement ("OWF CLA 1.0") ("Contribution License") by:

Microsoft Corporation,

Google LLC

Usage of this Specification is governed by the terms and conditions set forth in the Open Web Foundation Final Specification Agreement ("OWFa 1.0").

Note: The following clarifications, which distinguish technology licensed in the Contribution License and/or Specification License from those technologies merely referenced (but not licensed), were accepted by the Incubation Committee of the OCP:

INTELLIGENT PLATFORM MANAGEMENT INTERFACE (IPMI)

I2C TRADEMARK OF PHILLIPS SEMICONDUCTOR

I3C TRADEMARK OF MIPI ALLIANCE, INC

USB TRADEMARK OF USB IMPLEMENTORS FORUM, INC

PCIE TRADEMARK OF PCI-SIG

ESPI TRADEMARK OF INTEL CORP

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.

Acknowledgement

With the hope of making this specification useful for the entire OCP community, we acknowledge and appreciate the contributions, review, and feedback of over 150 individuals from 28 different companies.

References

- Open Compute Project. DC-SCM Subgroup. https://www.opencompute.org/projects/dc-scm-sub-project
- 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. System 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. Distributed Management Task Force (DMTF), Rev 1.2.0b, August 4th, 2020.
- MIPI alliance Specification for I3C Basic^{SM} Version 1.0 – July 19th 2018
- OCP NIC 3.0 Design Specification Version 1.0.9

Trademarks

Table of Contents

1 Overview 5

1.1 DC-SCM Architecture 6

2 Mechanical 7

2.1 Form Factor Options 7

2.2 Horizontal Form Factor 8

2.2.1 Horizontal Form Factor Dimensions 8

2.2.2 Horizontal Form Factor Keep Out Zones 9

2.2.3 Horizontal Form Factor I/O Faceplate 10

2.3 Vertical Form Factor 11

2.3.1 Vertical Form Factor Dimension Outline 11

3 Interface Definition 16

3.1 DC-SCI Card Edge Connector Definition 16

3.1 Gold Finger Plating Requirements 17

3.2 HPM Connector Definition 17

3.2.1 Straddle Mount Connector 17

3.2.2 Right Angle Connector 19

3.2.3 Vertical Connector 20

3.3 DC-SCI Pin Definition 20

3.4 DC-SCI Signal Descriptions 23

3.4.1 NC-SI 23

3.4.2 eSPI/SSIF 23

3.4.3 Serial GPIO 24

3.4.4 I2C 26

3.4.5 I3C 27

3.4.6 SPI 28

3.4.7 USB 30

3.4.8 PCIe 31

3.4.9 PECI 32

3.4.10 UARTS 32

3.4.11 JTAG 33

3.4.12 Standby Power and Boot Sequence 34

3.4.13 Battery Voltage 37

3.4.14 Miscellaneous Signals 37

4 Electrical Specifications 38

4.1 Input Voltage, Power, and Current 38

4.2 SCM Presence Detection and Power Protection 38

5 Routing Guidelines and Signal Integrity 39

5.1 NC-SI 39
5.1.1 NC-SI Data Timing 41
5.1.2 NC-SI Clock Timing 42
5.2 SGPIO 42
5.3 I2C and I3C 44
5.4 PCIe 44
6 Platform Interoperability 44
7 Acronyms 45

List of Figures

Figure 1. DC-SCM Example Block Diagram 7
Figure 2: Horizontal Form Factor Dimensions 8
Figure 3. HFF Keep Out Zone – Top View 9
Figure 4. HFF Keep Out Zone – Bottom View 10
Figure 5: HFF I/O Faceplate 11
Figure 6: Vertical DC-SCM form factor – Option 1 12
Figure 7: VFF Option 1 Backplate with IO Bracket- Low profile bracket 13
Figure 8: VFF Option 1 Backplate with IO Bracket- Full height bracket 14
Figure 9: Vertical Form Factor DC-SCM– Option 2 (Top View) 14
Figure 10: VFF Option 2 (Top View) - Form Factor and Mounting Holes 15
Figure 11: VFF Option 2 (Bottom View) – Form Factor and Mounting Holes 15
Figure 12. FFF Card Edge Connector Dimensions – Top Side (“B” Pins) 16
Figure 13. FFF Card Edge Profile Dimensions 17
Figure 14. FFF Card Edge Connector – Detail D 17
Figure 15. Straddle Mount Connector Dimensions (in mm) 18
Figure 16. Straddle Mount Connector 0mm Offset for 0.062”, 0.093”, and 0.105” HPM PCB 19
Figure 17. Straddle Mount Connector -0.3mm Offset for 0.076” HPM PCB 19
Figure 18. Right Angle Connector Dimensions (in mm) 19
Figure 19. Right Angle Connector Offset 20
Figure 20. Vertical Connector Dimensions (in mm) 20
Figure 21. ESPI Example Block Diagram 24
Figure 22: SGPIO Example Block Diagram 26
Figure 23: I2C Example Block Diagram 27
Figure 24: An Example I3C SPD DDR5 Block Diagram 28
Figure 25: SPI Example Block Diagram 30
Figure 26: USB Block Diagram 31
Figure 27: UART Example Block Diagram 33
Figure 28: JTAG Example Block Diagram 34
Figure 29: DC-SCM STBY Sequencing Signals Block Diagram 35
Figure 30: Power and Boot Sequence Diagram 36
Figure 31: DC-SCM Presence Detection and Power Protection 39
Figure 32: NC-SI Clock and Data Path Timing Delay Topology 40
Figure 33: SGPIO Data Input Timing 42

List of Tables

Table 1. Straddle Mount Connector PCB Thicknesses 18
Table 2. Straddle Mount Connector PCB Offsets 18
Table 3: DC-SCI Pinout 21
Table 4: NC-SI Signal Descriptions 23
Table 5: eSPI Signal Descriptions 24
Table 6: SGPIO Signal Descriptions 25
Table 7: I2C Signal Descriptions 26
Table 8: I3C Signal Descriptions 28
Table 9: SPI Signal Descriptions 29
Table 10: USB Signal Descriptions 30
Table 11: PCIe Gen3 Data Signal Description 32
Table 12: PCIe Gen5 Data Signal Description 32
Table 13: PCIe Clock Signal Description 32
Table 14: PECI Signal Descriptions 32
Table 15: UART Signal Descriptions 33
Table 16: JTAG Signal Descriptions 34
Table 17: Power Sequence Signal Descriptions 34
Table 18: Battery Voltage 37
Table 19: RoT IO via DC-SCI 37
Table 20: Debug IO via DC-SCI 37
Table 21: Interrupts via DC-SCI 37
Table 22: Other Miscellaneous IOs via DC-SCI 37
Table 23: Input Power Requirements 38
Table 24: NC-SI Timing Parameters 40
Table 25: NC-SI Board Timing Budget 41
Table 26: SGPIO timing parameters 43
Table 27: Platform Interoperability 45

1 Overview

This specification provides details for the design features needed to create a Datacenter-ready Secure Control Module (DC-SCM) with a standardized Datacenter-ready Secure Control Interface (DC-SCI). It moves common server management, security, and control features from a typical processor motherboard architecture onto a smaller common form factor module. This module contains all the FW states previously housed on a typical processor motherboard. This provides benefits to both the user and developer.

From a Data Center perspective, this enables a common management and security to be deployed across a higher percentage of platforms. It also enables deployment of management and security upgrades on platforms within a generation without redesign of more complex components.

From a Development perspective, this enables a solution provider to remove customer specific solutions from the more complex components (such as motherboards). This enables greater leverage of higher complexity components across platforms.

For the purposes of this specification, to clarify terminology, we introduce the following module definitions:

- HPM – Host Processor Module. This refers to any processing module to be managed by a SCM. In simplest terms, this is similar to today's motherboard with BMC and Security circuitry removed. However, this is not limited to standard processor architecture and can apply to any architecture utilizing management and security features.
- HPM FPGA – Host Processor Module FPGA. This refers to a programmable device on the HPM. Main functions include system power/reset control as well as serializing/de-serializing several IOs between the HPM and BMC.
- DC-SCM – The Datacenter-ready Secure Control Module. The DC-SCM is designed to interface to an HPM to enable a common management and security infrastructure across platforms within a data center.
- DC-SCI – The Datacenter-ready Secure Control Interface refers to the connector interface between the DC-SCM and the HPM.

A typical DC-SCM design enables the design and deployment of Host Processing Module (HPM) complex to become a simpler exercise with increased efficiency for time to market deployment. With a standardized DC-SCI pinout and definition, it can be used as a vehicle to drive common boot, monitoring, control, and remote debug for diverse platforms.

This specification considers three form factors for DC-SCM.

- Horizontal Form Factor – This form factor is intended for use in servers where the DC-SCM is installed in a coplanar fashion, at the front of the server with direct interface to the front server

bezel, or at the rear of the server. When installed at the front, standard front panel interfaces are contained on the DC-SCM and do not require cables.

- Vertical Form Factor – This form factor is intended for use in 2RU or taller servers in which the DC-SCM is installed vertically at the front panel (similar to a PCIe Card). Standard front panel interfaces are contained on the DC-SCM and do not require cables.
- Internal Form Factor – This form factor is intended for use in servers in which the DC-SCM is embedded internally to the server without direct interface to a front server bezel. In this application, external interfaces such as fan control and front panel require cabled interconnects.

The DC-SCI is intended to support all form factors of DC-SCM. However, many of the block diagrams and descriptions contained in this specification are based on the Horizontal Form Factor and Vertical Form Factor solutions and may not demonstrate the cabling requirements of the Internal Form Factor. Later specifications may better address this.

1.1 DC-SCM Architecture

For the purposes of this specification, the DC-SCM architecture is assumed to consist of the following primary elements:

- BMC – The Baseboard Management Controller is a specialized service processor that monitors the physical state of server.
- BMC Flash – One or more (typically two) flash devices used to contain the BMC firmware image.
- BIOS Flash – One or more (typically two) flash devices used to contain the BIOS firmware image.
- DC-SCM CPLD – A programmable logic device that contains the Serial GPIO logic and any required additional application specific logic.
- RoT Security Processor – An optional security processor responsible for attesting the BMC, BIOS and/or other firmware images on the system.
- TPM – Trusted Platform Module – A dedicated microcontroller designed to secure hardware through integrated cryptographic keys.

An example block diagram demonstrating the typical architectural building blocks of a DC-SCM is shown in Figure 1.

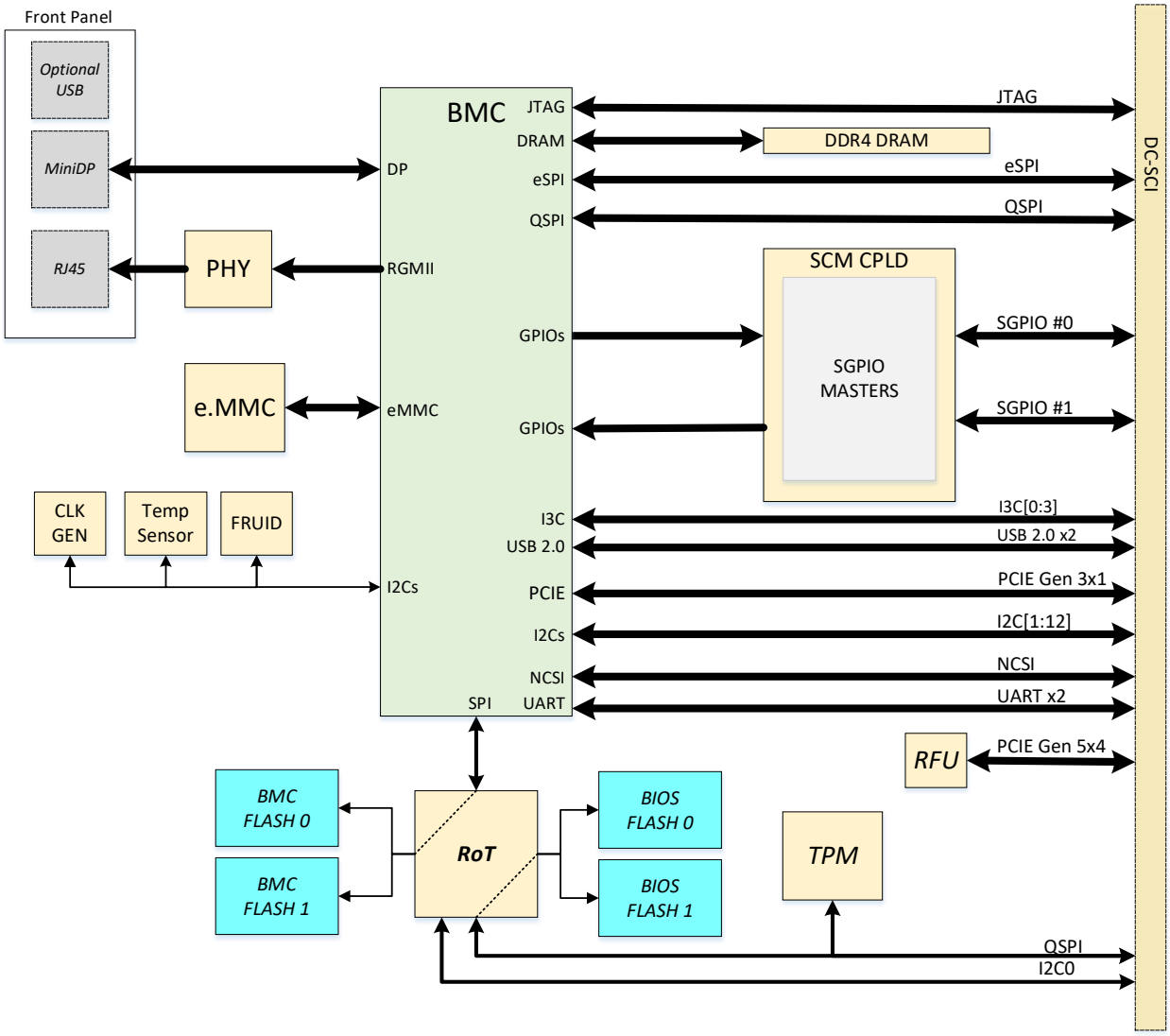


Figure 1. DC-SCM Example Block Diagram

2 Mechanical

2.1 Form Factor Options

The DC-SCM provides three form factor options:

- Horizontal Form Factor (HFF)
- Vertical Form Factor (VFF)
- Internal Form Factor (IFF)- To be updated in a future revision of the spec.

Each form factor supports an edge card connector interface to an HPM. The connector is defined to be an SFF-TA-1002 compliant 4C+ connector. The 4C+ connector is a 4C compliant connector with an additional 28-pin "OCP bay" defined in the OCP NIC 3.0 specification.

The front plate drawings shown for the various options are examples and can be customized for individual use cases.

2.2 Horizontal Form Factor

The Horizontal Form Factor (HFF) is similar to the OCP NIC 3.0 form factor with alterations to the connector interface and to the physical size in order to accommodate typical DC-SCM circuit requirements and ensure mechanical incompatibility between DC-SCM and OCP NIC. The DC-SCM is physically longer and wider ensuring that the DC-SCM cannot mate to an OCP NIC slot and an OCP NIC cannot mate to a DC-SCM slot.

2.2.1 Horizontal Form Factor Dimensions

The Horizontal DC-SCM form factor dimensions are shown in Figure 2.

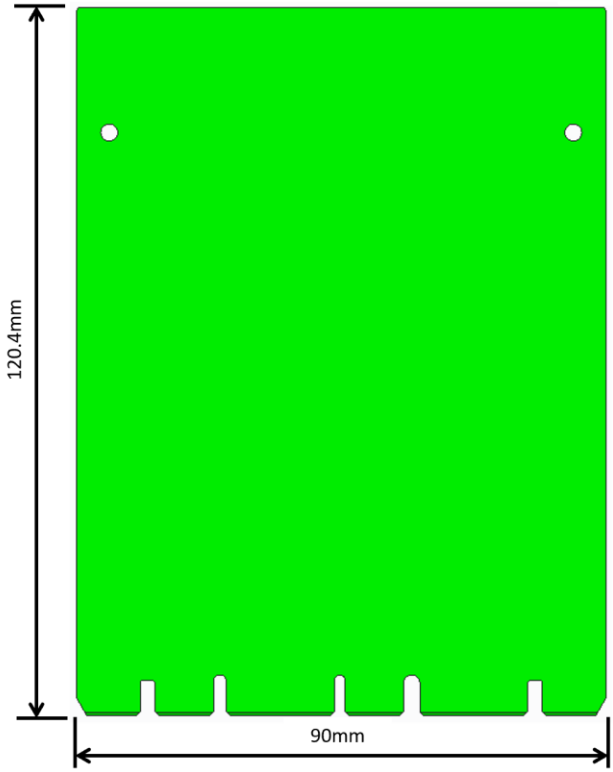


Figure 2: Horizontal Form Factor Dimensions

2.2.2 Horizontal Form Factor Keep Out Zones

The topside “keep-out” zones are shown in Figure 3. The bottom-side “keep-out” zones are shown in Figure 4.

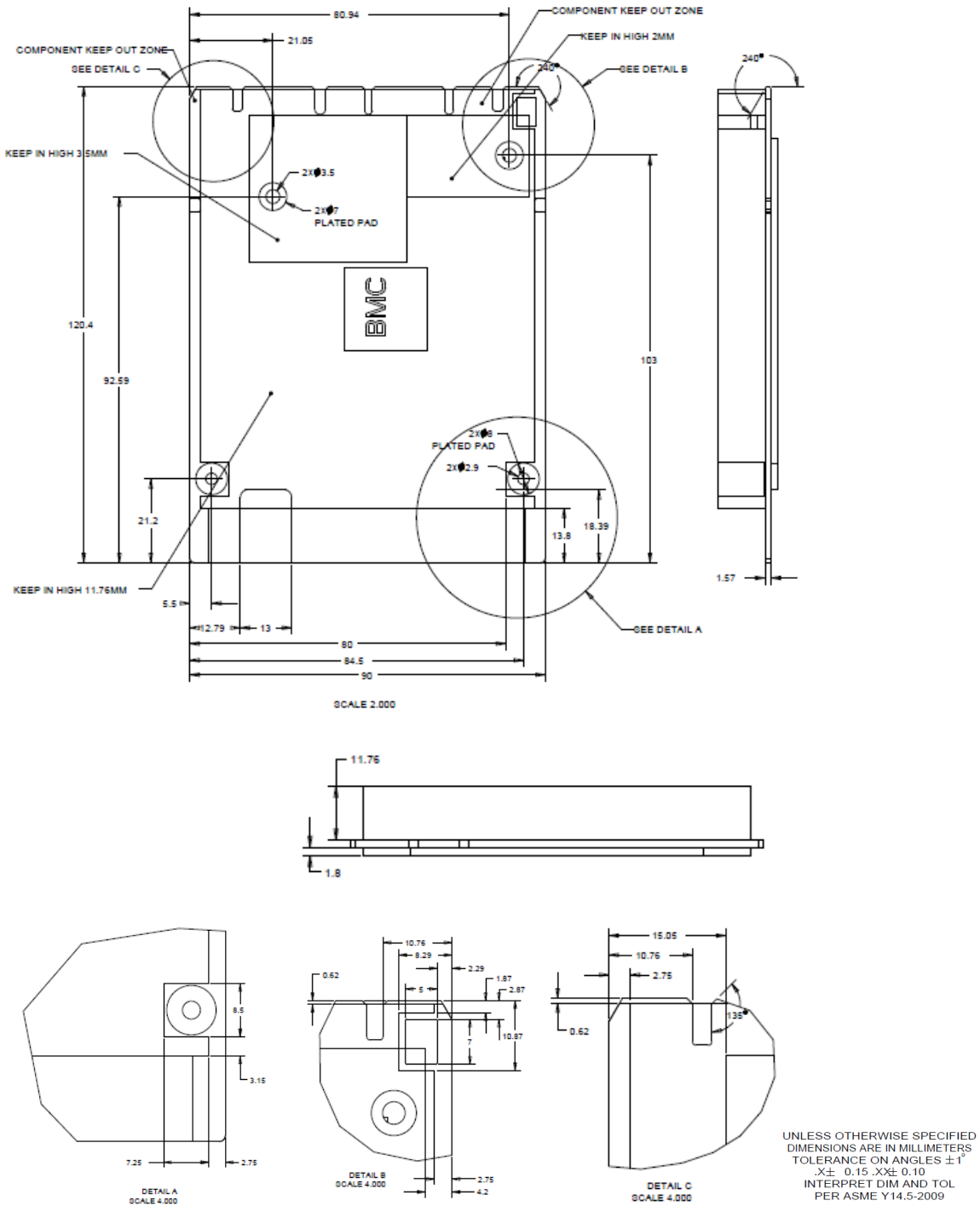


Figure 3. HFF Keep Out Zone – Top View

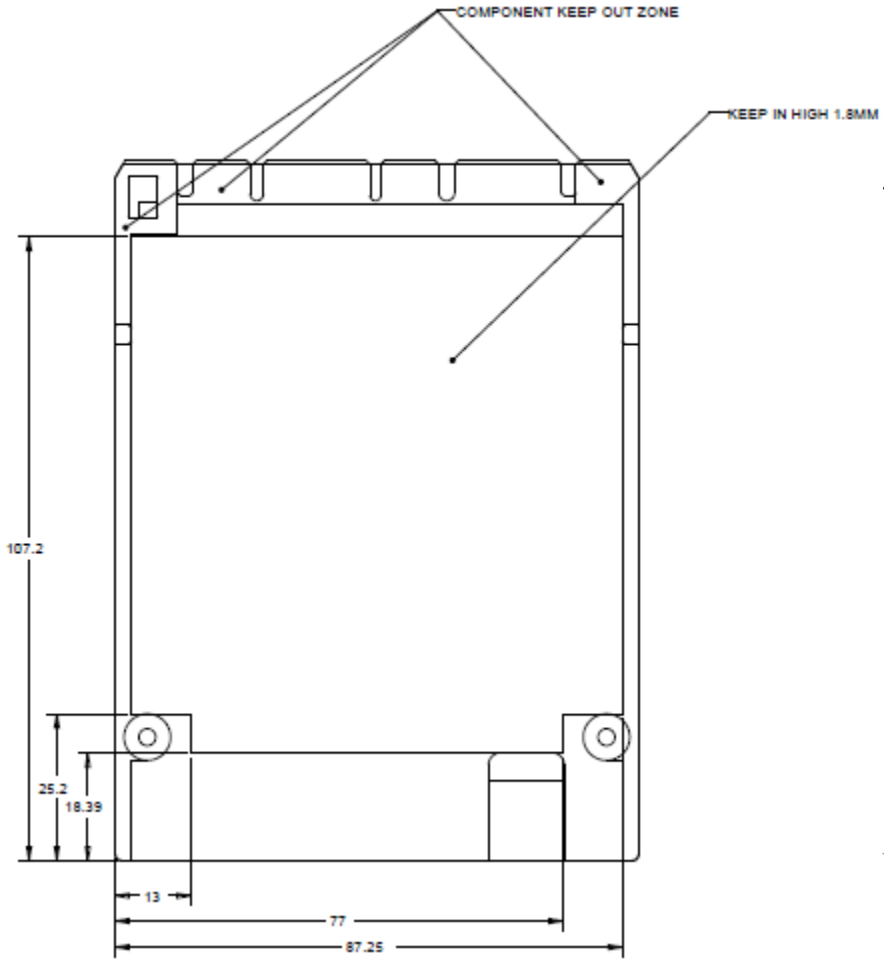


Figure 4. HFF Keep Out Zone – Bottom View

2.2.3 Horizontal Form Factor I/O Faceplate

The HFF supports a front I/O plate enabling front I/O access and securing the DC-SCM to the chassis. The faceplate dimensions are shown in Figure 5. Note that the face-plate cut outs and perforations shown are examples only and can be customized per system configuration and system airflow requirements.

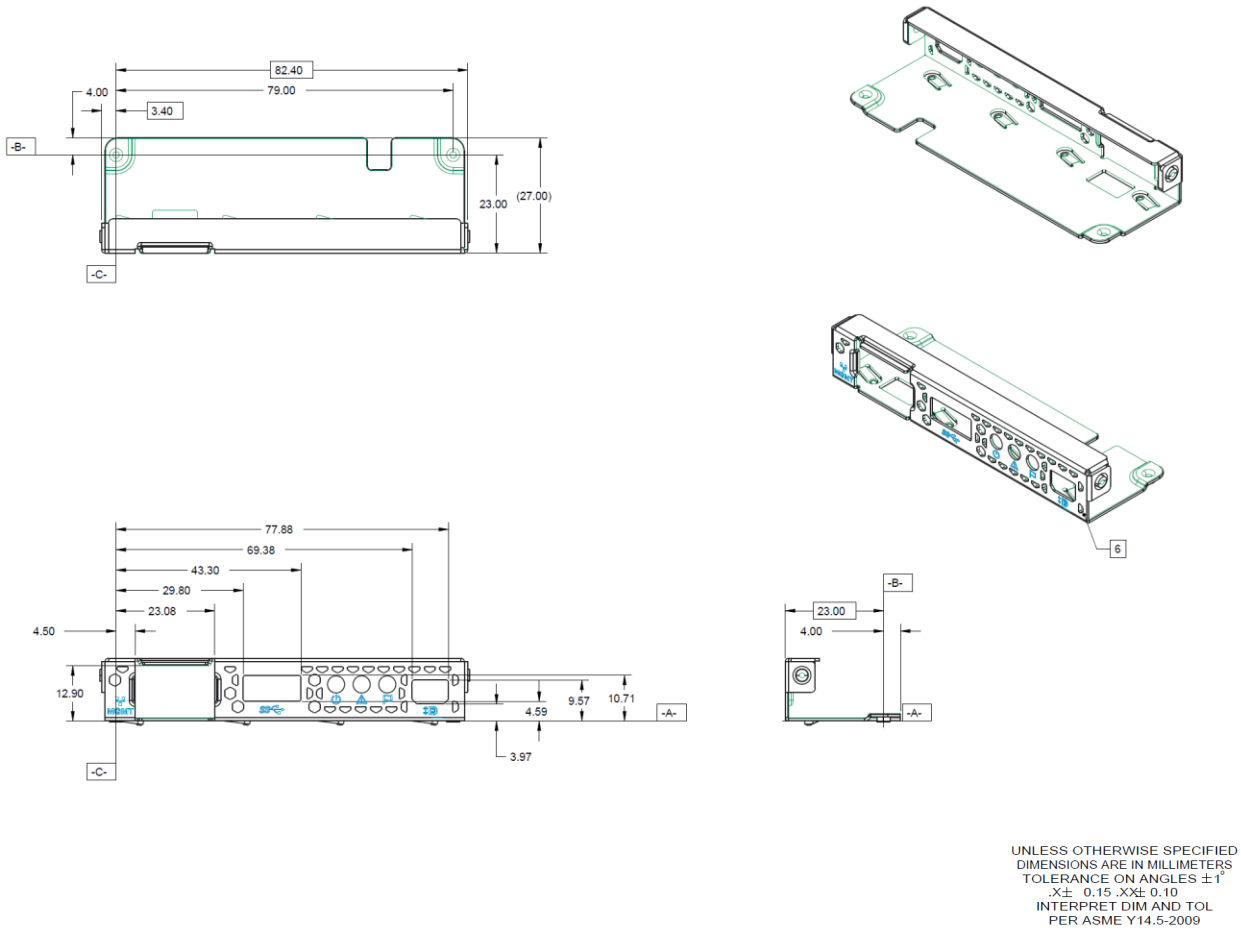


Figure 5: HFF I/O Faceplate

2.3 Vertical Form Factor

2.3.1 Vertical Form Factor Dimension Outline

The DC-SCM specification allows for flexibility in the Vertical Form Factor dimensions based on connector location on the baseboard. This section describes the dimensions of two different vertical form factor options. For VFF option 1, the 4C+ connector is placed closer to the front of the server chassis. For VFF option 2, the 4C+ connector is placed further back in the server chassis.

Figure 6, Figure 7, Figure 8 show the mechanical dimensions of a Vertical Form Factor Option 1 DC-SCM.

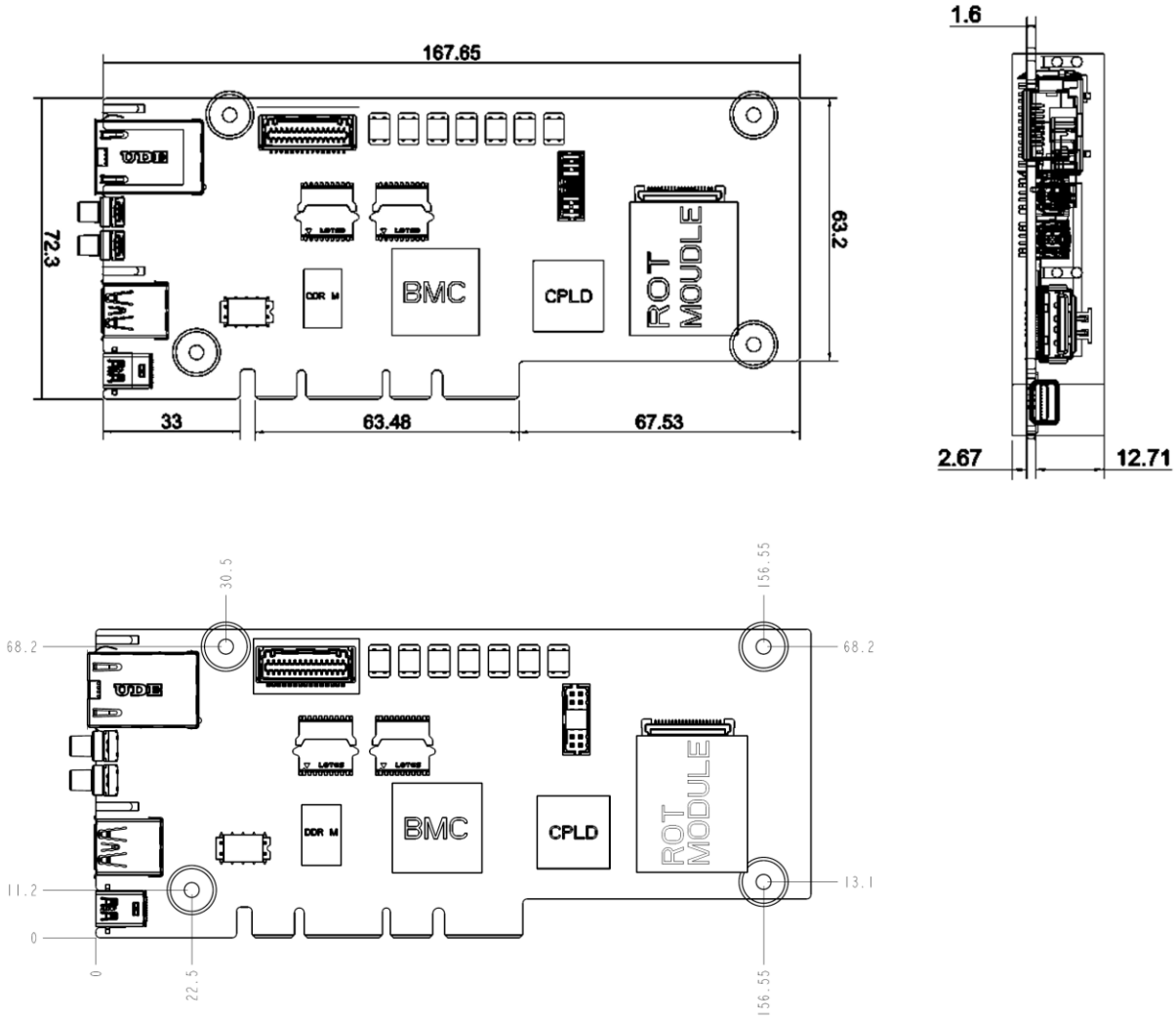
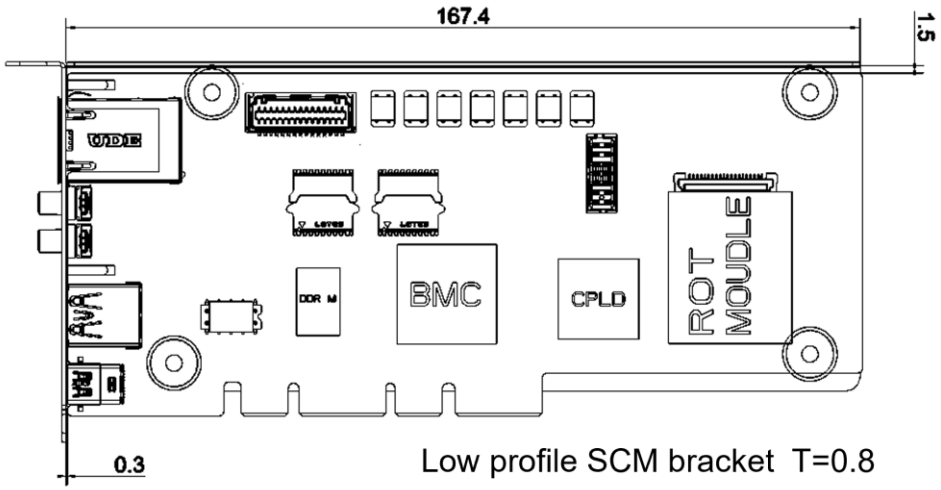


Figure 6: Vertical DC-SCM form factor – Option 1



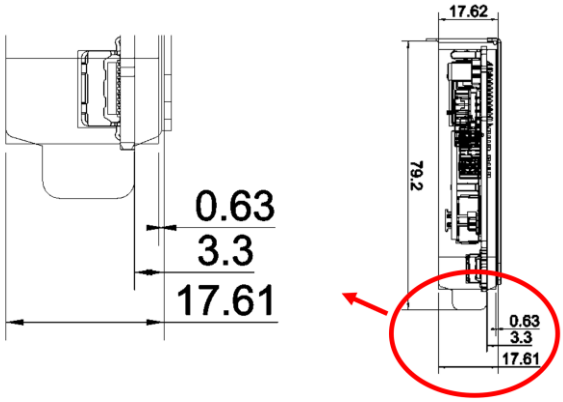
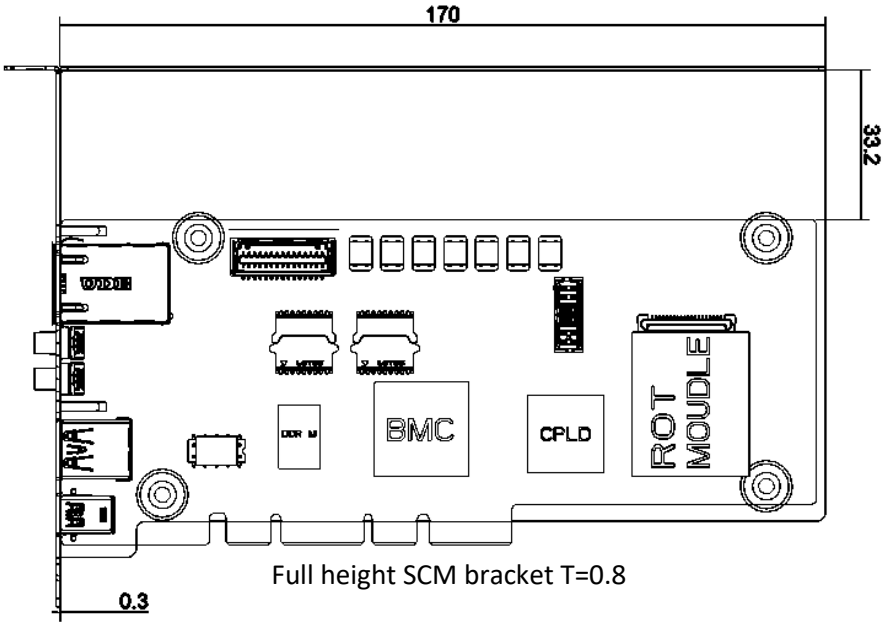


Figure 7: VFF Option 1 Backplate with IO Bracket- Low profile bracket



Full height SCM bracket T=0.8

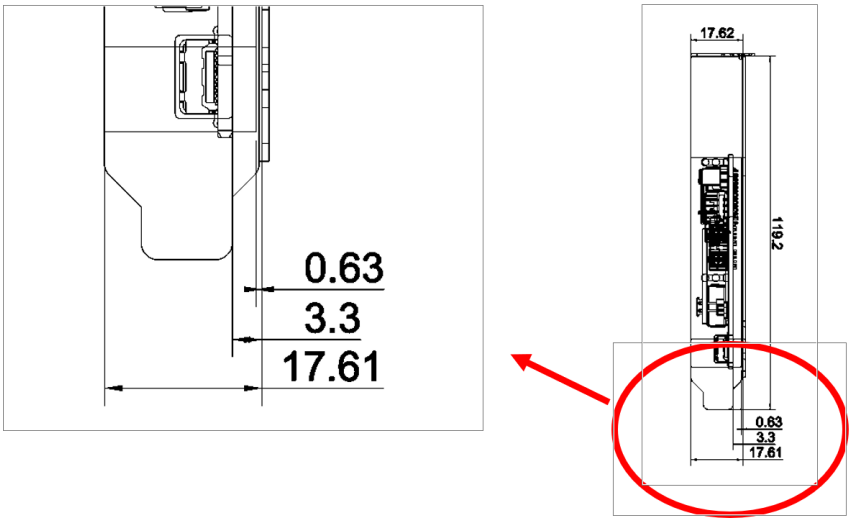


Figure 8: VFF Option 1 Backplate with IO Bracket- Full height bracket

Figure 9, Figure 10 and Figure 11 show the mechanical dimensions of a Vertical Form Factor Option 2 DC-SCM.

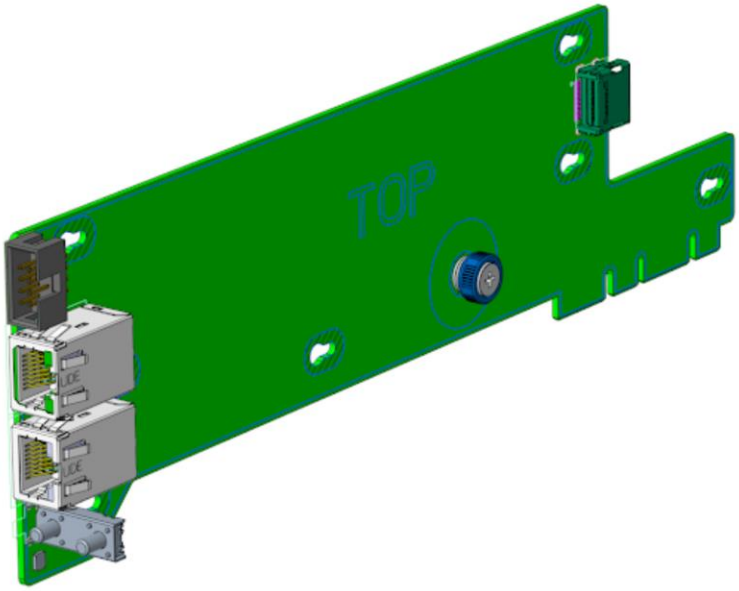


Figure 9: Vertical Form Factor DC-SCM– Option 2 (Top View)

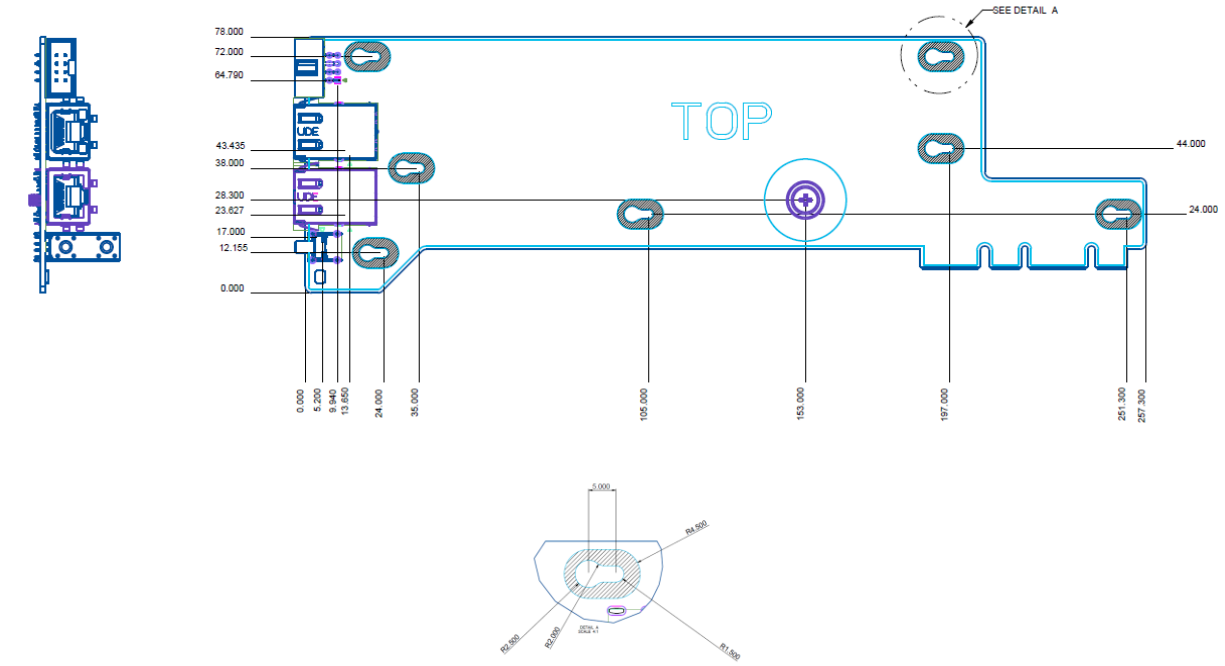


Figure 10: VFF Option 2 (Top View) - Form Factor and Mounting Holes

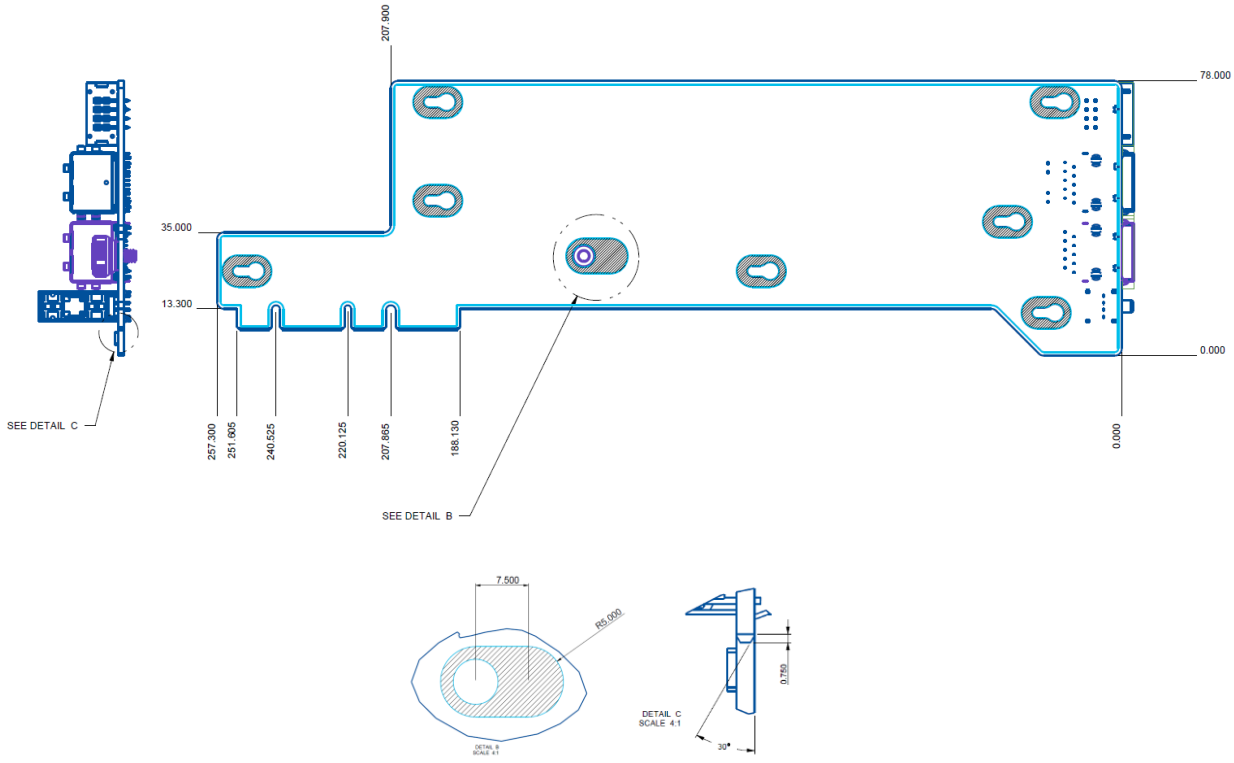


Figure 11: VFF Option 2 (Bottom View) – Form Factor and Mounting Holes

3 Interface Definition

3.1 DC-SCI Card Edge Connector Definition

The DC-SCI card edge connector interface is compliant to the SFF-TA-1002 specification with respect to the 4C+ connector size. Note that while the interface is mechanically compatible with the 4C+ specification, it does not support the SFF-TA-1007 pinout definition and is therefore not electrically compatible with EDSFF and OCP devices. The pinout is defined later in this document. Mechanical details of the edge finger requirements are shown in Figure 12, Figure 13, and Figure 14.

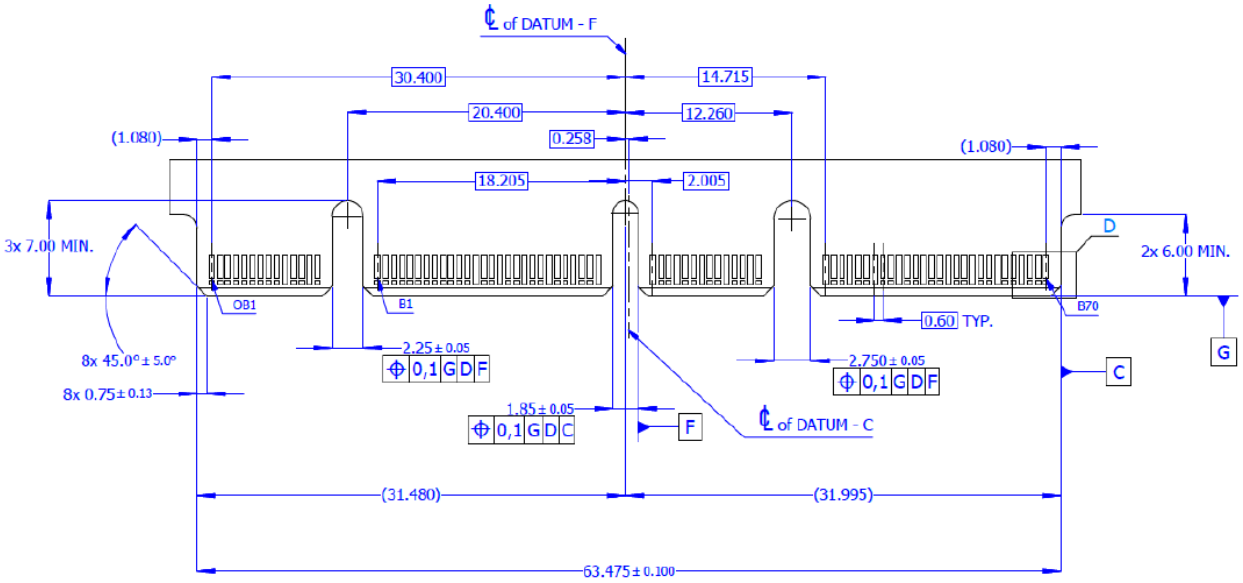


Figure 12. FFF Card Edge Connector Dimensions – Top Side ("B" Pins)

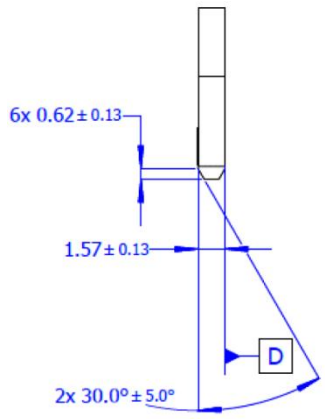


Figure 13. FFF Card Edge Profile Dimensions

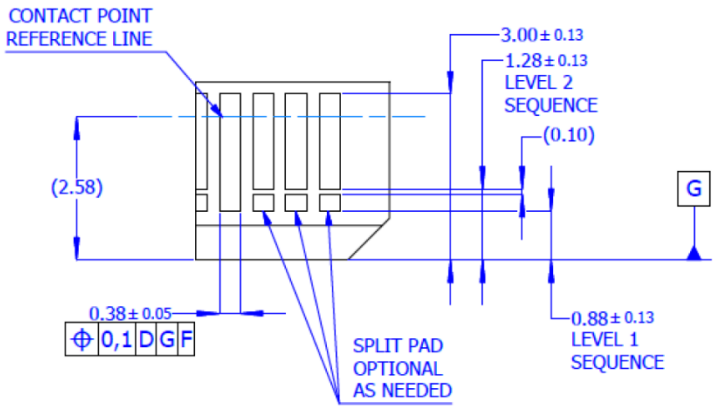


Figure 14. FFF Card Edge Connector – Detail D

3.1 Gold Finger Plating Requirements

The minimum DC-SCM gold finger plating shall be 30u" of gold over 50u" of nickel.

3.2 HPM Connector Definition

The mating connector on the HPM is compliant to the 4C+ connector as defined in the SFF-TA-1002 specification for right angle, straddle mount and vertical form factor connectors. All three connector options are supported by this specification.

3.2.1 Straddle Mount Connector

Straddle mount connectors are intended for use in designs in which the DC-SCM is installed fully co-planar to the HPM. The dimensions for the connector are shown in Figure 15.

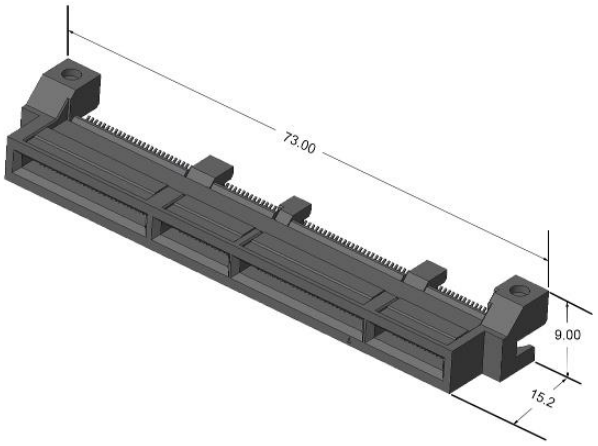


Figure 15. Straddle Mount Connector Dimensions (in mm)

The straddle mount connectors support four HPM PCB thicknesses. The available options are shown in Table 1. PCB thickness must be controlled to within ±10%. Note that the DC-SCM PCB thickness is required to be .062" (1.57mm) while the HPM PCB thickness can vary from .062" (1.57mm) to .110" (2.79mm)

Table 1. Straddle Mount Connector PCB Thicknesses

Connector	Mating (SCM) PCB Thickness	Host (HPM) PCB Thickness
A	.062" (1.57mm)	.062" (1.57mm)
B	.062" (1.57mm)	.076" (1.93mm)
C	.062" (1.57mm)	.093" (2.36mm)
D	.062" (1.57mm)	.105" (2.67mm)
E	.062" (1.57mm)	.110" (2.79mm)

The choice of HPM PCB thickness impacts the offset of the DC-SCM with respect to the HPM PCB. This needs to be accounted for in the system design. Table 2 and the accompanying Figure 16 and Figure 17 details the PCB thickness and offset supports for the connector options.

Table 2. Straddle Mount Connector PCB Offsets

Name	**Pins**	**Style and Baseboard Thickness**	**Offset (mm)**
4C+	168	.062" (1.57mm)	Coplanar (0mm)
4C+	168	.076" (1.93mm)	-0.3mm
4C+	168	.093" (2.36mm)	Coplanar (0mm)
4C+	168	.105" (2.67mm)	Coplanar (0mm)
4C+	168	.110" (2.79mm)	Coplanar (0mm)

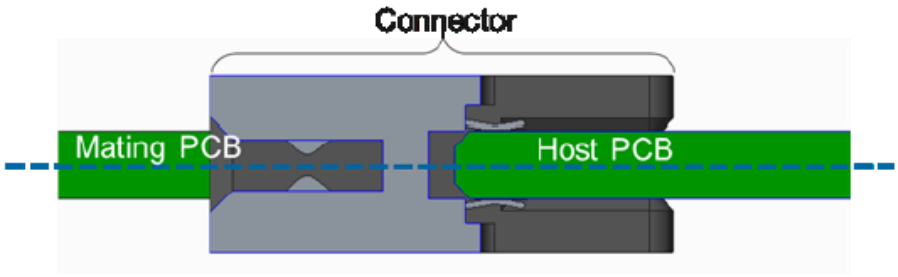


Figure 16. Straddle Mount Connector 0mm Offset for 0.062”, 0.093”, and 0.105” HPM PCB

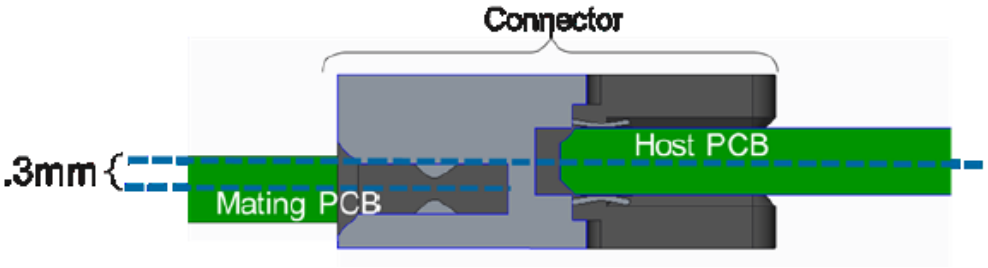


Figure 17. Straddle Mount Connector -0.3mm Offset for 0.076” HPM PCB

3.2.2 Right Angle Connector

Right angle connectors are intended for a similar use but enable an increased DC-SCM bottom side keep out. Use of a right-angle connector eliminates any impact of the HPM PCB thickness with relation to the connector offset ensuring a constant 4.05mm offset for all designs. The dimensions for the connector are shown in Figure 18.

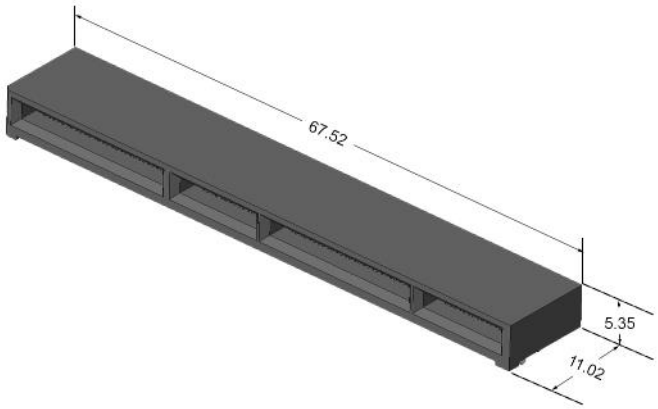


Figure 18. Right Angle Connector Dimensions (in mm)

Figure 19 details the PCB thickness and offset supports for this connector option.

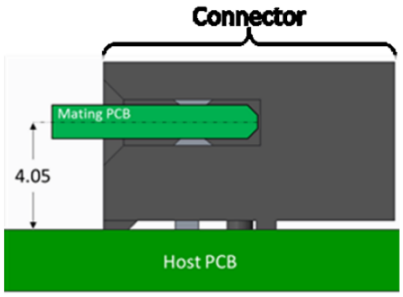


Figure 19. Right Angle Connector Offset

3.2.3 Vertical Connector

Vertical connectors are intended for use in vertical form-factors. The dimensions for the connector are shown in Figure 20.

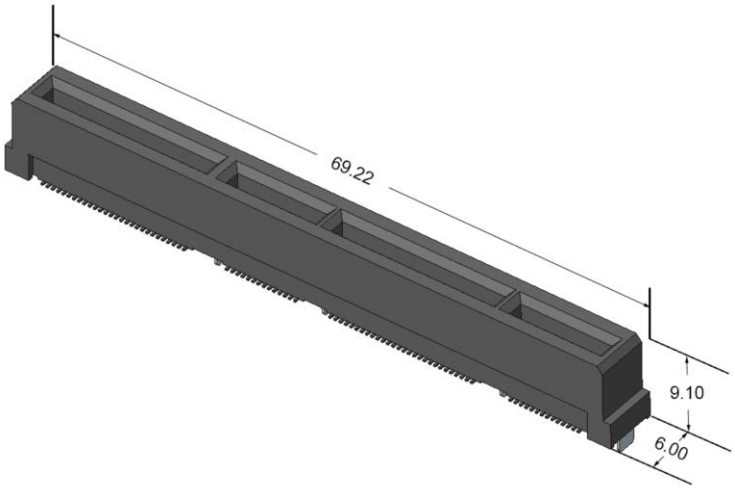


Figure 20. Vertical Connector Dimensions (in mm)

3.3 DC-SCI Pin Definition

The DC-SCI connector pinout is defined in Table 3. The contact sequence for each pin is shown to indicate the order in which the pins make contact between the HPM and the DC-SCM. The GND pins are required to be long pins or 1st mate. The PRSNT0_N/ PRSNT1_N pins and P12V_AUX pins are required to be short pins or 2nd mate. However, the remaining pins indicated as 2nd mate can be flexibly assigned as long pins/1st mate if dictated by design or DFM requirements.

Table 3: DC-SCI Pinout

Pin No.	Contact Sequence	Pin Name	Pin No.	Contact Sequence	Pin Name
OA1	2nd mate	P12V_AUX	OB1	2nd mate	P12V_AUX
OA2	2nd mate	P12V_AUX	OB2	2nd mate	P12V_AUX
OA3	1st mate	GND	OB3	2nd mate	PRSNT0_N
OA4	1st mate	GND	OB4	1st mate	GND
OA5	2nd mate	I3C[0]_SCL	OB5	2nd mate	UART1_SCM_TX
OA6	2nd mate	I3C[0]_SDA	OB6	2nd mate	UART1_SCM_RX
OA7	2nd mate	I3C[1]_SCL	OB7	1st mate	GND
OA8	2nd mate	I3C[1]_SDA	OB8	2nd mate	UART0_SCM_TX
OA9	2nd mate	I3C[2]_SCL	OB9	2nd mate	UART0_SCM_RX
OA10	2nd mate	I3C[2]_SDA	OB10	1st mate	GND
OA11	2nd mate	I3C[3]_SCL	OB11	2nd mate	SPI0_CLK
OA12	2nd mate	I3C[3]_SDA	OB12	2nd mate	SPI0_CS_N
OA13	1st mate	GND	OB13	2nd mate	SPI0_MOSI
OA14	2nd mate	VIRTUAL_RESEAT	OB14	2nd mate	SPI0_MISO
Key					
A1	2nd mate	I2C[0]_SCL	B1	2nd mate	ESPI_CLK
A2	2nd mate	I2C[0]_SDA	B2	2nd mate	ESPI_CS0_N
A3	2nd mate	I2C[1]_SCL	B3	2nd mate	ESPI_ALERT_N
A4	2nd mate	I2C[1]_SDA	B4	2nd mate	ESPI_RESET_N
A5	2nd mate	I2C[2]_SCL	B5	2nd mate	ESPI_IO0
A6	2nd mate	I2C[2]_SDA	B6	2nd mate	ESPI_IO1
A7	2nd mate	I2C[3]_SCL	B7	2nd mate	ESPI_IO2
A8	2nd mate	I2C[3]_SDA	B8	2nd mate	ESPI_IO3
A9	2nd mate	I2C[4]_SCL	B9	2nd mate	RSVD3
A10	2nd mate	I2C[4]_SDA	B10	1st mate	GND
A11	2nd mate	I2C[5]_SCL	B11	2nd mate	QSPI0_CLK
A12	2nd mate	I2C[5]_SDA	B12	2nd mate	QSPI0_CS0_N
A13	1st mate	GND	B13	2nd mate	QSPI0_D0
A14	2nd mate	CLK_100M_PCIE_DP	B14	2nd mate	QSPI0_D1
A15	2nd mate	CLK_100M_PCIE_DN	B15	2nd mate	QSPI0_D2
A16	1st mate	GND	B16	2nd mate	QSPI0_D3
A17	2nd mate	PCIE_BMC_TX_DP	B17	1st mate	GND
A18	2nd mate	PCIE_BMC_TX_DN	B18	2nd mate	NCSI_CLK
A19	1st mate	GND	B19	2nd mate	NCSI_CRS_DV
A20	2nd mate	PCIE_BMC_RX_DP	B20	2nd mate	NCSI_TXEN
A21	2nd mate	PCIE_BMC_RX_DN	B21	2nd mate	NCSI_TXD0
A22	1st mate	GND	B22	2nd mate	NCSI_TXD1
A23	2nd mate	I2C[6]_SCL	B23	2nd mate	NCSI_RXER
A24	2nd mate	I2C[6]_SDA	B24	2nd mate	NCSI_RXD0
A25	2nd mate	I2C[7]_SCL	B25	2nd mate	NCSI_RXD1
A26	2nd mate	I2C[7]_SDA	B26	1st mate	GND
A27	2nd mate	I2C[8]_SCL	B27	2nd mate	PECI_BMC
A28	2nd mate	I2C[8]_SDA	B28	2nd mate	PVCCIO_PECI
Key					

A29	2nd mate	I2C[9]_SCL	B29	2nd mate	SGPIO0_DO
A30	2nd mate	I2C[9]_SDA	B30	2nd mate	SGPIO_CLK
A31	2nd mate	I2C[10]_SCL	B31	2nd mate	SGPIO0_DI
A32	2nd mate	I2C[10]_SDA	B32	2nd mate	SGPIO0_LD
A33	1st mate	GND	B33	1st mate	GND
A34	2nd mate	JTAG_TCK	B34	2nd mate	SGPIO1_DO
A35	2nd mate	JTAG_TMS	B35	2nd mate	RSVD2
A36	2nd mate	JTAG_TDI	B36	2nd mate	SGPIO1_DI
A37	2nd mate	JTAG_TDO	B37	2nd mate	SGPIO1_LD
A38	2nd mate	I2C[11]_SCL	B38	1st mate	GND
A39	2nd mate	I2C[11]_SDA	B39	2nd mate	SGPIO_RESET_N
A40	2nd mate	I2C[12]_SCL	B40	2nd mate	SGPIO_INTR_N
A41	2nd mate	I2C[12]_SDA	B41	2nd mate	P3V0_BAT
A42	1st mate	GND	B42	2nd mate	QSPI0_CS1_N
Key					
A43	2nd mate	HPM_FW_RECOVERY	B43	2nd mate	QSPI1_CLK
A44	2nd mate	HPM_STBY_RDY	B44	2nd mate	QSPI1_CS0_N
A45	2nd mate	HPM_STBY_EN	B45	2nd mate	QSPI1_D0
A46	2nd mate	HPM_STBY_RST_N	B46	2nd mate	QSPI1_D1
A47	2nd mate	SYS_PWRBTN_N	B47	2nd mate	QSPI1_D2
A48	2nd mate	SYS_PWROK	B48	2nd mate	QSPI1_D3
A49	2nd mate	DBP_PREQ_N	B49	1st mate	GND
A50	2nd mate	DBP_PRDY_N	B50	2nd mate	USB2_DP
A51	2nd mate	RST_PLTRST_BUF_N	B51	2nd mate	USB2_DN
A52	2nd mate	SPARE1	B52	1st mate	GND
A53	2nd mate	RoT_CPU_RST_N	B53	2nd mate	USB1_DP
A54	2nd mate	CHASI#	B54	2nd mate	USB1_DN
A55	2nd mate	SPARE0	B55	1st mate	GND
A56	2nd mate	IRQ_N	B56	2nd mate	RSVD0
A57	2nd mate	PRSNT1_N	B57	2nd mate	RSVD1
A58	1st mate	GND	B58	1st mate	GND
A59	2nd mate	PCIE_HPM_RXP[0]	B59	2nd mate	PCIE_HPM_TXP[0]
A60	2nd mate	PCIE_HPM_RXN[0]	B60	2nd mate	PCIE_HPM_TXN[0]
A61	1st mate	GND	B61	1st mate	GND
A62	2nd mate	PCIE_HPM_RXP[1]	B62	2nd mate	PCIE_HPM_TXP[1]
A63	2nd mate	PCIE_HPM_RXN[1]	B63	2nd mate	PCIE_HPM_TXN[1]
A64	1st mate	GND	B64	1st mate	GND
A65	2nd mate	PCIE_HPM_RXP[2]	B65	2nd mate	PCIE_HPM_TXP[2]
A66	2nd mate	PCIE_HPM_RXN[2]	B66	2nd mate	PCIE_HPM_TXN[2]
A67	1st mate	GND	B67	1st mate	GND
A68	2nd mate	PCIE_HPM_RXP[3]	B68	2nd mate	PCIE_HPM_TXP[3]
A69	2nd mate	PCIE_HPM_RXN[3]	B69	2nd mate	PCIE_HPM_TXN[3]
A70	1st mate	GND	B70	1st mate	GND

3.4 DC-SCI Signal Descriptions

The following sections provide the signal descriptions of signals through the DC-SCI.

Note: Follow device datasheet recommendations to appropriately terminate un-used signals on the DC-SCM.

Abbreviation Definition:

Symbol	Description
_N or #	Denotes active low signal
I	Input to DC-SCM
O	Output from DC-SCM
I/O	Bi-directional signals between DC-SCM and HPM

3.4.1 NC-SI

The DC-SCI supports a RMII/NC-SI interface from the DC-SCM to the HPM. This enables cable-less support for OCP NIC 3.0 compliant ethernet adapters. This specification does not define a NC-SI cabled solution. Any accommodations for cabled requirements should reside directly on the DC-SCM or on the HPM. A description of the signals is shown in Table 4. To best account for timing requirements associated with NCSI clock, it is assumed that the clock source is located on the HPM.

Table 4: NC-SI Signal Descriptions

Signal Name	I/O	Voltage(V)	Description
NCSI_CLK_IN	I	3.3	RMII Reference clock input. The clock has a nominal frequency of 50MHz ±100ppm.
NCSI_CRS_DV	I	3.3	NC-SI carrier sense receive data valid signal.
NCSI_TXD0	O	3.3	BMC transmit to NC-SI interface
NCSI_TXD1	O	3.3	BMC transmit to NC-SI interface
NCSI_RXD0	I	3.3	BMC receive for NC-SI interface
NCSI_RXD1	I	3.3	BMC receive for NC-SI interface
NCSI_TXEN	O	3.3	NC-SI Transmit Enable
NCSI_RXER	I	3.3	NC-SI receive data error

3.4.2 eSPI/SSIF

There are two primary communication paths within different architectures used to enable communication from a processing unit on the HPM to the BMC.

- eSPI – Used by next generation Intel and AMD architectures.
- SSIF – I2C bus and alert used by ARM architectures.

The DC-SCM supports one eSPI interface between the DC-SCM and the HPM. Note that the LPC bus which was used in previous Intel and AMD architectures is not supported by the DC-SCM. A description of the eSPI signals is shown in Table 5.

For implementation supporting SSIF, please refer to Section 3.4.4.

Table 5: eSPI Signal Descriptions

Signal Name	I/O	Voltage(V)	Description
ESPI_CLK	I	1.8	eSPI clock from SOC to BMC
ESPI_CS0_N	I	1.8	eSPI CS0# from SOC to BMC
ESPI_IO0	I/O	1.8	eSPI IO Data bit 0. Connected to SOC
ESPI_IO1	I/O	1.8	eSPI IO Data bit 1. Connected to SOC
ESPI_IO2	I/O	1.8	eSPI IO Data bit 2. Connected to SOC
ESPI_IO3	I/O	1.8	eSPI IO Data bit 3 Connected to SOC
ESPI_ALERT_N	O	1.8	eSPI Alert from BMC to SOC
ESPI_RESET_N	I	1.8	eSPI Reset# from SOC to BMC

An example block diagram demonstrating the eSPI interface is shown in Figure 21. Since BMCs may share functionality on their eSPI bus with the legacy LPC bus, they may require appropriate strapping on the DC-SCM to select the eSPI interface.

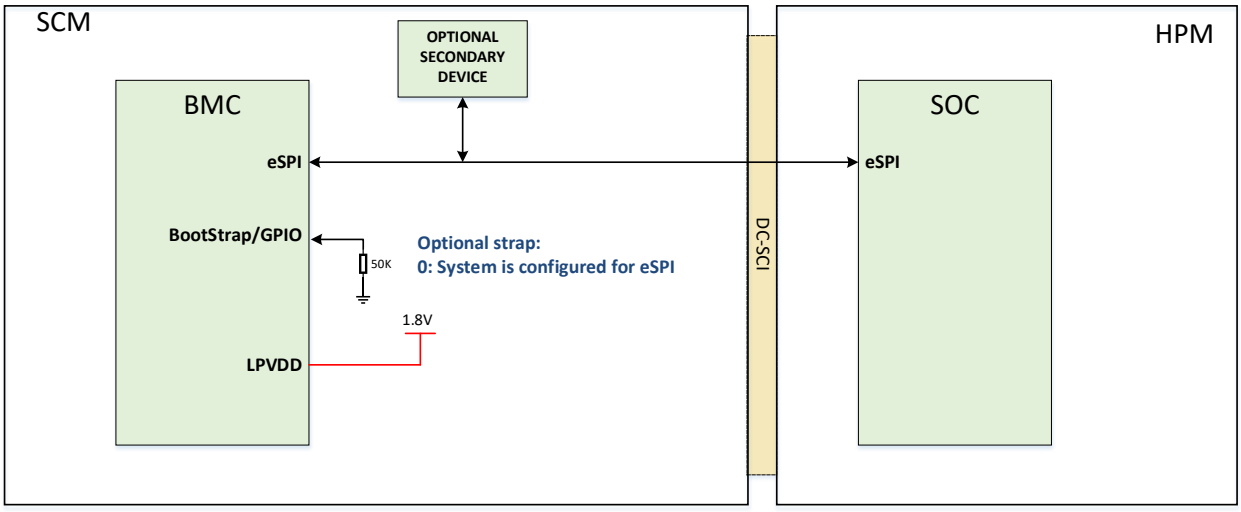


Figure 21. ESPI Example Block Diagram

3.4.3 Serial GPIO

The DC-SCI supports two Serial GPIO (SGPIO) interfaces between the DC-SCM and the HPM. The primary purpose of SGPIOs is to provide a low pin usage interface for transmitting status and control signals.

Use of SGPIOs enables this communication while minimizing the impact on today's BMC architectures that are heavily dependent on direct to BMC GPIOs.

The SGPIO has the following features:

- Source synchronous interface.
- DC-SCM provides the clock and load signal and is always the initiator.
- DC-SCI provides two SGPIO interfaces to enable assignment of signals with the goal of optimizing (if needed) for lowest possible latency.
- The SGPIO clock is common to both SGPIO0 and SGPIO1 interfaces, such that both interfaces are run synchronously.
- Single reset from DC-SCM to HPM to reset the responder SGPIOs.

A description of the SGPIO signals is shown in Table 6.

Table 6: SGPIO Signal Descriptions

Function	I/O	Voltage(V)	Description
SGPIO_CLK	O	3.3	SGPIO Clock from DC-SCM to HPM. This is common to SGPIO0 and SGPIO1.
SGPIO0_DI	I	3.3	SGPIO Data Input from HPM to DC-SCM
SGPIO0_DO	O	3.3	SGPIO Data Output from DC-SCM to HPM
SGPIO0_LD	O	3.3	SGPIO Data Load DC-SCM to HPM
SGPIO1_DI	I	3.3	SGPIO Data Input from HPM to DC-SCM
SGPIO1_DO	O	3.3	SGPIO Data Output from DC-SCM to HPM
SGPIO1_LD	O	3.3	SGPIO Data Load DC-SCM to HPM
SGPIO_RESET_N	O	3.3	Reset the serial bus latches and registers on HPM FPGA side for SGPIO0 and SGPIO1 interfaces
SGPIO_INTR_N	I	3.3	Optional SGPIO0/1 interrupt to DC-SCM CPLD from HPM FPGA.

An example block diagram demonstrating the SGPIO interfaces from the DC-SCM to the HPM is shown in Figure 22. In this example, a higher number of high latency tolerant status and control signals are placed on SGPIO #0. A lower number of low latency status and control are placed on SGPIO #1. Actual usage of signals interface to the SGPIOs will vary based on the system design requirements.

The SGPIO clocks are recommended to be operated in the 20-37 MHz range to guarantee lower latencies on the GPIOs. Please refer to Section 5.2 of this spec for detailed timing analysis on the SGPIO interface.

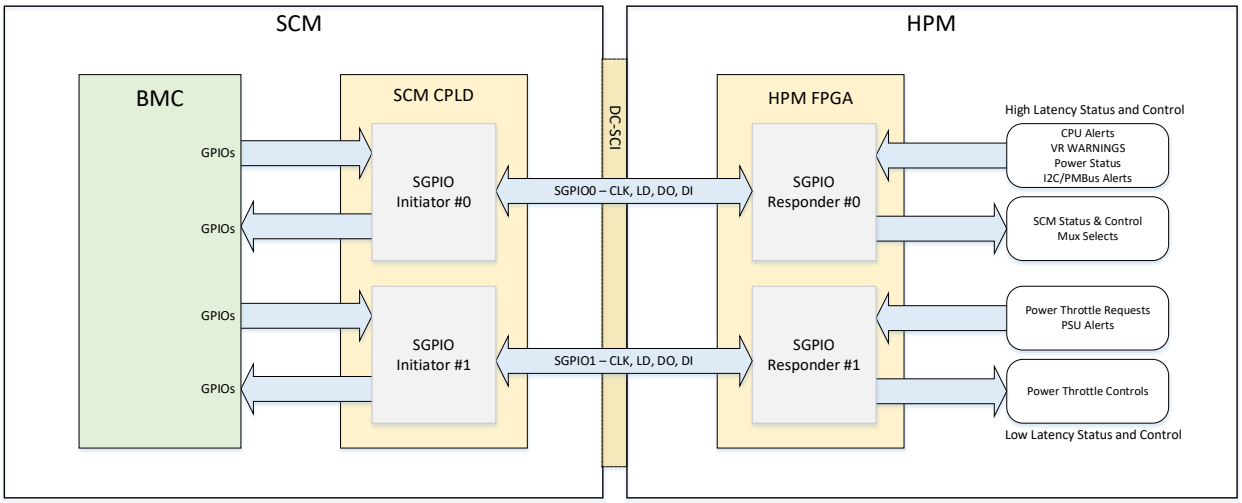


Figure 22: SGPIO Example Block Diagram

3.4.4 I2C

The DC-SCI supports a total 13 I2C ports from the DC-SCM to the HPM. These include I2C buses to RoT and BMC on the DC-SCM. The HPM must provide pullup resistors to the 3.3V STBY rail. Components on HPM that are attached to these buses, and powered by non-STBY rails, must be appropriately electrically isolated. Any local DC-SCM I2C channels should be kept separate from HPM I2C buses to simplify the design and eliminate potential for voltage leaks between the separate power domains. I2C Alerts can optionally be supported using the SGPIO bus.

Table 7: I2C Signal Descriptions

Signal Name	I/O	Voltage(V)	Description
I2C [0:12]_SCL	O	3.3	I2C Clock
I2C [0:12]_SDA	I/O	3.3	I2C Data

An example block diagram demonstrating I2C interfaces on the DC-SCM is shown in Figure 23.

To ensure interoperability between DC-SCM and different HPMs, this specification enforces the following rules -

- Fixed FRUID PROM address: It is required that the FRUID PROM be placed directly on channel I2C4 (Not behind a MUX) at address 0xA0 (8-bit address). This provides a fixed location for a BMC to detect a platform type and load the necessary platform specific parameters to ensure full functionality of the platform.
- Fixed I2C Channel for IPMI SSIF: When IPMI SSIF is supported by the system, it is required that I2C[12] be used by the HPM and DC-SCM for this purpose. The corresponding Alert can be routed over the SGPIO interface. A HPM that does not support IPMI SSIF may route this to any I2C device. On the DC-SCM side, I2C12 should be routed to a BMC I2C controller that can be configured either as an initiator or a responder.

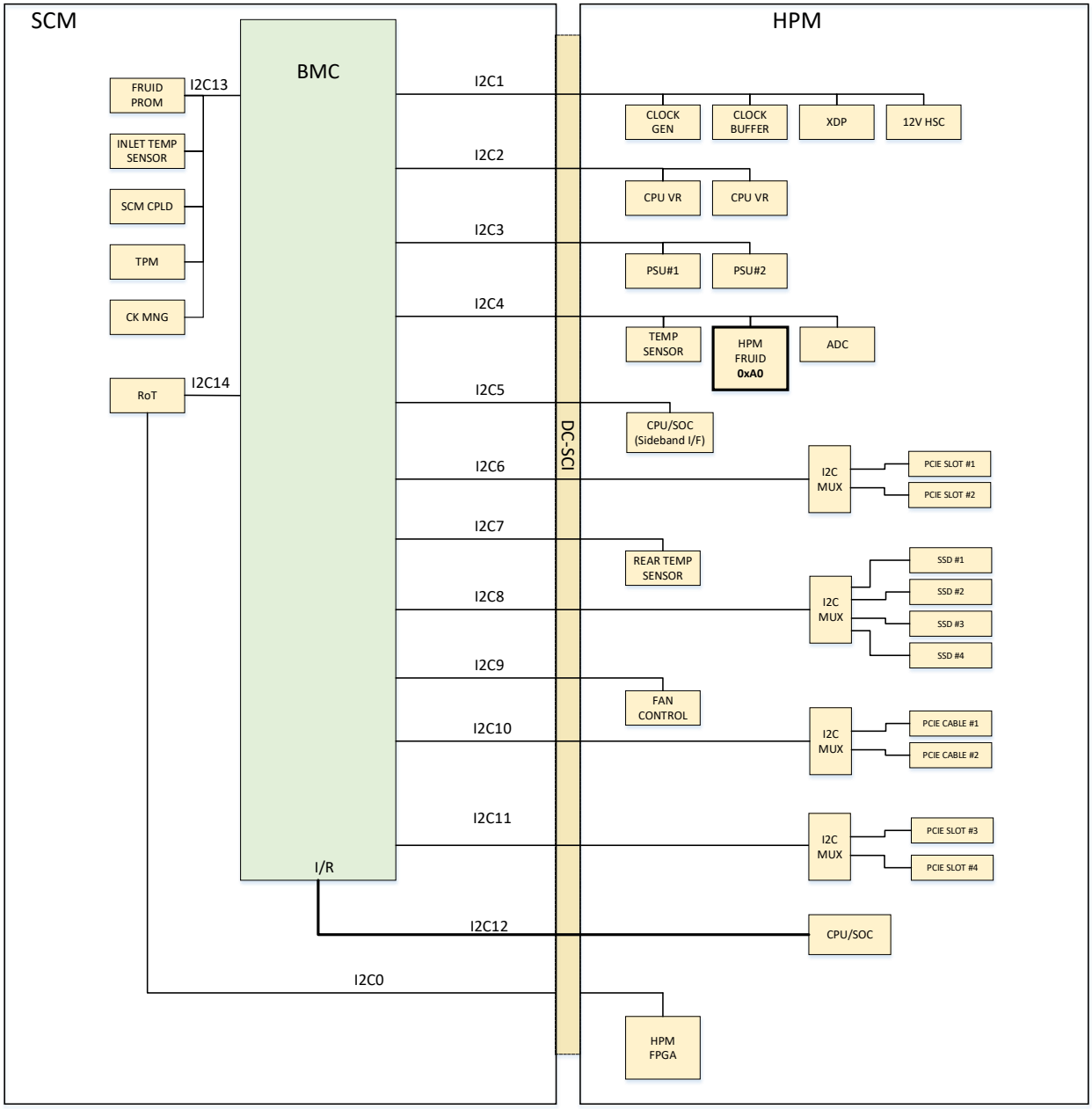


Figure 23: I2C Example Block Diagram

3.4.5 I3C

The DC-SCI supports four I3C buses. These are intended to enable future uses of I3C for HPM features such as DDR5 SPD. Per the I3C specification, these buses may also be used to connect I2C "responder-only" devices, that support fast mode with a true 50ns glitch filter on SCL, and no responder clock stretching.

Table 8: I3C Signal Descriptions

Signal Name	I/O	Voltage(V)	Description
I3C[0:3]_SCL	O	1.0	I3C Clock
I3C[0:3]_SDA	I/O	1.0	I3C Data

An example block diagram demonstrating the BMC low voltage I3C interface to DDR5 SPD is shown in Figure 24. Note that I3C supports multiple initiators on the same bus, but optional muxes can be added to eliminate secondary initiator negotiation.

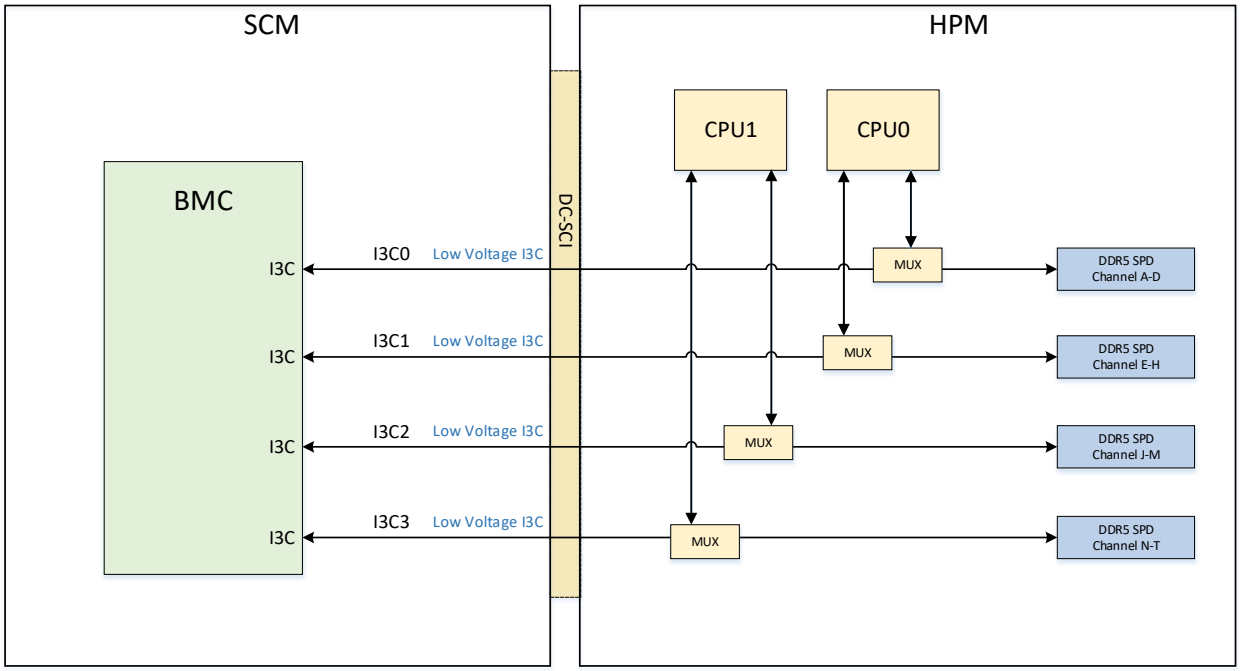


Figure 24: An Example I3C SPD DDR5 Block Diagram

3.4.6 SPI

The DC-SCI support three SPI interfaces:

- SPI0 – HPM is the initiator. This enables future expansion for next generation processors such as enabling separation of TPM from the BIOS flash QSPI port. SPI0_CS_N can be used as a second chip select for TPM on QSPI0 bus in current architectures. In future architectures they can be used as chip select for TPM on SPI0 bus.
- QSPI0 – HPM is the initiator. This enables HPM communication with the BIOS flash devices on the DC-SCM.

- QSPI1 – DC-SCM is the initiator. This enables DC-SCM communication with expansion devices on the HPM such as the HPM FPGA.

A description of the signals is shown in Table 9.

Table 9: SPI Signal Descriptions

Signal Name	I/O	Voltage(V)	Description
SPI0_CLK	I	3.3	SPI Clock from the HPM to the DC-SCM
SPI0_CS_N	I	3.3	SPI CS# from the HPM to the DC-SCM
SPI0_MOSI	I	3.3	SPI MOSI from the HPM to the DC-SCM
SPI0_MISO	O	3.3	SPI MISO from the DC-SCM to the HPM
QSPI0_CLK	I	3.3	QSPI Clock from HPM to BIOS Flash on the DC-SCM
QSPI0_CS0_N	I	3.3	QSPI CS0# from HPM to BIOS Flash on the DC-SCM
QSPI0_CS1_N	I	3.3	QSPI CS1# from HPM to BIOS Flash on the DC-SCM
QSPI0_D0	I/O	3.3	QSPI D0 from HPM to BIOS Flash on the DC-SCM
QSPI0_D1	I/O	3.3	QSPI D1 from HPM to BIOS Flash on the DC-SCM
QSPI0_D2	I/O	3.3	QSPI D2 from HPM to BIOS Flash on the DC-SCM
QSPI0_D3	I/O	3.3	QSPI D3 from HPM to BIOS Flash on the DC-SCM
QSPI1_CLK	O	3.3	QSPI Clock from DC-SCM to HPM FPGA on the HPM
QSPI1_CS_N	O	3.3	QSPI CS# from DC-SCM to HPM FPGA on the HPM
QSPI1_D0	I/O	3.3	QSPI D0 from DC-SCM to HPM FPGA on the HPM
QSPI1_D1	I/O	3.3	QSPI D1 from DC-SCM to HPM FPGA on the HPM
QSPI1_D2	I/O	3.3	QSPI D2 from DC-SCM to HPM FPGA on the HPM
QSPI1_D3	I/O	3.3	QSPI D3 from DC-SCM to HPM FPGA on the HPM

An example block diagram is shown in Figure 25. The example includes an optional RoT for attestation of BMC and BIOS flash to demonstrate one of the potential security aspects of DC-SCM.

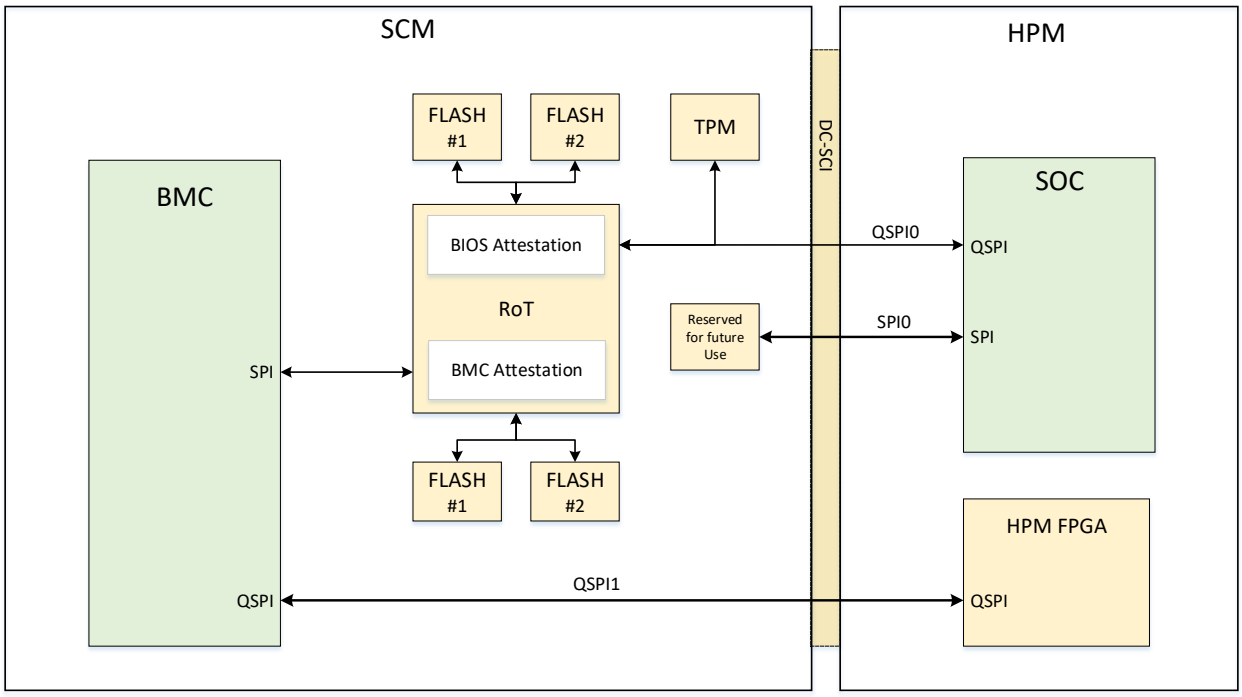


Figure 25: SPI Example Block Diagram

3.4.7 USB

The DC-SCI supports two USB ports between the DC-SCM and the HPM.

- USB 1 – This is typically used to support USB 2.0 connection between the HPM and the BMC. The HPM is the initiator.
- USB 2 – Second USB 2.0 interface that typically connects to expansion devices within the chassis. The initiator can be the DC-SCM or HPM depending on the HPM implementation and should be firmware selectable on DC-SCM and HPM.

Any additional USB port connections (e.g., Front USB) on the DC-SCM will require the use of USB hubs or switches. A description of the signals is shown in Table 10. An example block diagram demonstrating typical USB DC-SCM/HPM architecture is shown in Figure 26.

Table 10: USB Signal Descriptions

Function	I/O	Voltage(V)	Description
USB1_DP	I/O	-	USB 2.0 between HPM SOC and DC-SCM BMC
USB1_DN	I/O	-	USB 2.0 between HPM SOC and DC-SCM BMC
USB2_DP	I/O	-	USB 2.0 between DC-SCM BMC and HPM expansion device
USB2_DN	I/O	-	USB 2.0 from DC-SCM BMC and HPM expansion device

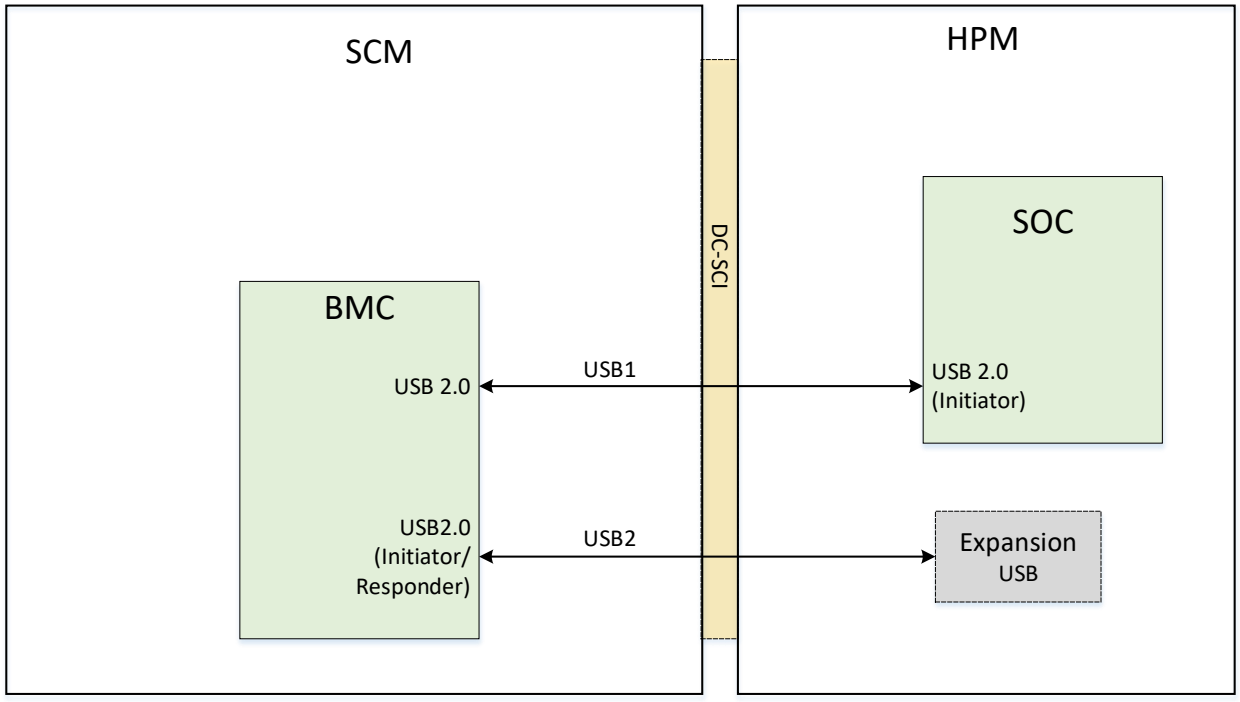


Figure 26: USB Block Diagram

3.4.8 PCIe

The DC-SCI supports two PCIe buses between the HPM and the DC-SCM.

- PCIe Gen 3.0 x1 Interface – This is typically connected to a BMC as a PCIe endpoint, thereby enabling host to BMC communication for out of band operations such as video and firmware update. A description of the signals is shown in Table 11.
- PCIe Gen 5.0 x4 Interface – This optional interface enables the HPM to communicate with a PCIe Gen 5.0 compliant end-point on the DC-SCM like an SSD. A description of the signals is shown in Table 12.

The DC-SCI supports one PCIe reference clock pair. When both PCIe Gen 3.0 x1 and PCIe Gen 5.0 x4 end-points are supported, the DC-SCM can either design in a clock buffer to distribute the clock to the two end-points or use separate reference clock architecture. When using the PCIe Gen 5.0 x4 interface, the reference clock from HPM should be capable of supporting up to PCIe Gen 5 speeds. A description of the signals is shown in Table 13. PCIe reset for the end-points can be sourced from RST_PLTRST_BUF_N signal supported over DC-SCI as described in Table 19.

Note that some processor architectures which employ different PCIe reference clock and PCIe reset domains for different sockets, may require that the two end-points on the DC-SCM are located on the same domain.

Table 11: PCIe Gen3 Data Signal Description

Function	I/O	Voltage(V)	Description
PCIE_BMC_TX_DP	O	-	PCIe Gen 3 TX from DC-SCM to HPM
PCIE_BMC_TX_DN	O	-	PCIe Gen 3 TX from DC-SCM to HPM
PCIE_BMC_RX_DP	I	-	PCIe Gen 3 RX from HPM to DC-SCM
PCIE_BMC_RX_DN	I	-	PCIe Gen 3 RX from HPM to DC-SCM

Table 12: PCIe Gen5 Data Signal Description

Function	I/O	Voltage(V)	Description
PCIE_HPM_TX_DP	I	-	PCIe Gen 5 TX from HPM to DC-SCM
PCIE_HPM_TX_DN	I	-	PCIe Gen 5 TX from HPM to DC-SCM
PCIE_HPM_RX_DP	O	-	PCIe Gen 5 RX from DC-SCM to HPM
PCIE_HPM_RX_DN	O	-	PCIe Gen 3 RX from DC-SCM to HPM

Table 13: PCIe Clock Signal Description

Function	I/O	Voltage(V)	Description
CLK_100M_PCIE_DP	I	-	PCIe Gen 5 capable Clock from HPM to DC-SCM
CLK_100M_PCIE_DN	I	-	PCIe Gen 5 capable Clock from HPM to DC-SCM

3.4.9 PECI

The DC-SCI supports a PECI interface for health monitoring of CPUs. When this interface is un-used by the HPM architecture, it should be appropriately terminated on the HPM in accordance with the BMC vendor specification. A description of the signals is shown in Table 14. Note that the PECI interface requires its own voltage supplied by the HPM.

Table 14: PECI Signal Descriptions

Function	I/O	Voltage(V)	Description
PECI_BMC	I/O	0.85-1.21	PECI interface from BMC to CPUs on the HPM
PVCCIO_PECI	I	0.85-1.21	PECI termination rail from HPM

3.4.10 UARTS

The DC-SCI supports two UARTs utilizing software flow control. Typical uses are as follows:

- UART0 - Host Debug Console
- UART1 - Expansion Consoles (PCIe Switch, Expansion SOCs)

Table 15: UART Signal Descriptions

Function	I/O	Voltage(V)	Description
UART0_SCM_TX	O	3.3	UART TX from DC-SCM to HPM. This would typically connect to the SOC on the HPM.
UART0_SCM_RX	I	3.3	UART RX From HPM to DC-SCM. This would typically connect to the SOC on the HPM.
UART1_SCM_TX	O	3.3	UART TX from DC-SCM to HPM. This would typically connect to any additional managed HPM entities such as PCIe Switch or PCIe SOC solution.
UART1_SCM_RX	I	3.3	UART RX from HPM to DC-SCM. This would typically connect to any additional managed HPM entities such as PCIe Switch or PCIe SOC solution.

An example block diagram demonstrating a typical UART DC-SCM/HPM architecture is shown in Figure 27.

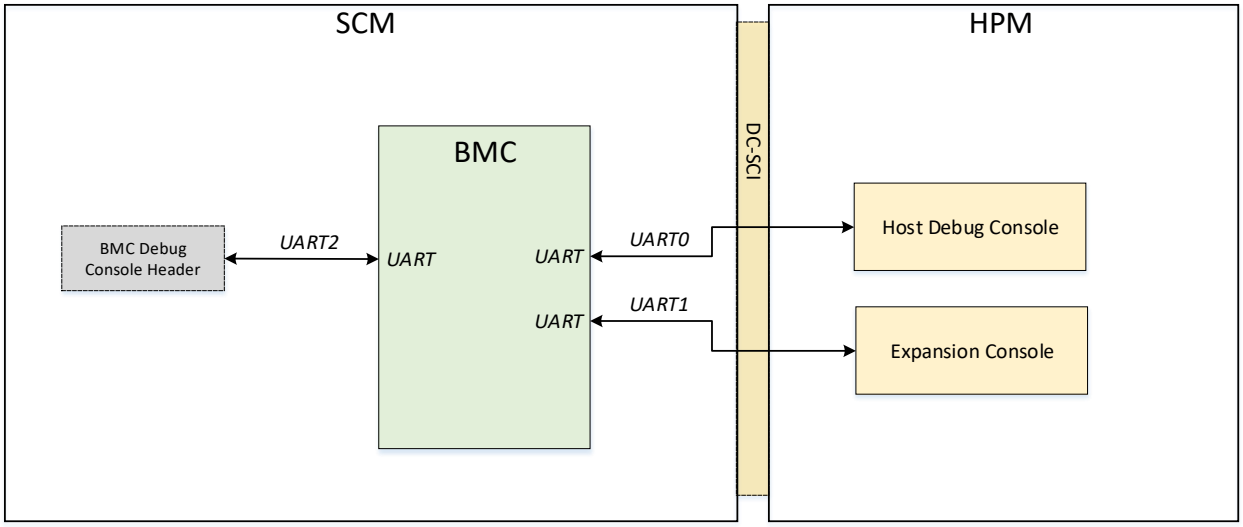


Figure 27: UART Example Block Diagram

3.4.11 JTAG

The DC-SCI supports a JTAG interface with BMC as the initiator on the DC-SCM. Typical uses are as follows:

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

A description of the signals is shown in Table 16. Note that the TRST_N (TAP reset) and SRST_N (Target system reset) if used, should be provisioned over the Serial GPIO bus.

Table 16: JTAG Signal Descriptions

Function	I/O	Voltage(V)	Description
JTAG_TCK	O	3.3	JTAG TCK from the DC-SCM to the HPM
JTAG_TMS	O	3.3	JTAG TMS from the DC-SCM to the HPM
JTAG_TDI	I	3.3	JTAG TDI from the HPM to the DC-SCM
JTAG_TDO	O	3.3	JTAG TDO from the DC-SCM to the HPM

An example block diagram demonstrating typical JTAG DC-SCM/HPM architecture is shown in Figure 28. The HPM_FW_RECOVERY signal provides a means of selecting the right JTAG MUX channel to recover the HPM FPGA if corrupted or blank as described in Table 22. C can program the device if it is in a blank or corrupted state. Once SGPIO communication is established, this selection will be done by the BMC.

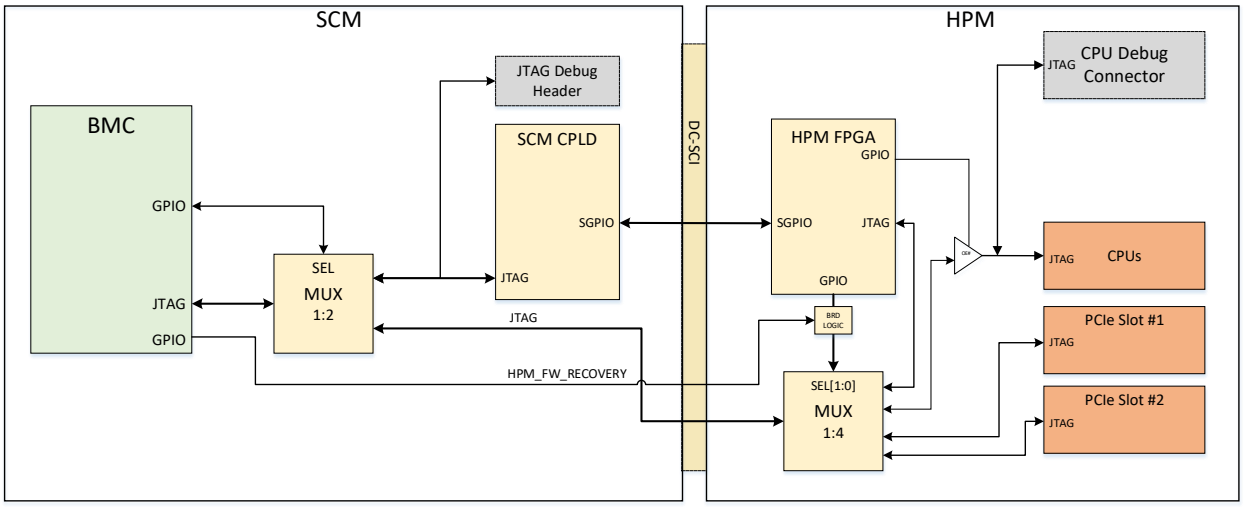


Figure 28: JTAG Example Block Diagram

3.4.12 Standby Power and Boot Sequence

The DC-SCI interface supports 12V for powering the DC-SCM. Sequencing is specified such that STBY power on the DC-SCM is enabled and valid before STBY power on the HPM. This ensures an orderly sequence that supports reasonable design rules to prevent voltage leaks and unpredictable system behavior. Sequencing of STBY power between the DC-SCM and HPM is controlled through the signals described in Table 17.

Table 17: Power Sequence Signal Descriptions

Signal Name	I/O	Voltage(V)	Description
HPM_STBY_EN	O	3.3	Active High. Indicates that all DC-SCM STBY power rails are enabled and good. Enables STBY power rails on the HPM
HPM_STBY_RDY	I	3.3	Active High. Indicates that all HPM STBY power rails are good. Can optionally be used to indicate that the HPM FPGA is configured. Enables DC-SCM to de-assert reset to BMC and associated circuitry

HPM_STBY_RST_N	O	3.3	Active Low. Holds HPM standby devices in reset. Driven high by the DC-SCM to bring the standby devices on the HPM out of reset

An example block diagram of the power sequencing architecture is shown below in Figure 29. In this block diagram, although the DC-SCM is not intended to support hot plug or hot removal, an eFUSE is included on the HPM to protect the DC-SCM from any overcurrent events. To ensure that there are no voltage leaks between the HPM and DC-SCM, it is recommended that pullup resistors for all I/O on the DC-SCI be placed on the HPM.

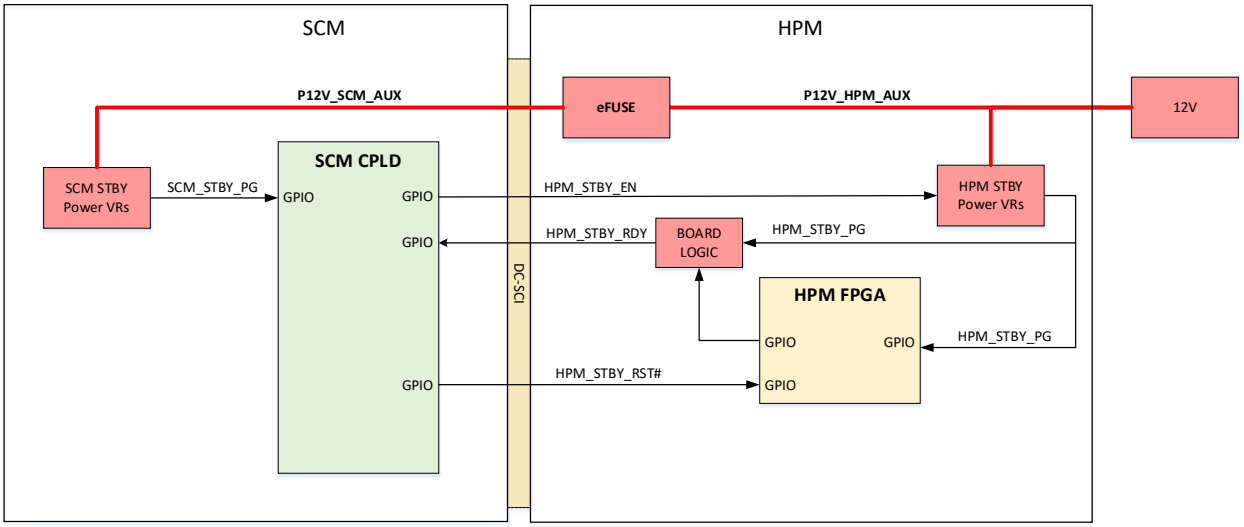


Figure 29: DC-SCM STBY Sequencing Signals Block Diagram

An example power-on and boot sequence diagram is shown in Figure 30. This provides a high-level description of the power and reset sequence requirements leading up to the release of system reset and OS boot on the HPM. Typical security attestation events have been included in the flow as an example. Actual implementation on the DC-SCM can vary depending on the application.

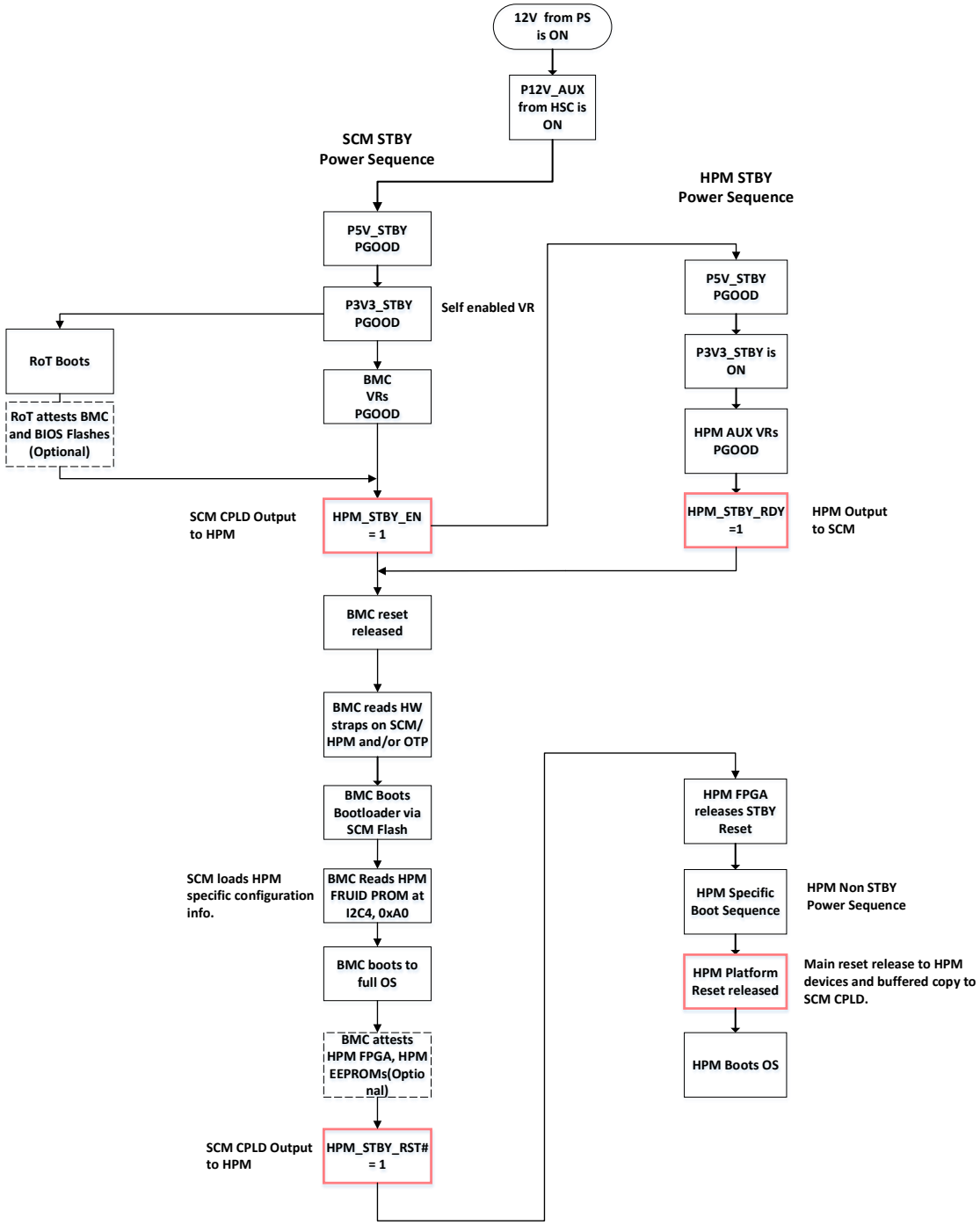


Figure 30: Power and Boot Sequence Diagram

3.4.13 Battery Voltage

The DC-SCI supports one pin for 3.0V battery power from the HPM.

Table 18: Battery Voltage

Signal Name	I/O	Voltage(V)	Description
P3V0_BAT	I	3.0	3.0V from coin cell battery located on HPM which can be used for features such as an optional chassis intrusion header located on DC-SCM or powering any battery backed latches on DC-SCM etc. The DC-SCM design must ensure that the current drain on this rail is less than 1 uA.

3.4.14 Miscellaneous Signals

Table 19, Table 20 and Table 21 below list the RoT, Debug and Interrupt signals provisioned on the DC-SCI respectively.

Table 19: RoT IO via DC-SCI

Signal Name	I/O	Voltage(V)	Description
RoT_CPU_RST_N	O	3.3	RoT to HPM FPGA, CPU reset control. Enables BIOS/UEFI boot after flash authentication.
RST_PLTRST_BUF_N	I	3.3	Buffered copy of Platform reset from SOC on HPM. Indication of platform reset status to RoT. PCIE Reset to BMC, Reset to TPM can be sourced from this signal.

Table 20: Debug IO via DC-SCI

Signal Name	I/O	Voltage(V)	Description
DBP_PREQ_N	O	3.3	Optional Remote debug control signal.
DBP_PRDY_N	I	3.3	Optional Remote debug control signal.

Note: FBRK_N (CPU early Break) if used, should be provisioned over the Serial GPIO bus.

Table 21: Interrupts via DC-SCI

Signal Name	I/O	Voltage(V)	Description
IRQ_N	I	3.3	Optional Interrupt from HPM FPGA to BMC

Note: BMC SMI (System management interrupt) to SOC and any additional interrupt signals can be provisioned over the Serial GPIO bus. CATERR_N can be provisioned over Serial GPIO bus, by ensuring that any decoding based on signal timing is done in the HPM FPGA before serializing.

Table 22 lists other miscellaneous IOs provisioned on the DC-SCI.

Table 22: Other Miscellaneous IOs via DC-SCI

Signal Name	I/O	Voltage(V)	Description
SYS_PWROK	I	3.3	From SOC via HPM FPGA to DC-SCM. Indicates HPM Main Power Ok
SYS_PWRBTN_N	O	3.3	Power button out signal from BMC to HPM

VIRTUAL_RESEAT	O	3.3	Active high signal from DC-SCM that causes all power rails (including Standby rails) to be removed completely for as long as the signal remains asserted, and then automatically restored. Support for Virtual Reseat is not mandatory, but when implemented, should guarantee that all rails drain down to < 5% of their nominal values before being restored
PRSNT0_N	O	3.3	Must be connected to PRSNT1_N on the DC-SCM. Must be pulled up on the HPM
PRSNT1_N	I	3.3	Must be connected to PRSNT0_N on the DC-SCM. Must be connected to GND on the HPM
CHASI#	I	3.3	Optional Chassis Intrusion alert from the HPM
HPM_FW_RECOVERY	O	3.3	Optional select signal from BMC to HPM, to force a firmware recovery. For e.g., HPM FPGA firmware recovery can be forced by selection of JTAG path from BMC, via this signal
SPARE [0:1]	I/O	3.3	Connect these signals between the HPM FPGA and the DC-SCM CPLD. Ensure that these are defined as inputs on both sides and pulled down on the DC-SCM side. Reserved for future expansion.
RSVD [0:3]	-	-	No connect. Reserved for Future Use

Note: Any PSU power status signals if used, should be provisioned over the Serial GPIO bus.

4 Electrical Specifications

The following sections provide specifications for the DC-SCM input voltage and current.

4.1 Input Voltage, Power, and Current

Table 23 lists the nominal, maximum, and minimum values for the DC-SCM input voltage. The maximum and minimum voltages include the effects of connector temperature, age, noise/ripple, and dynamic loading.

Table 23: Input Power Requirements

	Minimum	Nominal	Max
Input voltage	10V DC	12.3V DC	14V DC
Input Power	n/a	n/a	28W
Inrush Rise Time	5ms	n/a	200ms
*Input Current	n/a	n/a	2.8A

*Input current is based on 1A rating per pin, derated at 70%. Total of four power pins on the DC-SCI.

4.2 SCM Presence Detection and Power Protection

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 damage due to damaged connector pins, accidental removal or installation in a powered system etc.

The DC-SCI provides two active low pins (A57 and OB3) dedicated for presence detection, on both side of the connector. Table 22 provides the signal description for the PRSNT0_N and PRSNT1_N signals. The HPM design must ensure that power to the DC-SCM and HPM are disabled when presence is not detected.

Figure 31 shows a typical presence detection and power protection implementation.

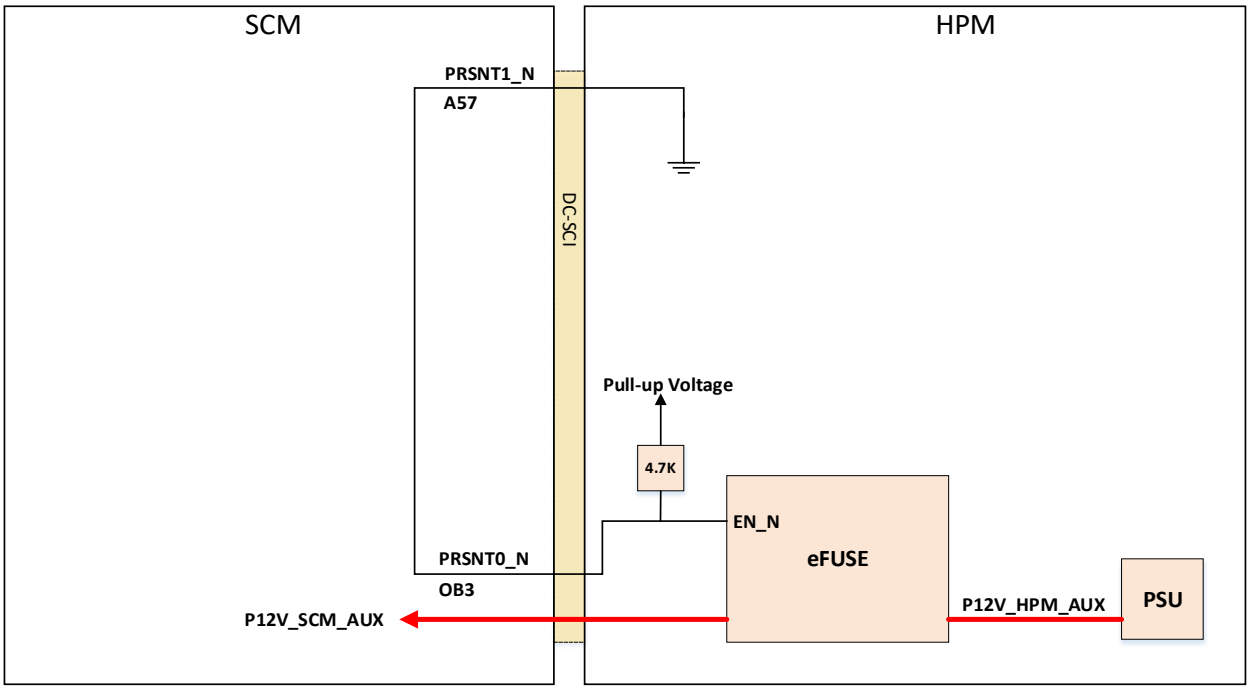


Figure 31: DC-SCM Presence Detection and Power Protection

5 Routing Guidelines and Signal Integrity

5.1 NC-SI

The following section describes the timing requirements that need to be met while routing the NC-SI bus. It defines the portion of the overall propagation delay budget allocated to the HPM and to the DC-SCM, as well as additional requirements for each. HPM and DC-SCM implementers shall analyze their design to ensure the timing budget is not violated.

The traces shall be implemented as 50 Ohm ±15% impedance-controlled nets. HPM and DC-SCM designers are encouraged to follow the guidelines defined in the RMII and NC-SI specifications for physical routing. Figure 32 outlines the NC-SI clock and the data path timing delays on a typical design with the NC-SI bus routed to an OCP NIC 3.0.

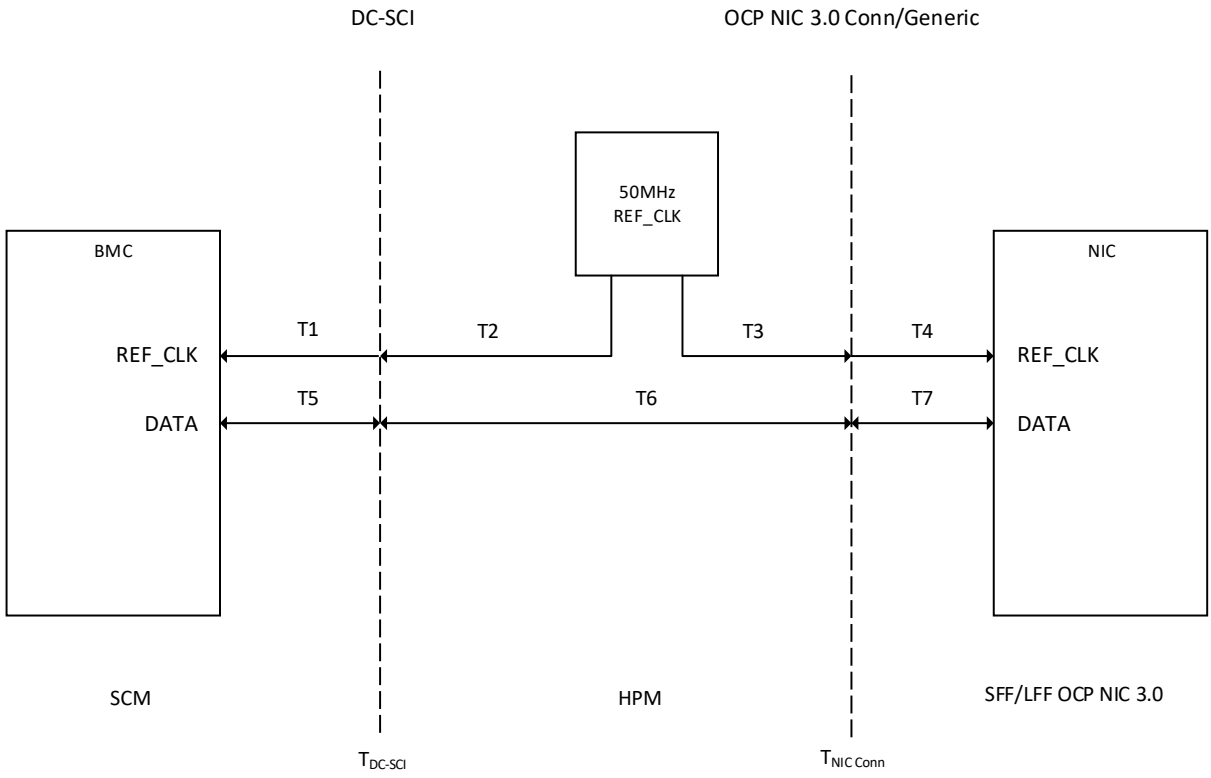


Figure 32: NC-SI Clock and Data Path Timing Delay Topology

Table 24 shows the various timing parameters derived from the NC-SI interface specification (DSP0222) and the OCP NIC 3.0 specification. The propagation delay on the DC-SCM PCB (T5) is assumed to be 680ps.

Table 24: NC-SI Timing Parameters

Parameter	Value	Description
T_{CLK}	20 ns	Period of 50MHz REF_CLK
$T_{CO[max]}$	12.5 ns	Max permissible clock-to-out value per DSP0222
$T_{SU[min]}$	3 ns	Min permissible single ended data setup to REF_CLK rising edge
$T_{SKEW[max]}$	1.5 ns	Max permissible REF_CLK skew between any two devices in the system

$T_{PD,Budget}$	3000 ps	Total propagation delay between BMC and the target ASIC
$T_{NIC,SFF}$(T7)	900 ps	Max permissible propagation delay for an SFF OCP NIC 3.0 card
$T_{NIC,LFF}$(T7)	1350 ps	Max permissible propagation delay for an LFF OCP NIC 3.0 card
T_{SCM} (T5)	680 ps	SCM propagation delay
$T_{DC\ SCI}$	110 ps	Typical propagation delay over the DC-SCI connector
$T_{NIC\ Conn\ Straddle}$	110 ps	Typical propagation delay over an OCP NIC 3.0 Straddle Connector
$T_{NIC\ Conn\ RA}$	130 ps	Typical propagation delay over an OCP NIC 3.0 Right Angle Connector

5.1.1 NC-SI Data Timing

Based on the values in Table 24 , the data timing budget from the BMC to the NIC ASIC is 3 ns as shown in the formula below. Note that the hold time is guaranteed by the RMII spec.

$$Timing\ Budget = T_{CLK} - T_{CO[max]} - T_{SU[min]} - T_{SKEW[max]}$$
$$= 20\ ns - 12.5\ ns - 3\ ns - 1.5\ ns = 3\ ns$$

This maximum allowable propagation delay on the data lines from the BMC to each NIC is shared across the DC-SCM (T5), HPM (T6), and the OCP NIC (T7) boards as shown Figure 32 . Considering the connector propagation delays, the following requirement shall be met for the total propagation delay:

$$T5 + T_{DC\ SCI} + T6 + T_{NIC\ Conn} + T7 < 3000\ ps$$

The Table 25 below calculates the typical data signal timing budget on an HPM (T6) using LFF and SFF OCP NIC 3.0 cards, based on values in Table 24.

Table 25: NC-SI Board Timing Budget

	Max SCM Delay (T5)	Max NIC Card Delay (T7)	Max HPM Delay ($T_{DC\text{-}SCI}$ + T6 + $T_{NIC\ Conn}$)
NIC-LFF	680 ps	1350 ps	970 ps
NIC-SFF	680 ps	900 ps	1420 ps

5.1.2 NC-SI Clock Timing

The maximum clock skew ($T_{SKEW[max]}$) between the reference clocks, as specified in DSP0222, is noted in Table 24. The critical delays are shown in Figure 32 as T1, T2, T3, and T4. The following equation summarizes the skew requirement.

$$|(T1 + T_{DC\ SCI} + T2) - (T3 + T_{NIC\ Conn} + T4)| \leq T_{SKEW[max]}$$

$$|(T1 + T_{DC\ SCI} + T2) - (T3 + T_{NIC\ Conn} + T4)| \leq 1500\ ps$$

5.2 SGPIO

The following section describes the timing requirements that need to be met while routing the SGPIO bus. Data Out (DO) is clocked out by DC-SCM CPLD on the rising edge of SGPIO clock and the Data In (DI) is clocked into the DC-SCM CPLD on the falling edge of the SGPIO clock.

Figure 33 shows the timing constraint on the critical path involving Data In (DI).

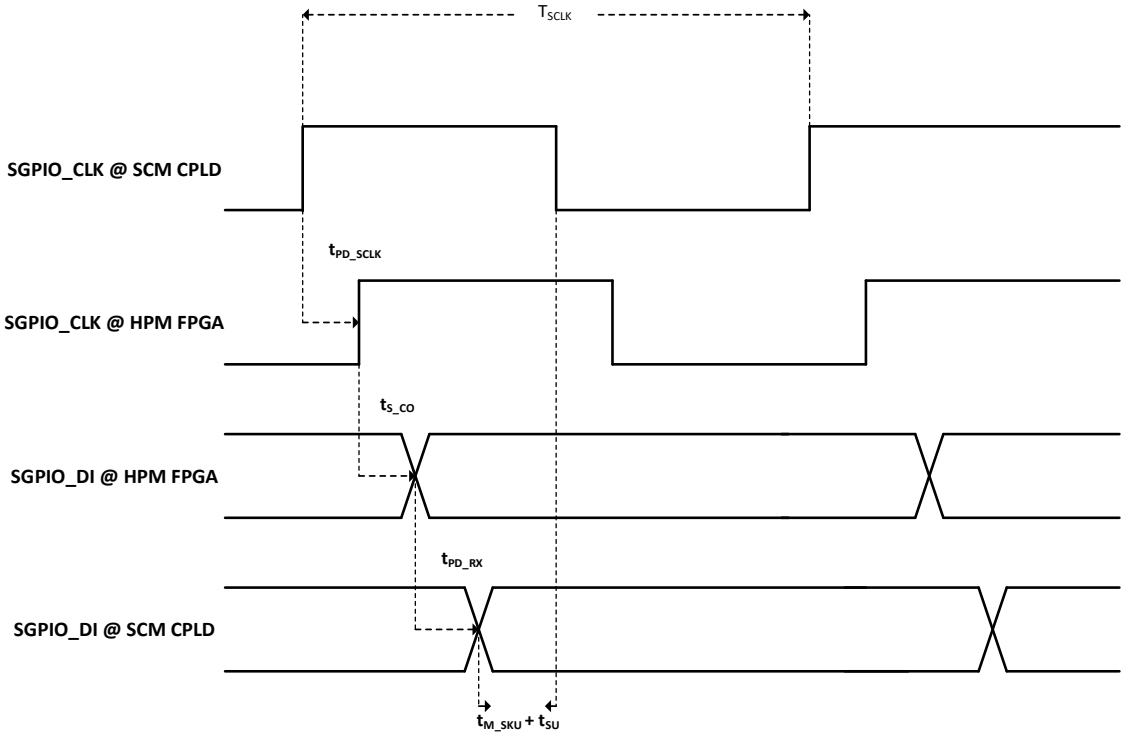


Figure 33: SGPIO Data Input Timing

Table 26 describes the timing parameters.

Table 26: SGPIO timing parameters

Symbol	Description
T_{SCLK}	Period of the interface clock (half the period bounds the critical transaction)
t_{PD_SCLK}	Total PCB propagation delay of SGPIO_CLK from DC-SCM CPLD to HPM FPGA
$t_{PD\_SCLK\_SCM}$	PCB propagation delay of SGPIO_CLK on DC-SCM
$t_{PD\_SCLK\_HPM}$	PCB propagation delay of SGPIO_CLK on HPM
t_{S_CO}	Clock to out delay on HPM FPGA
t_{PD_RX}	Total PCB propagation delay of SGPIO_DI from HPM FPGA to DC-SCM CPLD
$t_{PD\_RX\_SCM}$	PCB propagation delay of SGPIO_DI on DC-SCM
$t_{PD\_RX\_HPM}$	PCB propagation delay of SGPIO_DI on HPM
t_{M_SKU}	Maximum internal clock skew on DC-SCM CPLD
t_{SU}	Set up time for DC-SCM CPLD input

$$t_{PD\_SCLK} = t_{PD\_SCLK\_SCM} + t_{PD\_SCLK\_HPM}$$

$$t_{PD\_RX} = t_{PD\_RX\_SCM} + t_{PD\_RX\_HPM}$$

Bounding maximum total propagation delay for SGPIO_CLK and SGPIO_DI on DC-SCM and HPM each to 1 ns,

$$t_{PD\_SCLK} = t_{PD\_RX} = 2 \text{ ns}$$

The sum of the delays needs to be less than half the period of the clock:

$$t_{PD\_SCLK} + t_{S\_CO} + t_{PD\_RX} + t_{M\_SKU} + t_{SU} \leq \frac{T_{SCLK}}{2}$$

Substituting with typical values from the Lattice MachX02 family datasheet,

$$t_{PD\_SCLK} + 8\ ns + t_{PD\_RX} + 1\ ns + 0.25\ ns \leq \frac{T_{SCLK}}{2}$$

$$2\ ns + 8\ ns + 2\ ns + 1\ ns + 0.25\ ns = 13.25\ ns$$

A 37MHz clock yields a half period of around 13.5 ns. Given the assumptions noted above, 37MHz is the theoretical upper frequency bound for this SGPIO interface.

5.3 I2C and I3C

For the I2C interfaces, HPM and DC-SCM designers shall follow the System Management Bus (SMBus) Specification, Version 3.0. Refer to this specification for DC characteristics and all AC timings.

For I3C interface, HPM and DC-SCM designers shall follow the MIPI I3C specification v1.1. Refer to this specification for DC characteristics and all AC timings. The total capacitance of the I3C bus on the DC-SCM, including the BMC output pin capacitance, DC-SCM trace capacitance and DC-SCI pin capacitance should be less than 25pF @12.5MHz.

5.4 PCIe

DC-SCM suppliers shall follow the routing guidelines outlined in the PCI Express® Card Electromechanical Specification, while routing the PCIE clock and data lines, in order to meet the impedance, loss and timing requirements.

The DC-SCI provisions for one PCIe Gen 5.0 capable reference clock pair. When supporting two PCIe end points on the DC-SCM, designers can use SRIS/SRNS architecture or add a clock buffer to the DC-SCM to support common clock architecture. DC-SCM designers are recommended to perform signal integrity simulations and analysis to ensure that the clock to the end-points meet the propagation delay and jitter performance requirements specified by the PCI Express® Card Electromechanical Specification.

6 Platform Interoperability

The DC-SCM specification attempts to support full electrical and mechanical interoperability between all DC-SCMs and DC-SCM supported HPMs, within the same HPM/DC-SCM vendor as well as across different vendors. However, it is expected and within the scope of this specification to not have this inter-operability “out-of-the-box” and to require different firmware sets (BMC firmware, DC-SCM CPLD and HPM FPGA firmware) to be loaded in the system to account for differences in processors used, SGPIO mapping, I2C mapping, fan control methods etc, in order to enable interoperability. The DC-SCM spec enables and requires these differences to be accounted for by firmware changes only.

In order to ensure that unused buses and signals are properly terminated on the HPM, Table 27 outlines the required and optional interfaces through the DC-SCI and the expected termination on HPM when unused in the system.

Table 27: Platform Interoperability

Interface Name	Required? (Y/N)	HPM termination if un-used
NC-SI	N	No
ESPI/SSIF	N	No
SGPIO[0:1]	Y	NA
I2C[0:3], I2C[5:12]	N	10K Pull-up to 3.3V STBY level
I2C[4]	Y (HPM FRUID at 0xA0)	NA
I3C[0:3]	N	10K Pull-up to 1.0V STBY/MAIN level
SPI0	N	No
QSPI0	N	No
QSPI1	N	No
USB[1:2]	N	No
PCIe TX/RX	N	No
PCIe Clock	N	No
PECI	N	No
PVCCIO_PECI	N	Connect to 1.0V
UART[0:1]	N	No
JTAG	N	No
P3V3_BAT	N	No
STBY BOOT SEQUENCE SIGNALS	Y	NA
PRSNT[0:1]	Y	NA
All other Misc. signals	N	No

7 Acronyms

For the purposes of the DC-SCM specification, the following acronyms apply:

Acronym	Definition
AIC	Add-in Card
ASIC	Application Specific Integrated Circuit
BGA	Ball Grid Array
BMC	Baseboard Management Controller
BOM	Bill of Materials
CAD	Computer Aided Design
CBB	Compliance Base Board
CEM	Card Electromechanical
CFD	Computational Fluid Dynamics
CFM	Cubic Feet per Minute
CLB	Compliance Load Board
CTD	Chain of Trust for Detection
CTF	Critical to Function
CTU	Chain of Trust for Update
DC-SCM	Data Center Secure Control Module
DC-SCI	Data Center Secure Control Interface
DMTF	Distributed Management Task Force
DRAM	Dynamic Random Access Memory
EDSFF	Enterprise and Datacenter SSD Form Factor
EMI	Electro Magnetic Interference

ESD	Electrostatic Discharge
ESPI	Enhanced Serial Peripheral Interface
EU	European Union
FCC	Federal Communications Commission
FRU	Field Replaceable Unit
I/O	Input / Output
HFF	Horizontal Form Factor
HPM	Host Processor Module
I2C	Inter-Integrated Circuit - two wire serial protocol
I3C	MIPI Alliance Improved Inter-Integrated Circuit – two wire serial protocol
IEC	International Electrotechnical Commission
IPC	Institute for Printed Circuits
IPMI	Intelligent Platform Management Interface
ISO	International Organization for Standardization
LED	Light Emitting Diode
LFF	Large Form Factor
LFM	Linear Feet per Minute
LPC	Low Pin Count bus
MAC	Media Access Control
MC	Management Controller
MCTP	Management Component Transport Protocol
ME	Management Entity
MSA	Multi-source Agreement
NC	No Connect
NC-SI	Network Controller Sideband Interface
NEBS	Network Equipment Building-System
NIC	Network Interface Card
OCP	Open Compute Project
SCM	Secure and Control Module
SRIS	Separate Reference Clocks with Independent Spread-Spectrum Clocking
SRNS	Separate Reference Clocks with No Spread-Spectrum Clocking
SSIF	IPMI SMBus System Interface
VFF	Vertical Form Factor