



OPEN
Compute Project

Datacenter Secure Control Module Specification

Authors:

Microsoft: Priya Raghu, Mark A. Shaw, Mason Possing

Google: Prakash Chauhan, Siamak Tavallaei, Mike Branch

Intel: Johan Van De Groenendaal, Qian Wang, Kasper Wszolek, Yi Zeng, Lumin Zhang

Dell: Tim Lambert, Shawn Dube

Revision History

Version	Date	Notes
0.8	Nov 9 th 2020	Initial public review.
0.95	Dec 2 nd 2020	Feedback Implemented
1.0	March 11 th 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
A	Dec 31 st 2020	DC-SCM 2.0 Initial public review.
A.1	July 2021	DC-SCM2.0 updates using DC-SCM1.0 as base
A.2	Sept 2021	Updates from working group decisions

-

Open Compute Project • DC-SCM Specification

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 BasicSM Version 1.0 – July 19th 2018
- OCP NIC 3.0 Design Specification Version 1.0.9

Trademarks

Names and brands may be claimed as trademarks by their respective companies. I2C® is a trademark of NXP Semiconductor. PCIe® and PCI Express® are the registered trademarks of PCI-SIG. I3C is a trademark of MIPI Alliance, Inc.

Table of Contents

1	Overview	5
1.1	<i>DC-SCM Architecture</i>	6
1.2	<i>Multi-Node Support</i>	7
2	Mechanical	8
2.1	<i>Form Factor Options</i>	8
2.2	<i>Horizontal Form Factor</i>	9
2.2.1	Horizontal Form Factor Dimensions	9
2.2.2	Horizontal Form Factor Keep Out Zones	9
2.2.3	Horizontal Form Factor I/O Faceplate	11
2.3	<i>Vertical Form Factor</i>	12
2.3.1	Vertical Form Factor Dimension Outline	12
3	Interface Definition	17
3.1	<i>DC-SCI Card Edge Connector Definition</i>	17
3.2	<i>Gold Finger Plating Requirements</i>	18
3.3	<i>HPM Connector Definition</i>	18
3.3.1	Straddle Mount Connector	18
3.3.2	Right Angle Connector	20
3.3.3	Vertical Connector	21
3.4	<i>DC-SCI Pin Definition</i>	21
3.5	<i>DC-SCI Signal Descriptions</i>	22
3.5.1	NC-SI	22
3.5.2	ESPI/SSIF <<<SSIF is “just another I2C” so it should not be included in this chapter...and FYI SSIF requires an alert signal ...assumed virtual?>>>>	22
3.5.3	LTPI (LVDS Tunneling Protocol & Interface)	23
3.5.4	I2C <<<TO DO....update for bus counts, voltages, protocols)	36
3.5.5	I3C	38
3.5.6	SPI	38
3.5.7	USB	39
3.5.8	PCIe	41
3.5.9	PECI	42
3.5.10	JTAG	42
3.5.11	Standby Power and Boot Sequence	43
3.5.12	Battery Voltage	46
3.5.13	Miscellaneous Signals	46
4.1	<i>Input Voltage, Power, and Current</i>	47

4.2	<i>SCM Presence Detection and Power Protection</i>	47
5	Routing Guidelines and Signal Integrity	48
5.1	<i>NC-SI</i>	48
5.1.1	NC-SI Data Timing	50
5.1.2	NC-SI Clock Timing	51
5.2	SGPIO	51
5.3	<i>I2C and I3C</i>	53
5.4	<i>PCIe</i>	53
6	Platform Interoperability	53
7	Acronyms	54

List of Figures

Figure 1. DC-SCM Example Block Diagram	7
Figure 2: Horizontal Form Factor Dimensions	9
Figure 3. HFF Keep Out Zone – Top View	10
Figure 4. HFF Keep Out Zone – Bottom View	11
Figure 5: HFF I/O Faceplate	12
Figure 6: Vertical DC-SCM form factor – Option 1	13
Figure 7: VFF Option 1 Backplate with IO Bracket- Low profile bracket	14
Figure 8: VFF Option 1 Backplate with IO Bracket- Full height bracket	15
Figure 9: Vertical Form Factor DC-SCM– Option 2 (Top View)	15
Figure 10: VFF Option 2 (Top View) - Form Factor and Mounting Holes	16
Figure 11: VFF Option 2 (Bottom View) – Form Factor and Mounting Holes	17
Figure 12. FFF Card Edge Connector Dimensions – Top Side (“B” Pins)	17
Figure 13. FFF Card Edge Profile Dimensions	18
Figure 14. FFF Card Edge Connector – Detail D	18
Figure 15. Straddle Mount Connector Dimensions (in mm)	19
Figure 16. Straddle Mount Connector 0mm Offset for 0.062”, 0.093”, and 0.105” HPM PCB	20
Figure 17. Straddle Mount Connector -0.3mm Offset for 0.076” HPM PCB	20
Figure 18. Right Angle Connector Dimensions (in mm)	20
Figure 19. Right Angle Connector Offset	21
Figure 20. Vertical Connector Dimensions (in mm)	21
Figure 21. ESPI Example Block Diagram	25
Figure 22: SGPIO Example Block Diagram	Error! Bookmark not defined.
Figure 23: I2C Example Block Diagram	39
Figure 24: An Example I3C SPD DDR5 Block Diagram	40
Figure 25: SPI Example Block Diagram	42
Figure 26: USB Block Diagram	Error! Bookmark not defined.
Figure 27: UART Example Block Diagram	Error! Bookmark not defined.
Figure 28: JTAG Example Block Diagram	Error! Bookmark not defined.
Figure 29: DC-SCM STBY Sequencing Signals Block Diagram	48
Figure 30: Power and Boot Sequence Diagram	49
Figure 31: DC-SCM Presence Detection and Power Protection	52
Figure 32: NC-SI Clock and Data Path Timing Delay Topology	53
Figure 33: SGPIO Data Input Timing	55

List of Tables

Table 1. Straddle Mount Connector PCB Thicknesses	19
Table 2. Straddle Mount Connector PCB Offsets	19
Table 4: NC-SI Signal Descriptions	22
Table 5: eSPI Signal Descriptions	23
Table 7: Example of LTPI Frame encoding	27
Table 8: Config and State Registers	29
Table 9 Example GPIO Channel Definition	30
Table 10 I2C Channel Buses	31
Table 11 UART Channel Interfaces	32
Table 12: I2C Signal Descriptions	36
Table 15: USB Signal Descriptions	39
Table 21: Power Sequence Signal Descriptions	43
Table 22: Battery Voltage	46
Table 23: RoT IO via DC-SCI	46
Table 25: Interrupts via DC-SCI	46
Table 26: Other Miscellaneous IOs via DC-SCI	46
Table 27: Input Power Requirements	47
Table 28: NC-SI Timing Parameters	49
Table 29: NC-SI Board Timing Budget	50
Table 30: SGPIO timing parameters	52
Table 31: Platform Interoperability	53

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.

The DC-SCM 2.0 is an evolution of original DC-SCM 1.0 specification. The goal is to allow for future scalability and longevity across a few generations of server platforms. It considers that server platforms will drop support for some of legacy requirements in favor of new use cases such as Multi Node support and new manageability solutions based on high-speed interfaces. This requires the DC-SCM spec to allow more flexibility in interface usage and pinout definition. Thus, we introduce the LTPI (Multi-Channel Serial Interface).

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. <<<REPLACE/UPDATE>>>

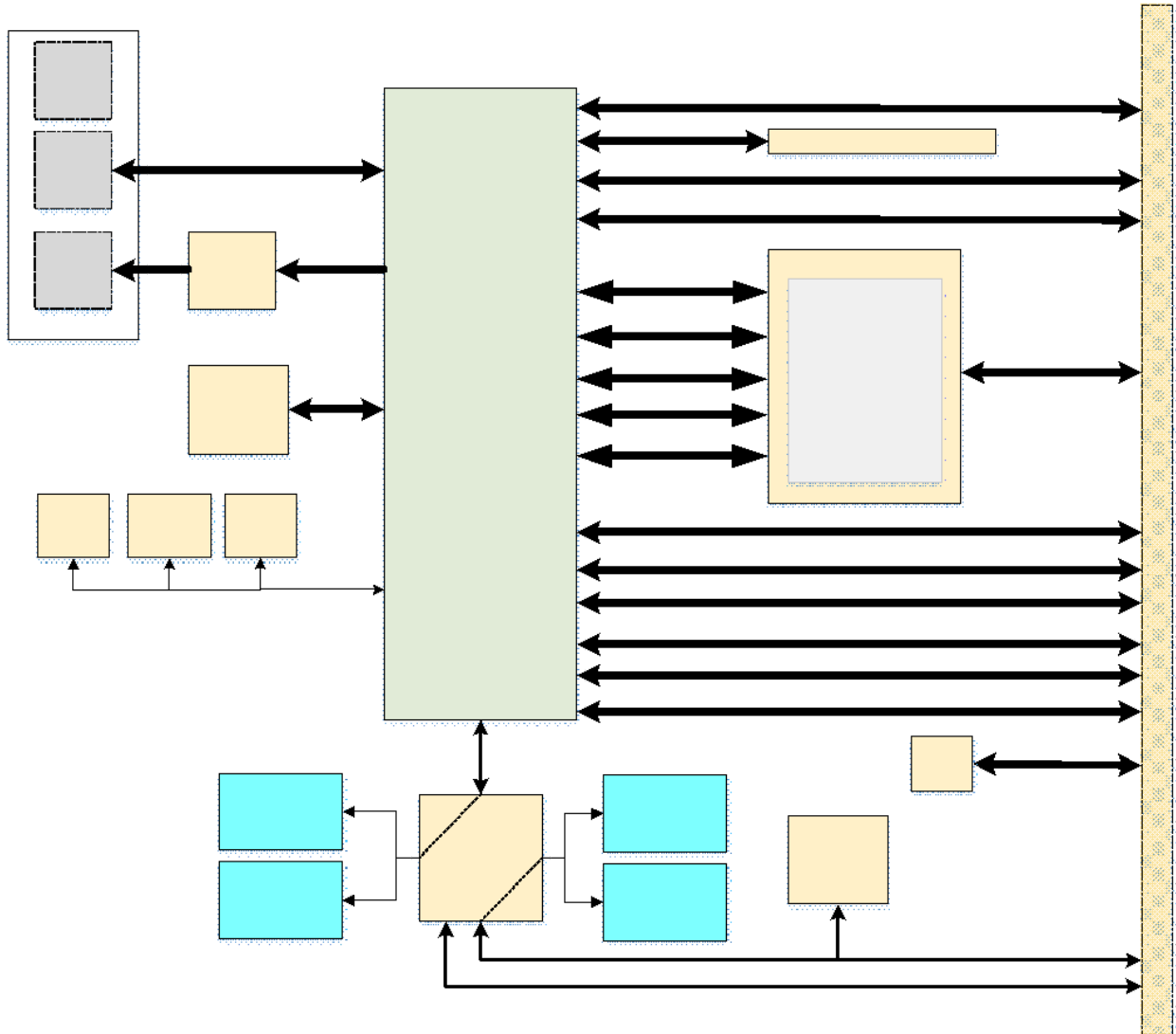


Figure 1. DC-SCM Example Block Diagram

This version of the DC-SCM will incorporate independent node support for server platforms. In this version of the pin definition, the signals are arranged to expand as the number of nodes supported by the system. This is achieved by consolidating various low speed interfaces over the LTPI connection and make pins available for additional interfaces, such as PCIe, ESPI and SPI, which are dedicated to each socket.

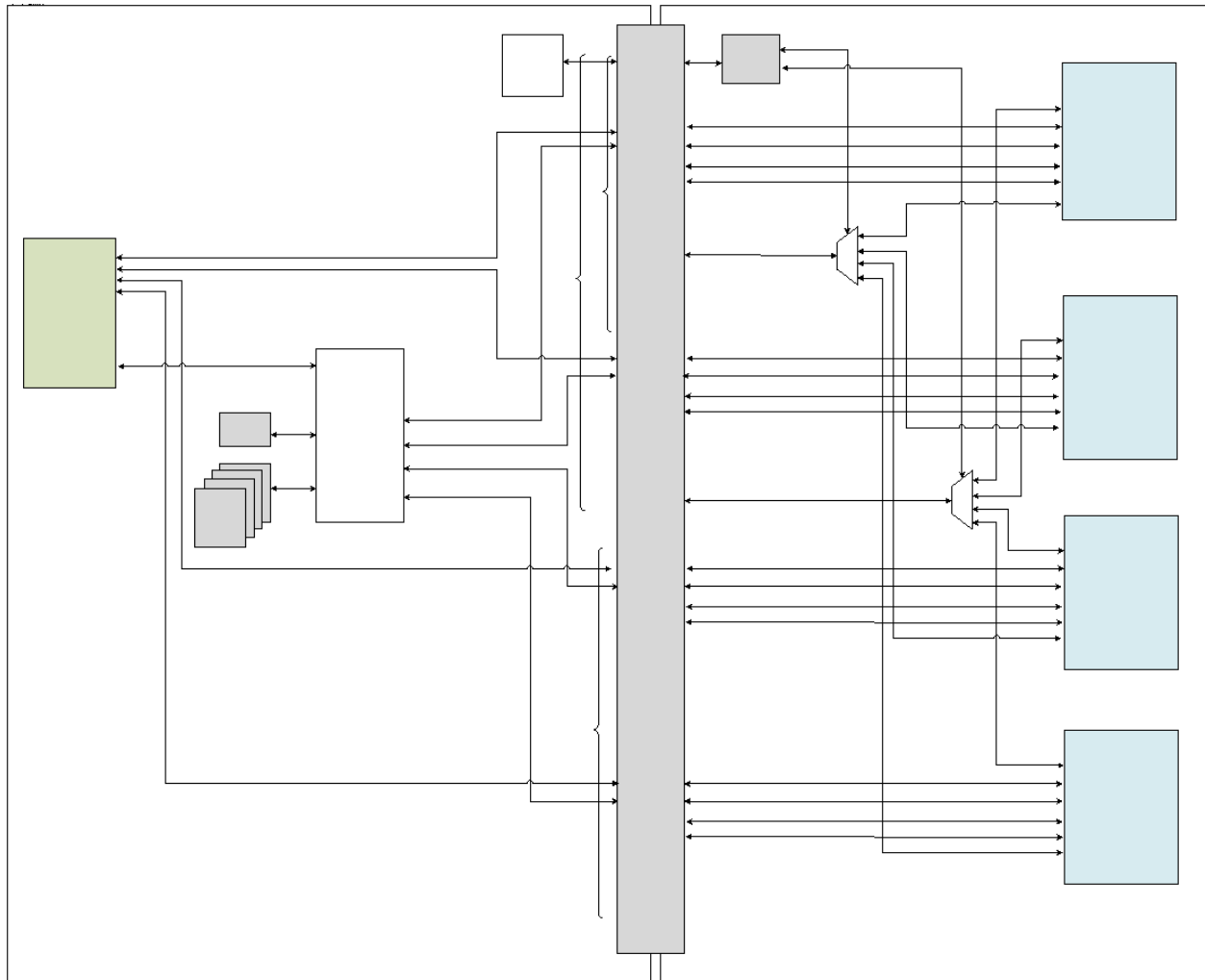


Figure 2. Multi-Node Block Diagram

1 Mechanical

The DC-SCM provides two form factor options:

- Horizontal Form Factor (HFF)
- Vertical Form Factor (VFF)

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 can be customized for individual use cases.

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.

1.4.1 Horizontal Form Factor Dimensions

The Horizontal DC-SCM form factor dimensions are shown in Figure 3.

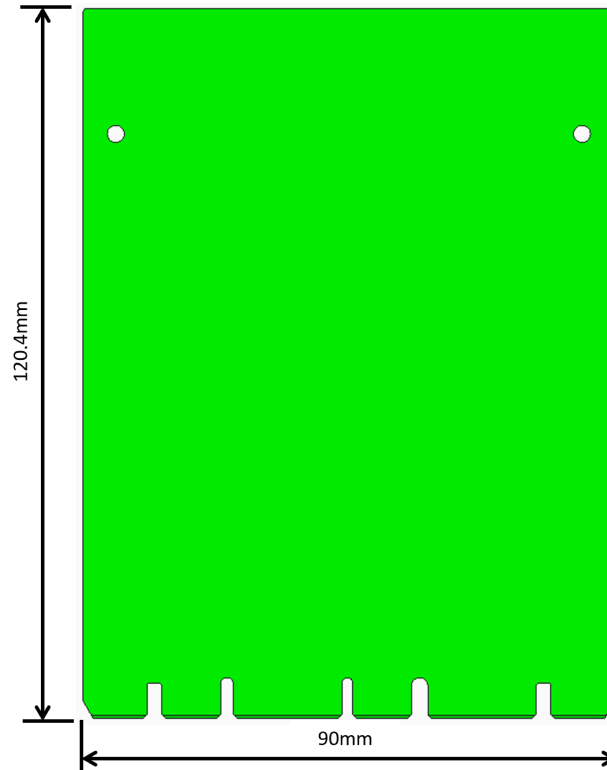
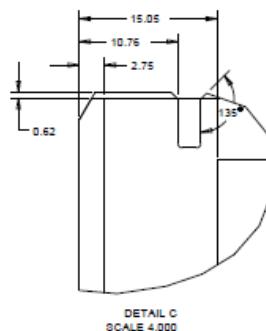
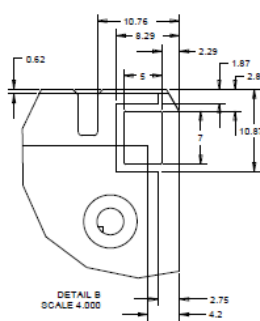
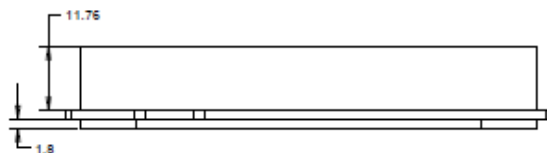


Figure 3: Horizontal Form Factor Dimensions

1.4.2 Horizontal Form Factor Keep Out Zones

The topside “keep-out” zones are shown in Figure 4. The bottom-side “keep-out” zones are shown in Figure 5.



UNLESS OTHERWISE SPECIFIED
DIMENSIONS ARE IN MILLIMETERS
TOLERANCE ON ANGLES $\pm 1^\circ$
.X $\pm$ 0.15 .XX $\pm$ 0.10
INTERPRET DIM AND TOL
PER ASME Y14.5-2009

Figure 4. HFF Keep Out Zone – Top View

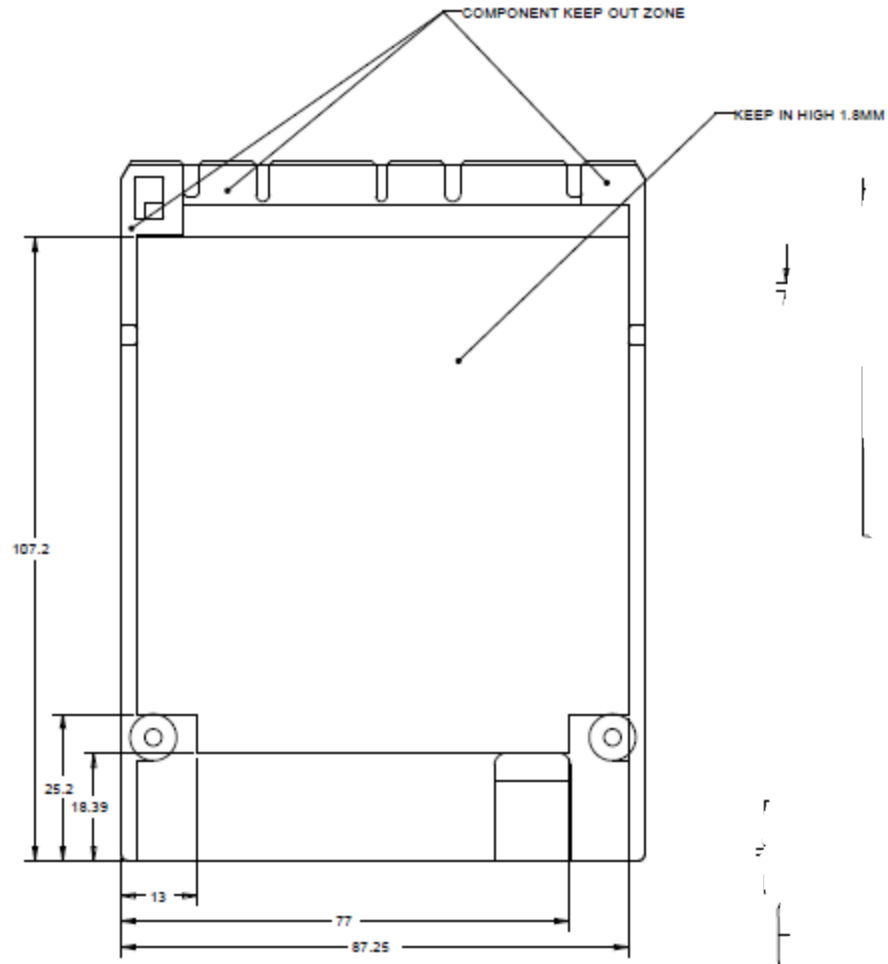
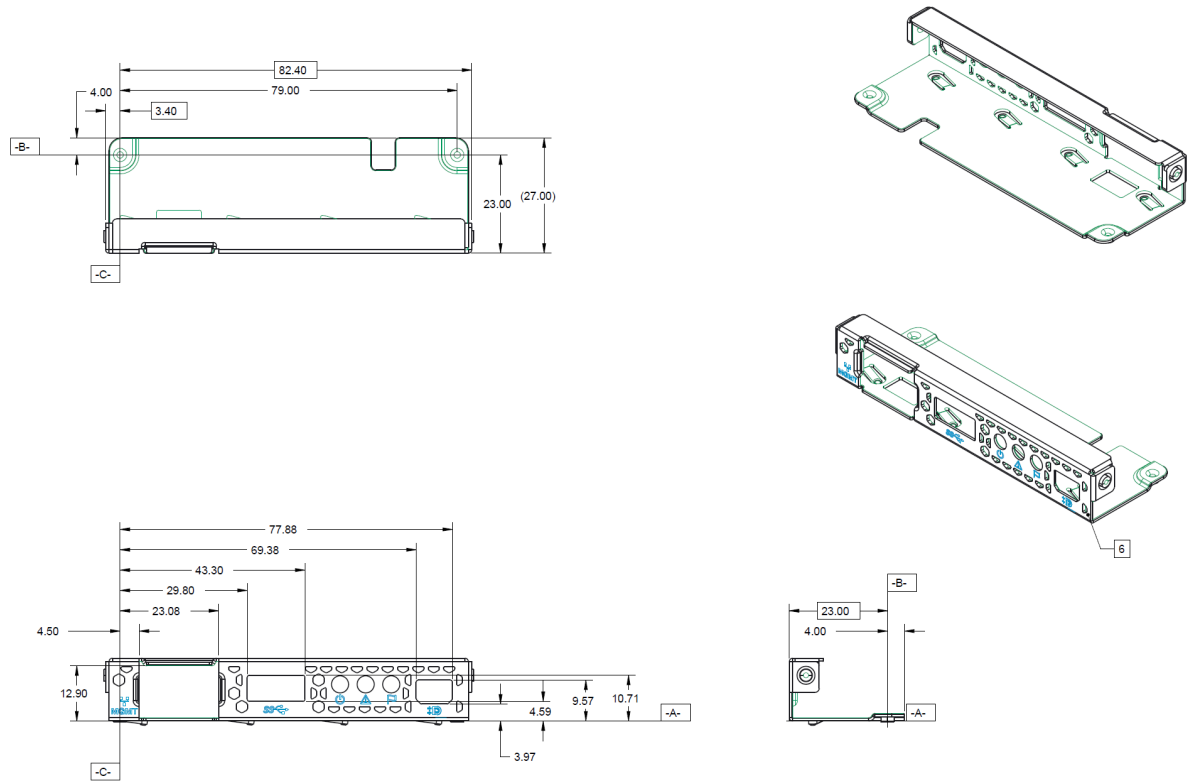


Figure 5. HFF Keep Out Zone – Bottom View

1.4.3 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 6. Note that the face-plate cut outs and perforations shown are examples only and can be customized per system configuration and system airflow requirements.



UNLESS OTHERWISE SPECIFIED
DIMENSIONS ARE IN MILLIMETERS
TOLERANCE ON ANGLES $\pm 1^\circ$
.X $\pm$ 0.15 .XX $\pm$ 0.10
INTERPRET DIM AND TOL
PER ASME Y14.5-2009

Figure 6: HFF I/O Faceplate

1.5.1 Vertical Form Factor Dimension Outline

NOTE: DC-SCM 2.0 makes no modifications to the vertical form factor from version 1.0, inclusive of prevention of plugging a 1.0 vertical card into a 2.0 HPM and vice versa.

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 7, Figure 8, Figure 9 show the mechanical dimensions of a Vertical Form Factor Option 1 DC-SCM.

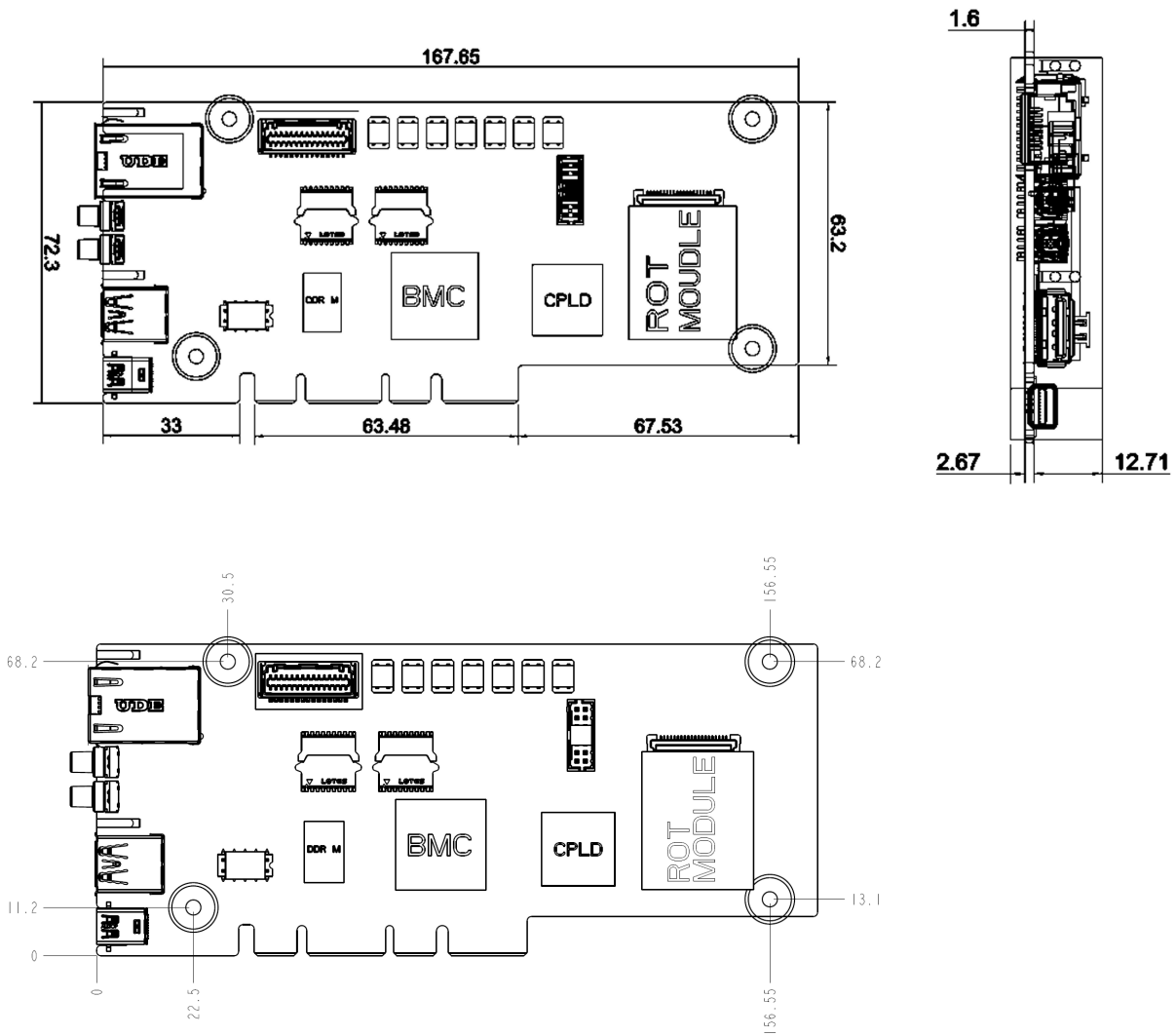


Figure 7: Vertical DC-SCM form factor – Option 1

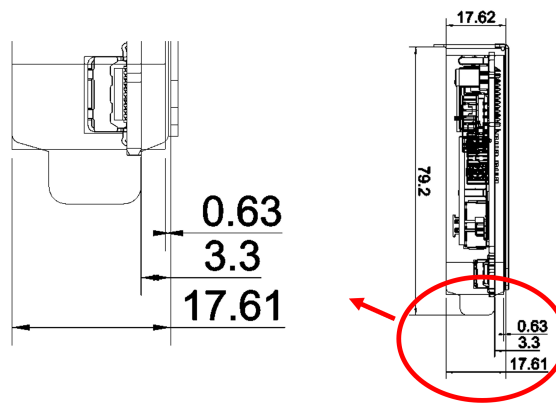
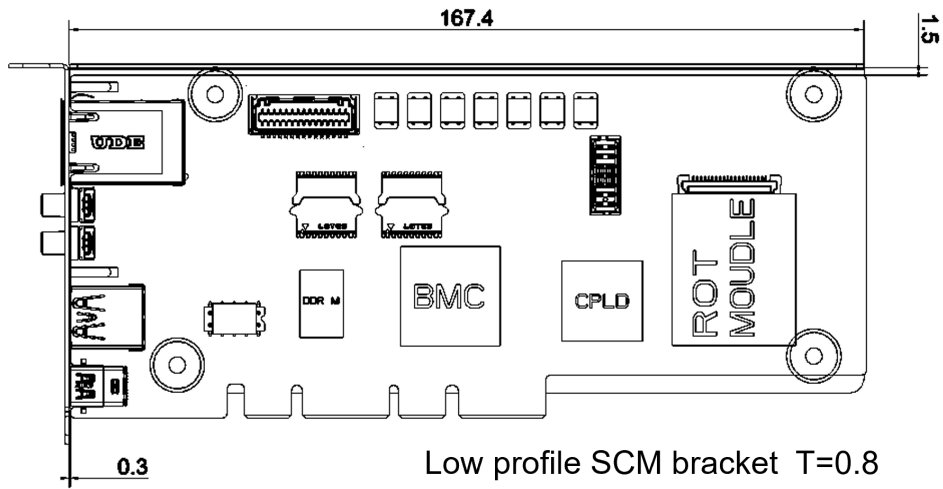
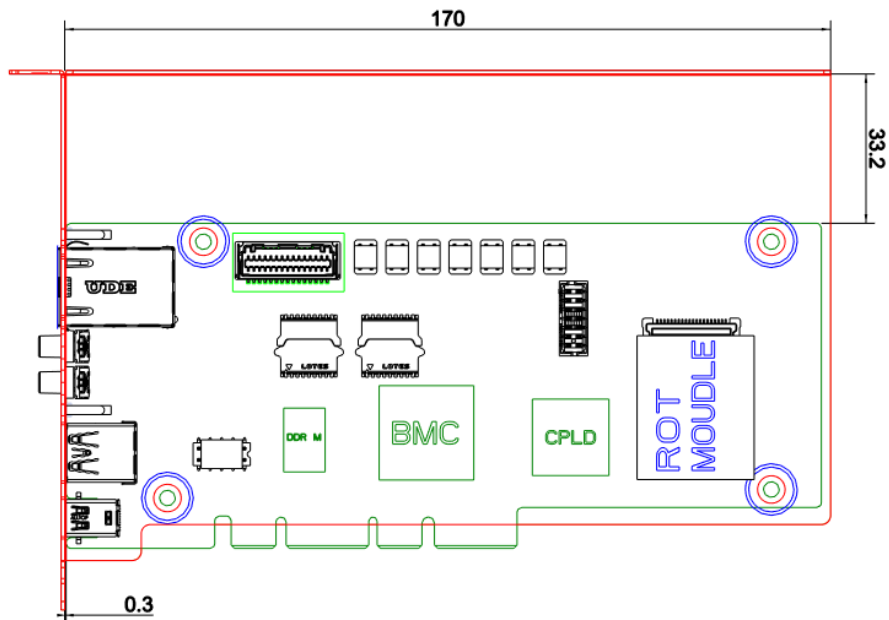


Figure 8: VFF Option 1 Backplate with IO Bracket- Low profile bracket



Full height SCM bracket T=0.8

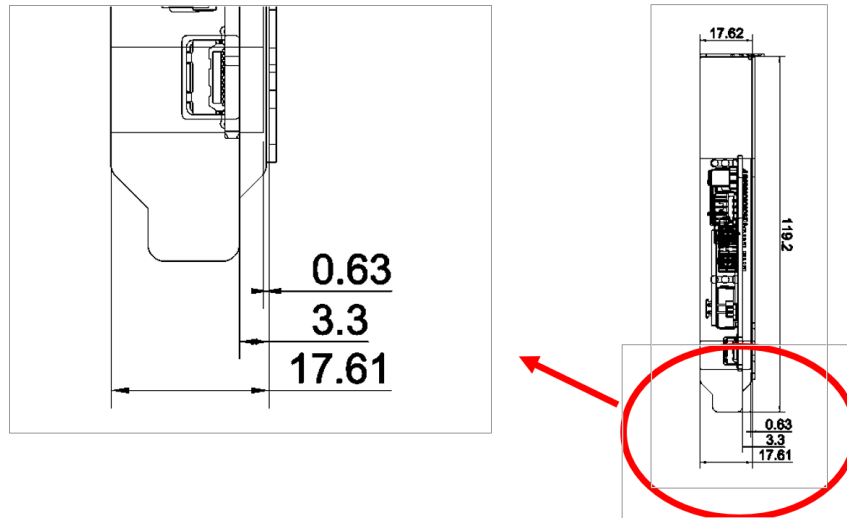


Figure 9: VFF Option 1 Backplate with IO Bracket- Full height bracket

Figure 10, Figure 11 and Figure 12 show the mechanical dimensions of a Vertical Form Factor Option 2 DC-SCM.

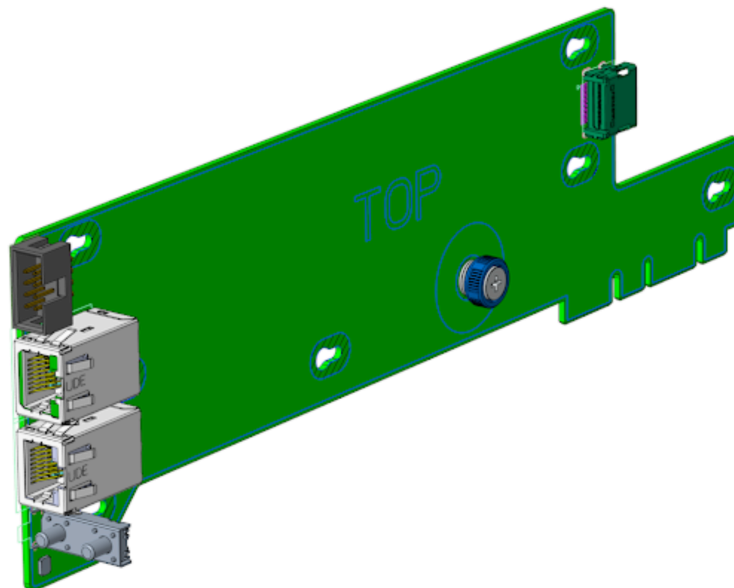


Figure 10: Vertical Form Factor DC-SCM– Option 2 (Top View)

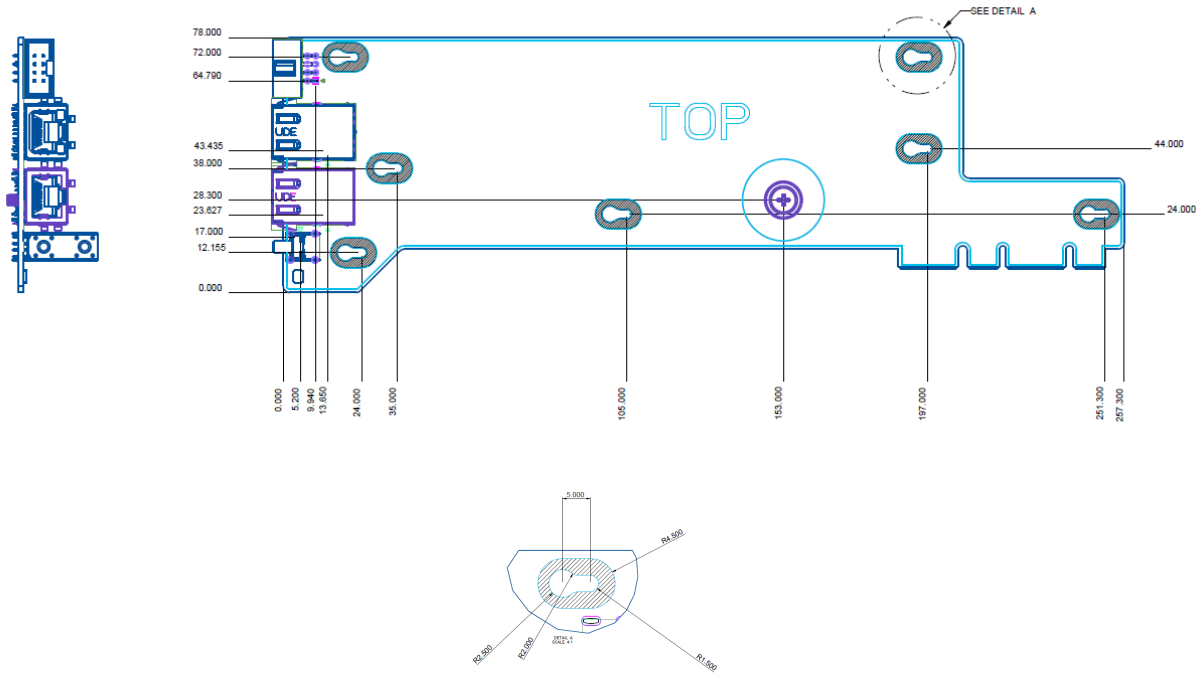
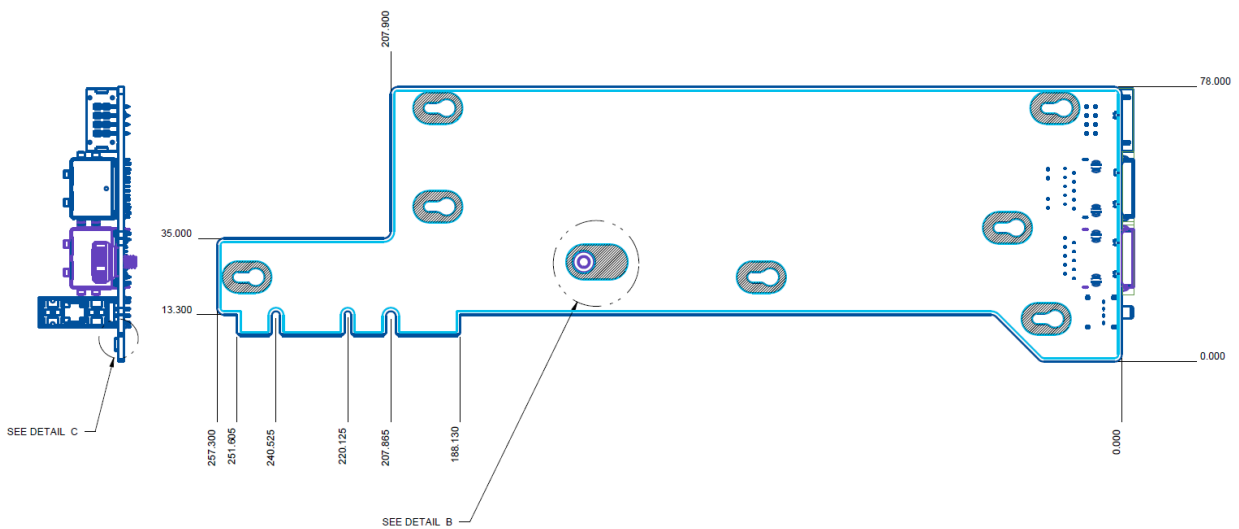


Figure 11: VFF Option 2 (Top View) - Form Factor and Mounting Holes



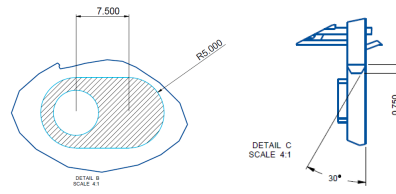


Figure 12: VFF Option 2 (Bottom View) – Form Factor and Mounting Holes

2 Interface 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 NIC devices. The pinout is defined later in this document. Mechanical details of the edge finger requirements are shown in Figure 13, Figure 14, and Figure 15.

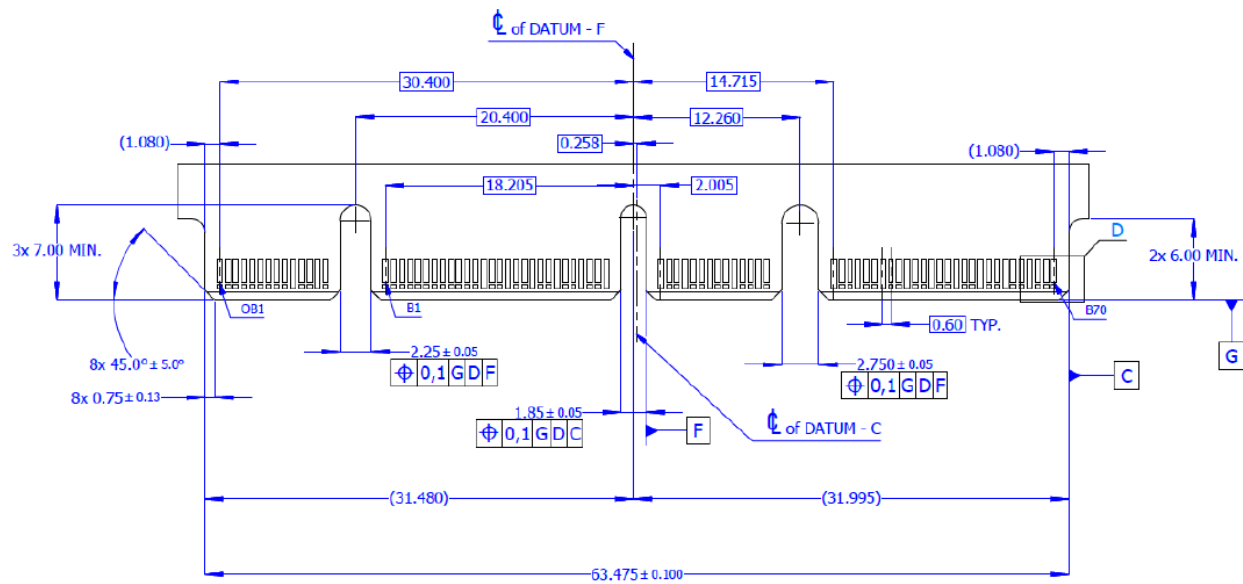


Figure 13. FFF Card Edge Connector Dimensions – Top Side ("B" Pins)

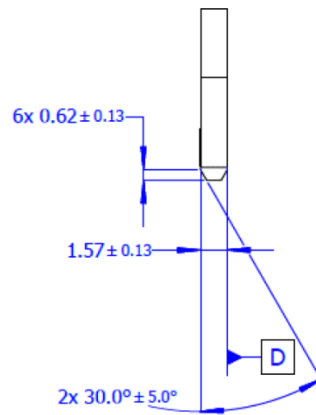


Figure 14. FFF Card Edge Profile Dimensions

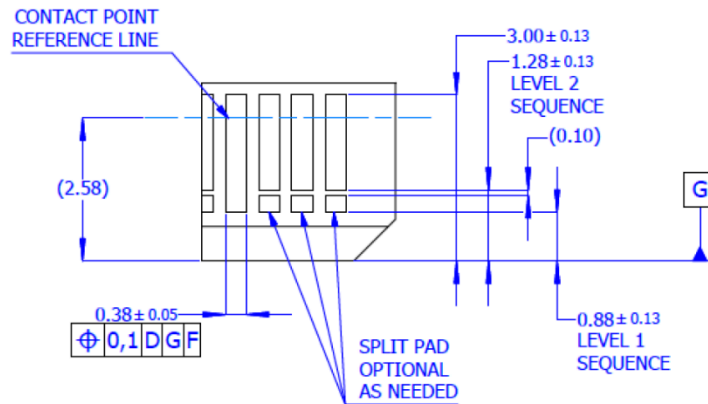


Figure 15. FFF Card Edge Connector – Detail D

1.1 Gold Finger Plating Requirements

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

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.

2.2.1 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 16.

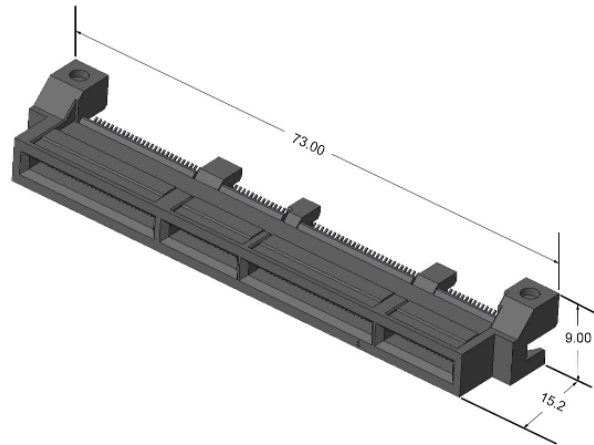


Figure 16. Straddle Mount Connector Dimensions (in mm)

The straddle mount connectors support four HPM PCB thicknesses. The available options are shown in Table 1. PCB thickness must be controlled to within $\pm 10\%$. 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 17 and Figure 18 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)
-----	-----	----------------	----------------

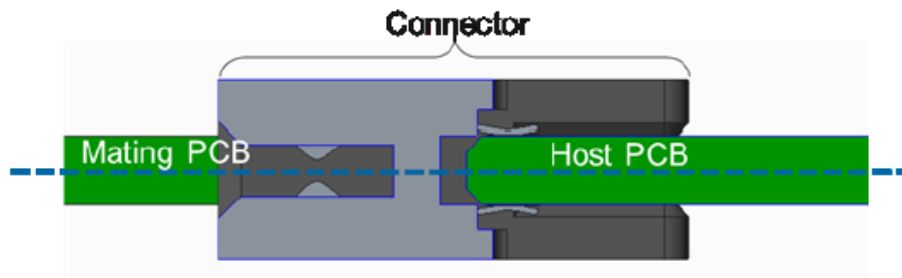


Figure 17. Straddle Mount Connector 0mm Offset for 0.062", 0.093", and 0.105" HPM PCB

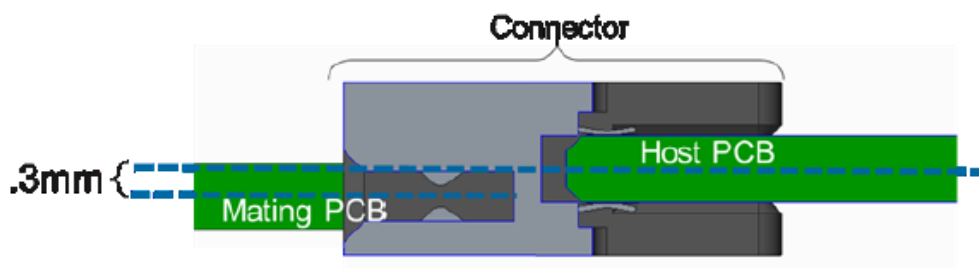


Figure 18. Straddle Mount Connector -0.3mm Offset for 0.076" HPM PCB

2.2.2 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 19.

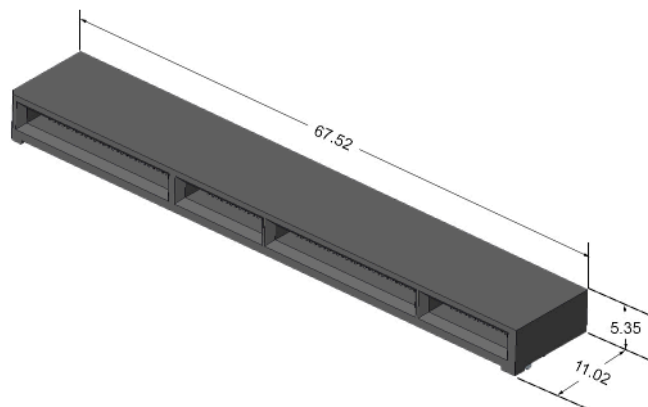


Figure 19. Right Angle Connector Dimensions (in mm)

Figure 20 details the PCB thickness and offset supports for this connector option.

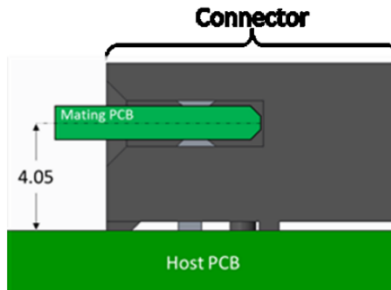


Figure 20. Right Angle Connector Offset

2.2.3 Vertical Connector

Vertical connectors are intended for use in vertical form-factors. The dimensions for the connector are shown in Figure 21.

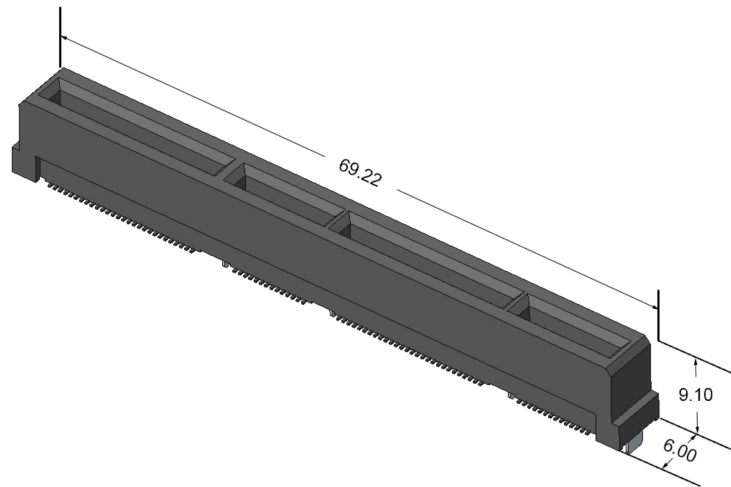


Figure 21. Vertical Connector Dimensions (in mm)

The DC-SCI connector pinlist and pinout are defined in an accompanying spreadsheet. This includes the single name (preferred board net name that include functional and directional nomenclature), gold finger lengths, single node usages, voltage, direction, typical usages and dual node usage.

The contact sequence for each pin indicates 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.

Multi-function DC-SCI pins list the functions in order starting with the most typical expected usage.

When multiple voltages are listed for a signal, they map the respective alternate pin function order.

The detailed signal descriptions are included in the accompanying spreadsheet. The signal names are constructed using the notation of:

function_(bus source)_(signal source)_(signal destination)_Instance#_Partition#_Polarity

Implementers should reference the relevant bus specifications for frequencies, signal integrity aspects and functional details. There is not attempt to duplicate such information here.

2.4.1 NC-SI

The DC-SCI supports up to 2X RMII/NC-SI interfaces from the DC-SCM to the HPM. This enables high speed sideband management to NIC(s). Note: 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 $\pm$ 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

2.4.2 ESPI/SSIF <<<SSIF is “just another I2C” so it should not be included in this chapter...and FYI SSIF requires an alert signal ...assumed virtual?>>>>

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 per partition. There is no LPC bus support. 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_CS1_N	I	1.8	eSPI CS1# from SOC to an optional second endpoint on the DC-SCM
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 22. 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.

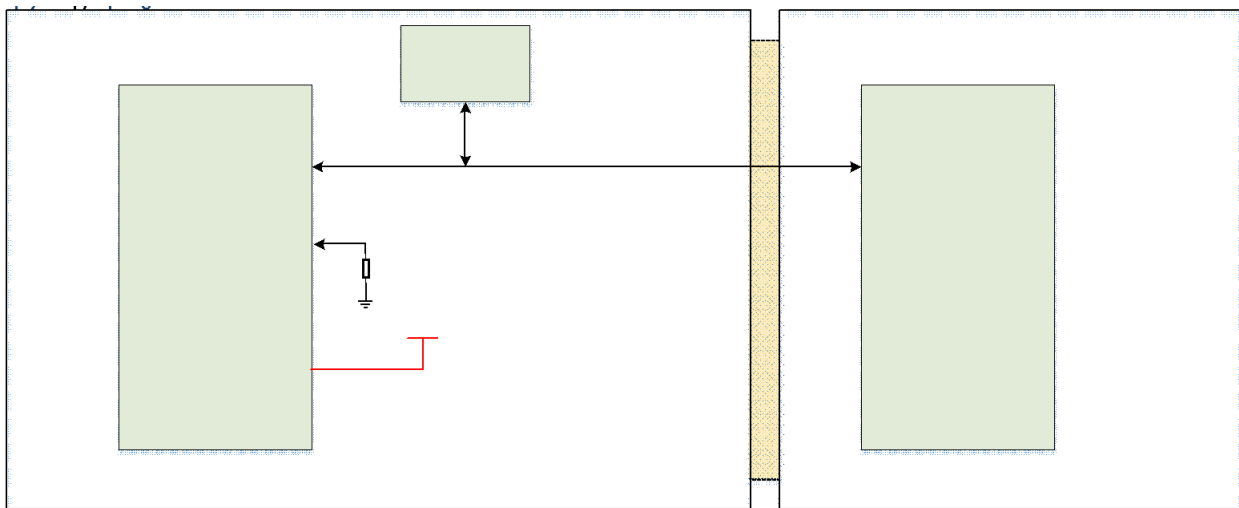


Figure 22. ESPI Example Block Diagram

2.4.3 LTPI (LVDS Tunneling Protocol & Interface)

LTPI is a protocol and interface designed for tunneling various low-speed interfaces between the HPM and SCM. The LTPI protocol goes over the LVDS (Low Voltage Differential Signals) electrical interface on the CPLDs. This is the next generation protocol for DC-SCM 2.0 as the replacement to SGPIO interface. The LVDS interface is faster and provides better scalability than the SGPIO interface allowing for utilization as status and control signals as well as low speed serial interfaces such as SMBus, I2C, UART and additional proprietary OEM interfaces. The DC-SCM 2.0 follows the **[TBD: DC-SCM Cross-PLD LTPI Interface Specification]** specification for implementing the LTPI logical interface.

The LVDS interface can be implemented with two CPLD devices for configurations with BMC devices that do not support LVDS interface (Figure 23):

1. HPM FPGA – providing a bridging of local HPM interfaces to LVDS
2. SCM CPLD – providing an LVDS bridging to local SCM interfaces

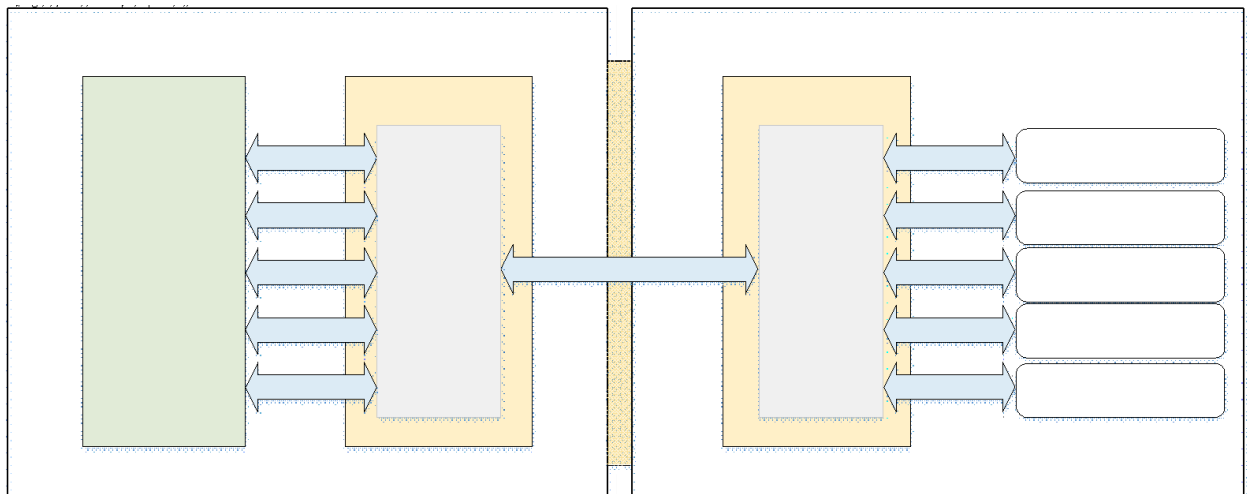


Figure 23 LVDS connection to SCM CPLD.

For configurations with BMC SoC devices supporting LVDS interface compliant with **[TBD: DC-SCM Cross-PLD LVDS Interface Specification]** the SCM CPLD does not need to be implemented and LVDS interface is directly handled by BMC SoC as shown in Figure 24.

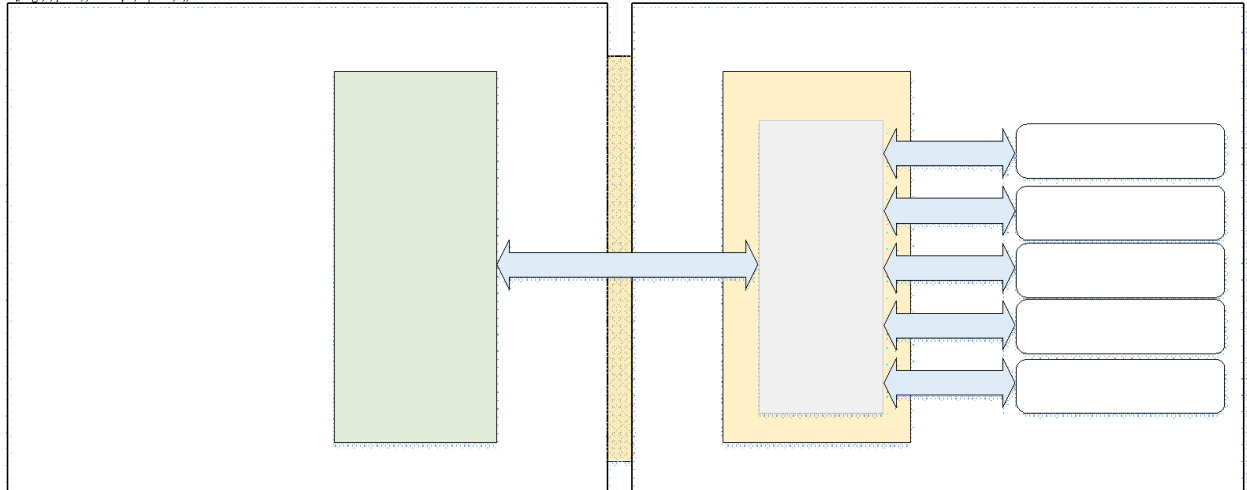
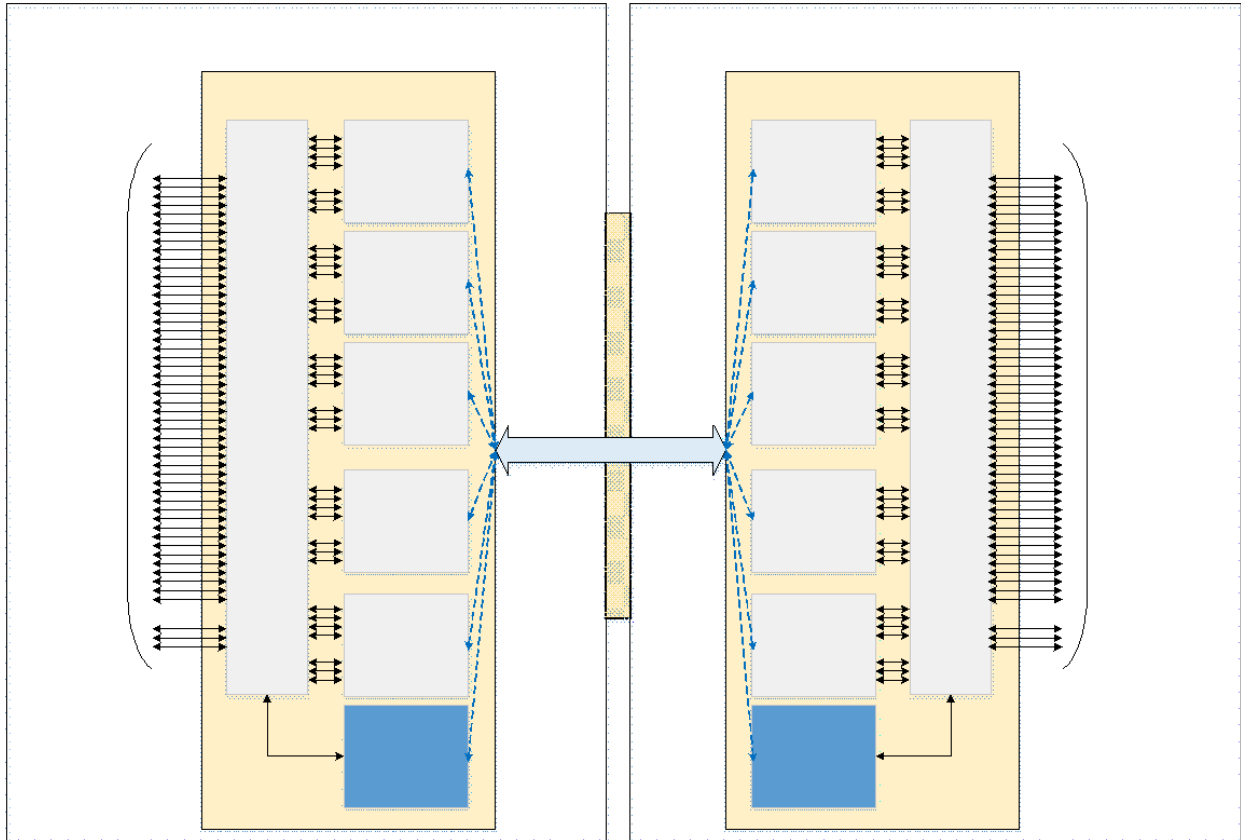


Figure 24 Direct connection of LVDS interface to the BMC.

The LVDS interface in both the HPM FPGA and SCM CPLD implements a concept of channels that are serialized with the LVDS interface ([Figure 25](#)). The assignment of physical board interfaces to the LVDS

channels is done through LVDS channels mapping and allows for design flexibility and inclusion of additional logic if required in specific design. The details of LVDS serialization and channel encapsulation is covered in the [\[TBD: DC-SCM Cross-PLD LVDS Interface Specification\]](#).



[Figure 25 SCM and HPM interfaces mappings via. LVDS](#)

The DC-SCM LVDS interface implements the concept of Time Division Multiplexing of high speed LVDS full-duplex interface to transmit and receive LVDS channels between SCM and HPM. As shown in the Figure 26 each LVDS channel is being provided with a portion of bits in the LVDS Frame transported in each direction. The number of bits assigned to specific channel and how often the frame with given channel is sent depends on the Channel bandwidth requirements.

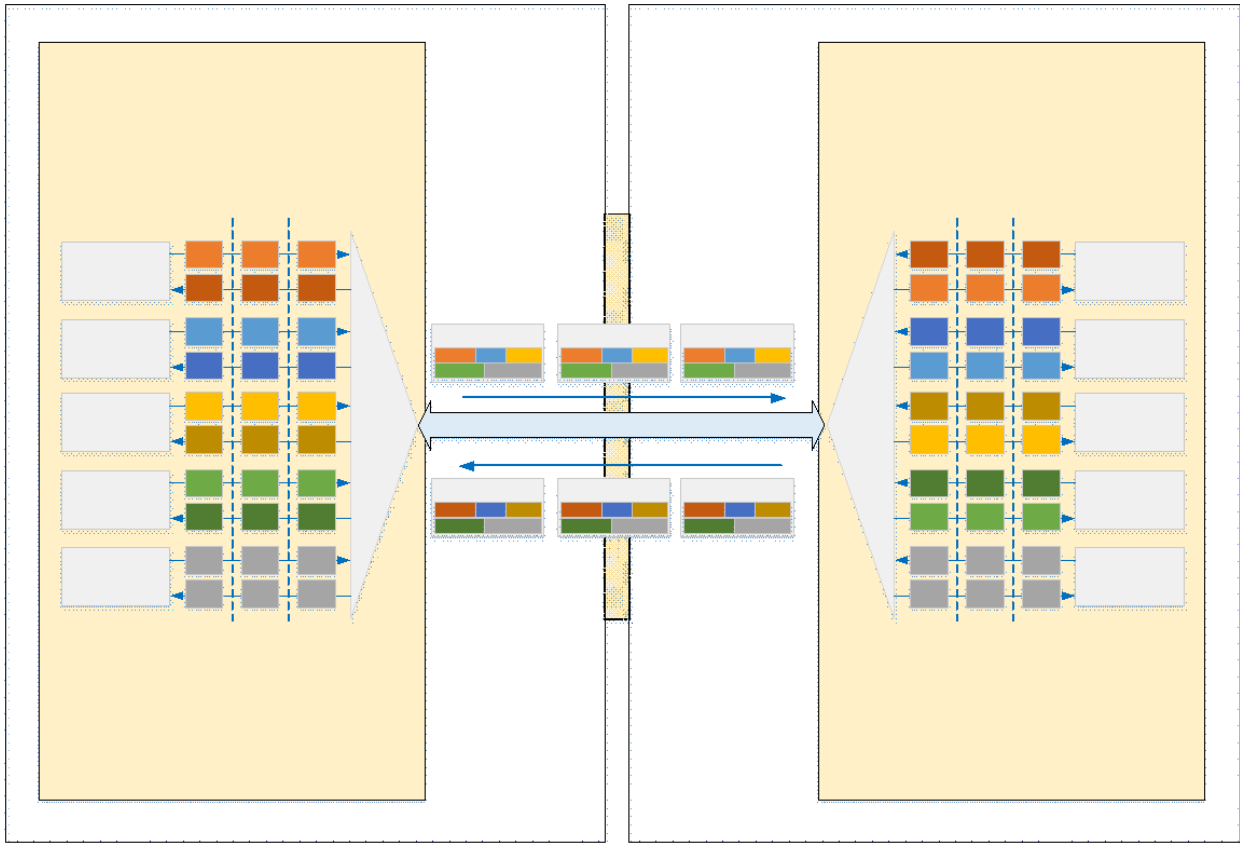


Figure 26 LVDS Channels encapsulation and serialization.

The example LVDS Channels serialization frame definition is shown in the Table 7 below. The details of bit definitions, frame encodings, link setup etc. are covered in the [TBD: DC-SCM Cross-PLD LVDS Interface Specification].

Table 7: Example of LTPI Frame encoding

Frame Offset [bytes]	Size [bits]	Description
0	8	LTPI alignment symbol.
1	8	Frame Count
2	8	Command
3	8	GPIO Channel Low Latency (8 GPIO signals sent every frame)
4	8	GPIO Channel Normal (8 GPIOs from GPIO Channel Group N – N is FrameCount % Maximum N)
5	4	I2C Bus 0
	4	I2C Bus 1
	4	I2C Bus 2
	4	I2C Bus 3
7	4	I2C Bus 4
	4	I2C Bus 5

8	4	UART0
	4	UART1
9	8	OEM
10	8	OEM
11	8	Data Channel
12	8	Reserved
13	8	CRC

The LTPI Channels mapping provides a way to map the LTPI channels to physical interfaces on SCM and HPM modules. Some of the channels might be mapped directly to physical interfaces e.g. GPIO mapped to CPLD/FPGA GPIO or through additional logic converted to other interface like SGPIO with additional SGPIO Logic or a combination of both. The mapping is done in SCM CPLD and HPM FPGA depending on a specific design choice for SCM and HPM. Examples of different interface mapping for GPIO Channels in

SCM and HPM are presented in Figure 27 below. The same mapping concept applies to all LTPI channels and allows the HPM/SCM designer to match specific design needs and limitations.

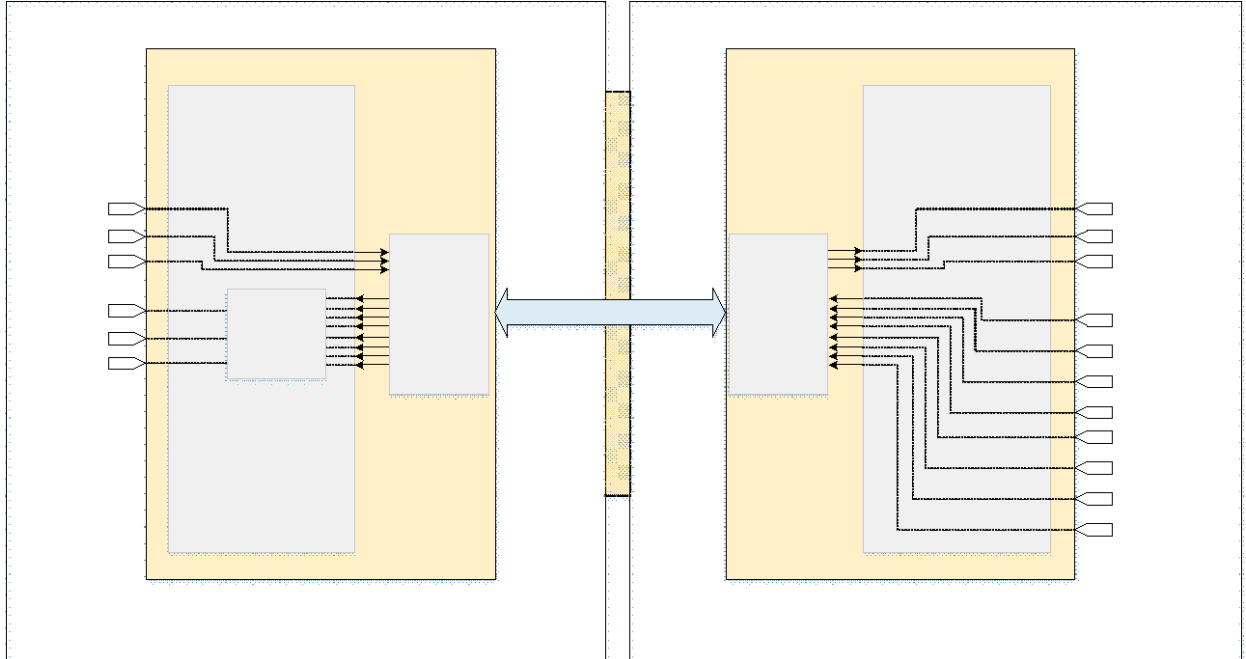


Figure 27 Example mapping of LTPI GPIO Channel to physical GPIOs and SGPIO

The LTPI interface provides a Configuration Space Registers that are mapped between the HPM CPLD and SCM CPLD. The config space is defined as memory mapped registers that BMC can access through OEM-defined interface such as I2C, SPI or proprietary interface. The config space is used for BMC FW to manage the LTPI CPLD in the following scenarios:

1. LTPI interfaces discovery and detection
2. HPM board type discovery and capabilities detection
3. LTPI CPLD status and diagnostics
4. LTPI CPLD update protocol

The example definition of LTPI CSR registers is shown in the Table 8 below. The Dynamic Registers are updated by the LTPI logic during runtime e.g. Status register or Diagnostics Registers. Depending on implementation the configuration registers can be modified by the BMC to allow for LTPI interface parameters modifications e.g. Channel Priority/Bandwidth changes. Those changes require the LTPI Link to be reinitialized for changes to take effect.

Table 8: Config and State Registers

Register	Size	Dynamic	Description
Status	4 bytes	Yes	LTPI Status bits (connection status, self-test results)
Link	4 bytes	Yes	Link information (state, speed, CRC)
HPM Identity	32 bytes	No	HPM Identification Register (GUID, MFR ID, Vendor ID, Board ID, Revision)
SCM Identity	32 bytes	No	SCM Identification Register (GUID, MFR ID, Vendor ID, Module ID, Revision, RoT)
OEM Specific	128 bytes	-	Reserved for OEM Usage
Channel Capabilities	8 bytes	No	Channels supported (GPIO, I2C, etc.)
Channel Properties	64 bytes	Yes*	Channels configuration (Priorities, BW distribution, etc.)
Diagnostics [OEM]	64 bytes	Yes	Configurable diagnostics (errors, data rate, etc.)
Channel GPIO	32 bytes	Yes*	Channel interfaces mapping
Channel I2C	32 bytes	Yes*	Channel interfaces mapping
Channel UART	32 bytes	Yes*	Channel interfaces mapping
Channel Data	32 bytes	Yes*	Channel interfaces mapping
Channel OEM0	32 bytes	Yes*	Channel interfaces mapping
Channel OEM1	32 bytes	Yes*	Channel interfaces mapping
...	...	...	...
Channel OEMn	32 bytes	Yes*	Channel interfaces mapping

*) Changes in registers will require link reset in order to be applied.

The Static CSR registers content is being populated and mapped between SCM and HPM LTPI during the LTPI Interface setup and link bring up phase. For example, the HPM Identity needs to be read by SCM from HPM during LTPI interface bring up. Similarly, the SCM identity is read by HPM LTPI and populated in HPM CSR. The content of HPM and SCM identity registers such as GUID, Vendor ID, Board ID etc. can be either stored in SCM CPLD or HPM FPGA bitstream/internal Flash memory or can be stored in dedicated FRU device on SCM or HPM boards. Example of different CSR registers content population solutions are presented on the **Error! Reference source not found.** below i.e. HPM CSRs are populated based on HPM FRU Memory accessible by I2C.

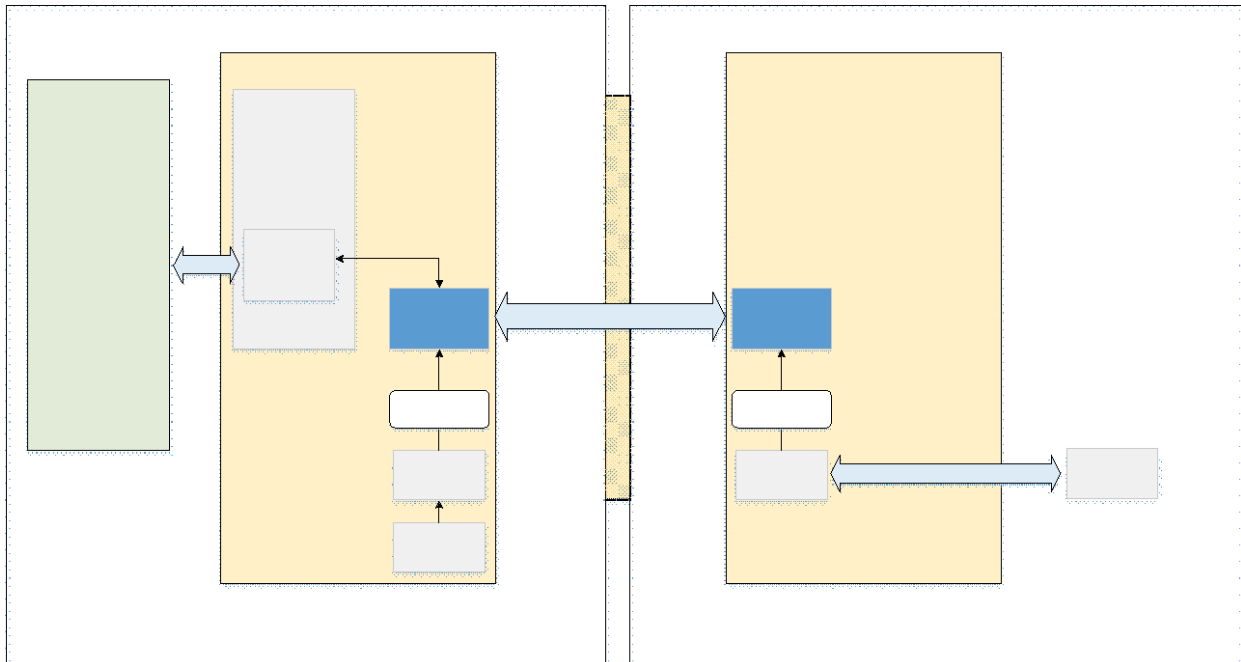


Figure 28 Example mapping of LTPI GPIO Channel to physical GPIOs and SGPIO

The GPIO Channel is used to tunnel low speed HPM GPIO interfaces through LTPI interface. The GPIO channel defines 256 GPIOs. Typical GPIOs used on server platforms are predefined, other GPIOs can be assigned to match a specific OEM design needs.

Table 9 Example GPIO Channel Definition

GPIO#	HPM GPIO Signal	Direction	Description
0	FP_PWR_BTN_I_N	I	
1	FP_PWR_BTN_O_N	O	
2	FP_RST_BTN_I_N	I	
3	FP_RST_BTN_O_N	O	
4	BMC_ONCTL_N	O	
5	SLP_S3_N	I	
6	SLP_S4_N	I	
7	FP_ID_LED_N	O	
8	FP_LED_STS_AMBER_N	O	
9	FP_LED_STS_GREEN_N	O	
10	FP_LED_ID_N	O	
11	FP_NMI_BTN_N	I	
12	FP_ID_BTN_N	I	
13	FORCE_BMC_UPDATE_N	I	
14	INTRUDER_N	I	
15	BMC_SPEAKER	O	
16-35	I2C_[0...19]_ALERT_N	I	
36-43	FAN_PRSTN_[0...7]_N	I	
44-51	FAN_PWM_[0...7]_N	O	
52-59	FAN_TACH_[0...7]_N	I	
60-67	CPU_[0...7]_ERR0_N	I	
68-75	CPU_[0...7]_ERR1_N	I	
76-83	CPU_[0...7]_ERR2_N	I	
83-127	Reserved	I/O	Reserved for future use
127-255	OEM	I/O	OEM defined

The I2C Channel is used to tunnel I2C buses through LTPI interface for the links where SCM is the only Master. The I2C channel defines 64 I2C Buses. The Table 10 shows the mapping of I2C buses to I2C Channel buses.

Table 10 I2C Channel Buses

I2C Bus#	HPM GPIO Signal	Direction	Description
0-19	I2C_[0...19]	I/O	I2C Bus 0 to 19
20-31	Reserved	I/O	Reserved for future use
32-63	OEM	I/O	OEM defined

The HPM I2C buses with Slave devices are being tunneled through LTPI interface and I2C signals are reconstructed on SCM side. As shown in **Error! Reference source not found.** below from BMC perspective the I2C buses are accessible exactly the same as if they were physically routed through SCI interface.

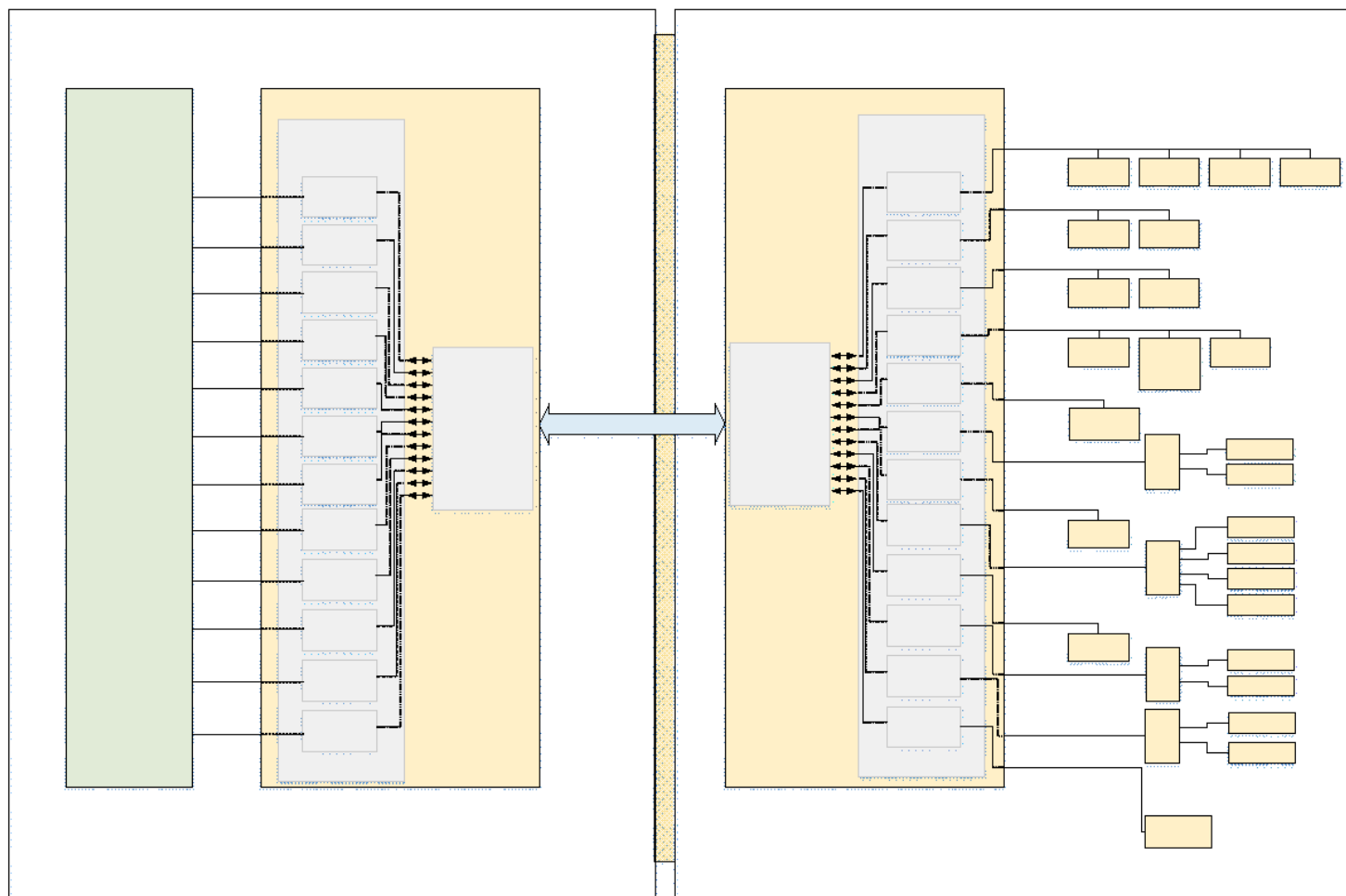


Figure 29 Example mapping of I2C Channel to physical I2C buses on HPM

The UART Channel is used to tunnel HPM physical UART interfaces through LTPI. The UART Channel supports tunneling up to 8 UART interfaces.

Table 11 UART Channel Interfaces

UART#	HPM GPIO Signal	Direction	Description
0-7	UART_[0...7]	I/O	UART Interface 0 to 7

Similar to I2C Buses the UART interface is tunneled through LTPI and reconstructed into physical UART interface. As shown in the Figure 30 below the UART interfaces can be connected to BMC or USB-UART Bridge following specific design choices of HPM and SCM modules.

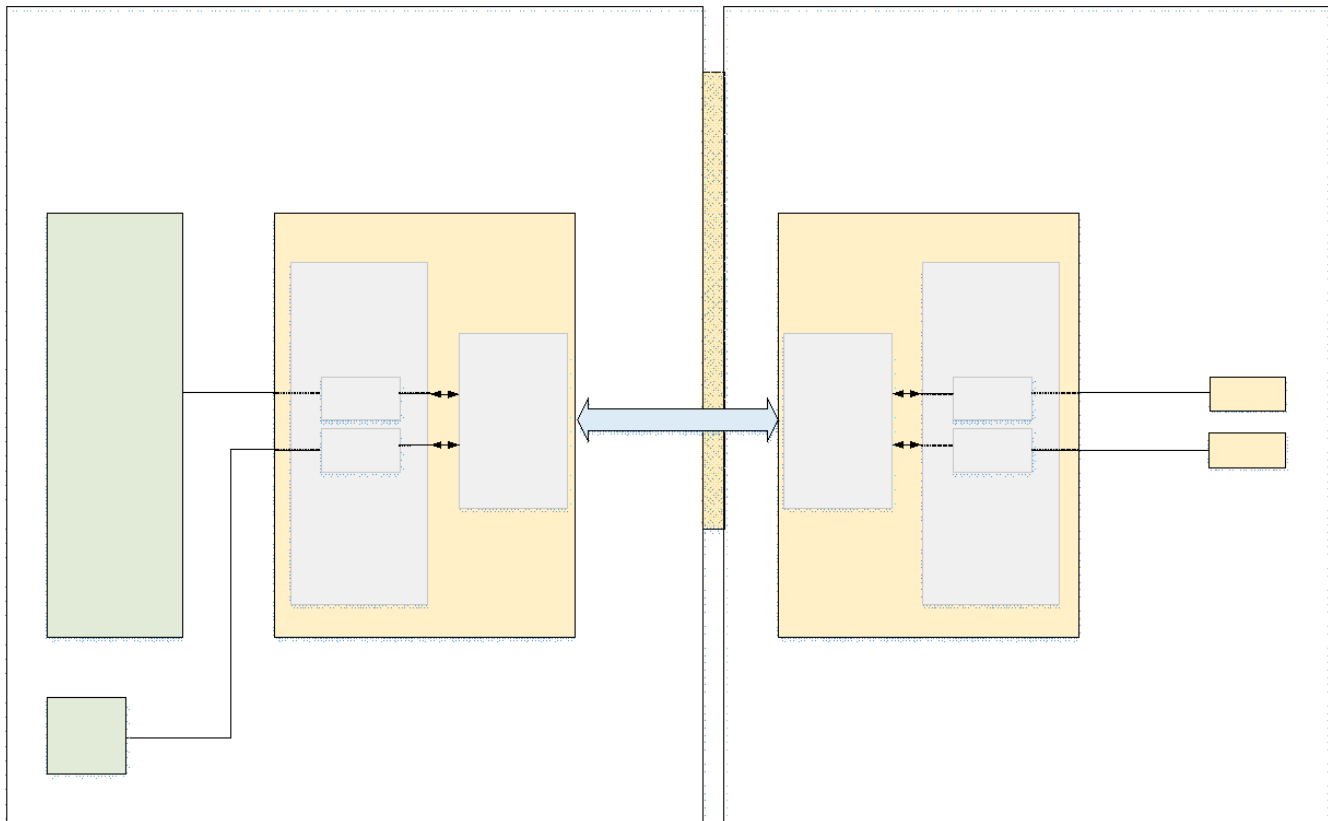


Figure 30 Example mapping of UART Channel to physical UART interfaces on HPM and SCM

The OEM LTPI Channels allows for OEM Specific interface implementation. The OEM can implement proprietary interface tunneling via LTPI by following the same approach as used in other Channels. It is out of scope of this specification to define the OEM-specific interface details. OEM Channels is only defined as placeholder for OEM extension and proprietary interfaces implementation using DC-SCM LTPI.

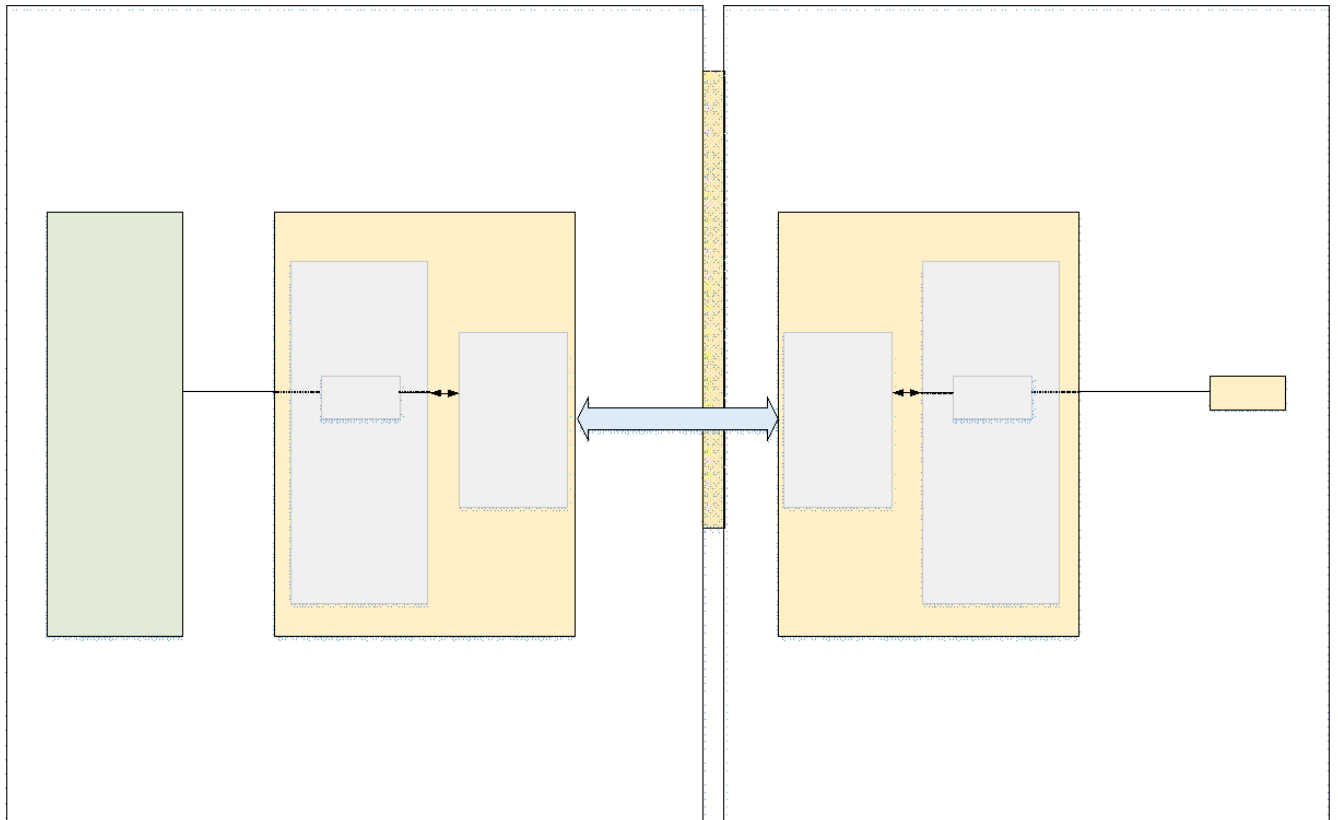


Figure 31 Example of OEM Channel usage for tunneling OEM-specific interface

The Data Channel allows for tunneling of Data between SCM CPLD and HPM FPGA via LTPI. This adds a flexibility and possibility to implement LTPI extensions to match specific design needs. The Data Channel follows a concept of a Memory Mapped Interfaces such as Avalon Memory Mapped (AVMM). As shown in the example in the Figure 32 below the Data Channel implements an internal AVMM bus that allows

for mapping Memory Spaces between SCM CPLD and HPM FPGA and use of standardized IP blocks that follows AVMM. Other Data Channel implementations might use different Memory Mapped interfaces.

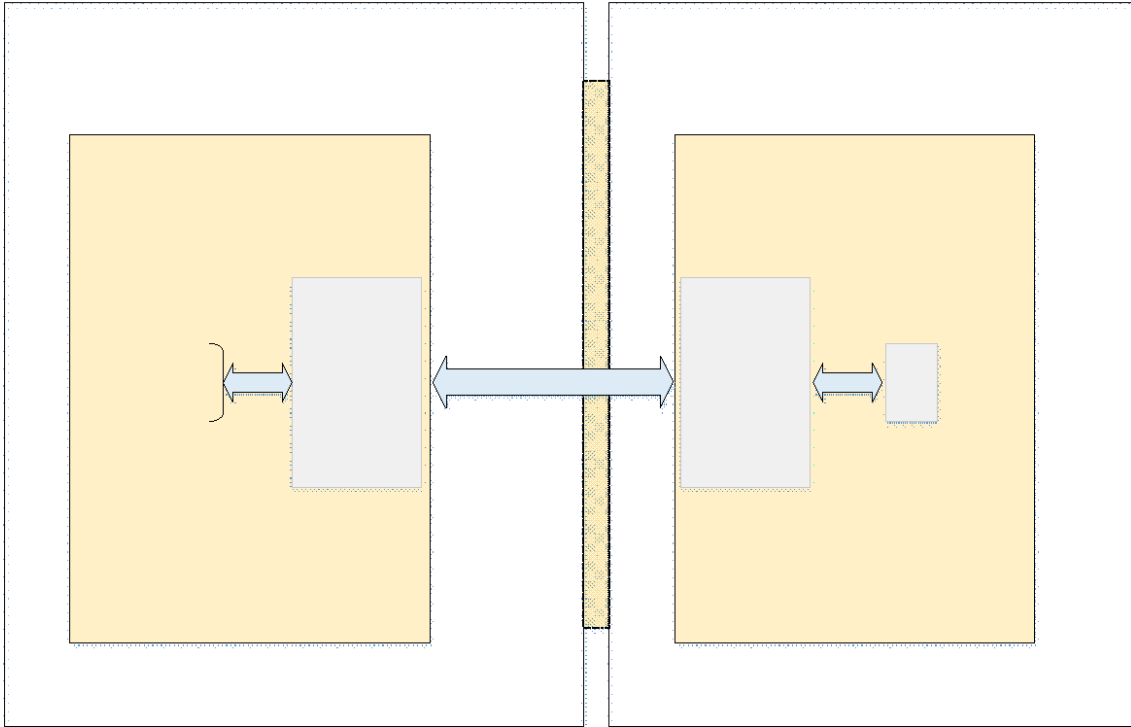


Figure 32 Data Channel internal AVMM interface.

One of the examples of Data Channel usage is shown in the Figure 33 below where Data Channel is used to access the Analog Digital Converter readings from ADC built in HPM FPGA. The BMC access to ADC readings can be implemented by the I2C interface that allows for reading and writing the SCM CPLD Mailbox.

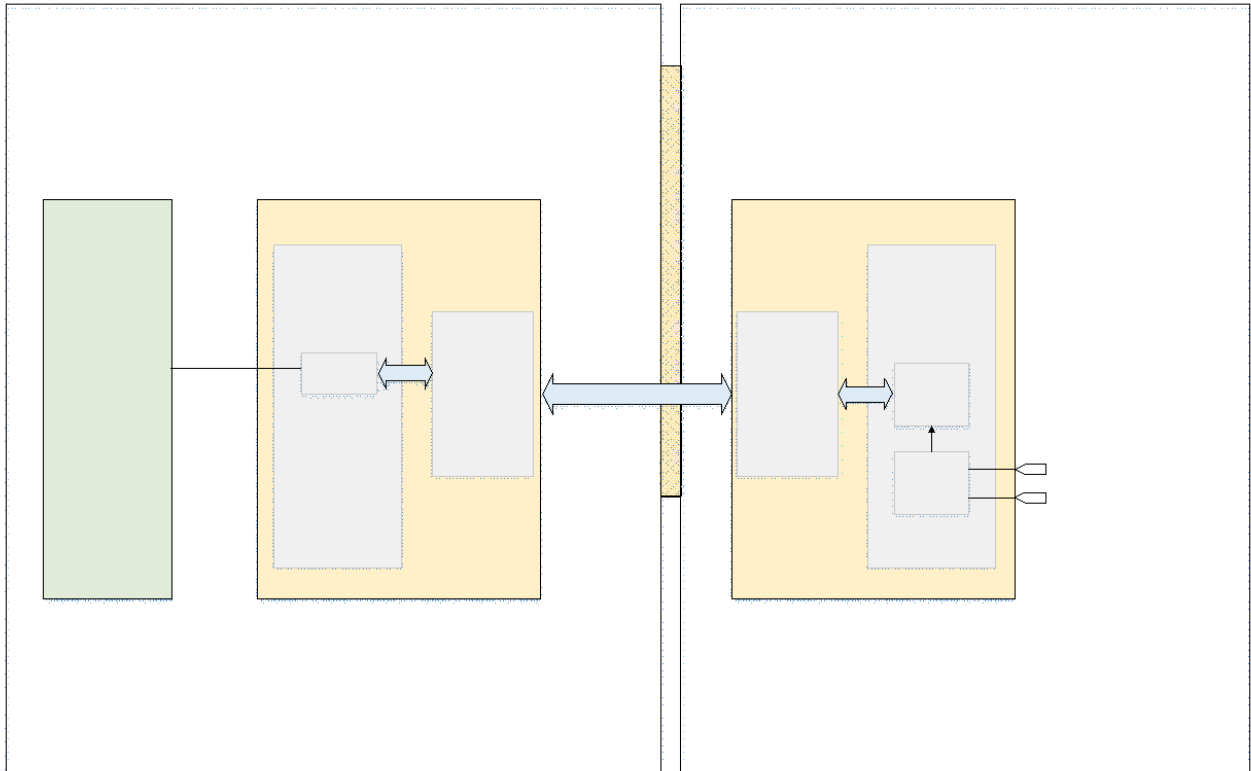


Figure 33 Data Channel usage as a way to access ADC registers in HPM FPGA

2.4.4 I2C <<<TO DO....update for bus counts, voltages, protocols)

The DC-SCI supports a total 13 I2C ports from the DC-SCM to the HPM. 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 12: 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 34.

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 I2C0 (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.

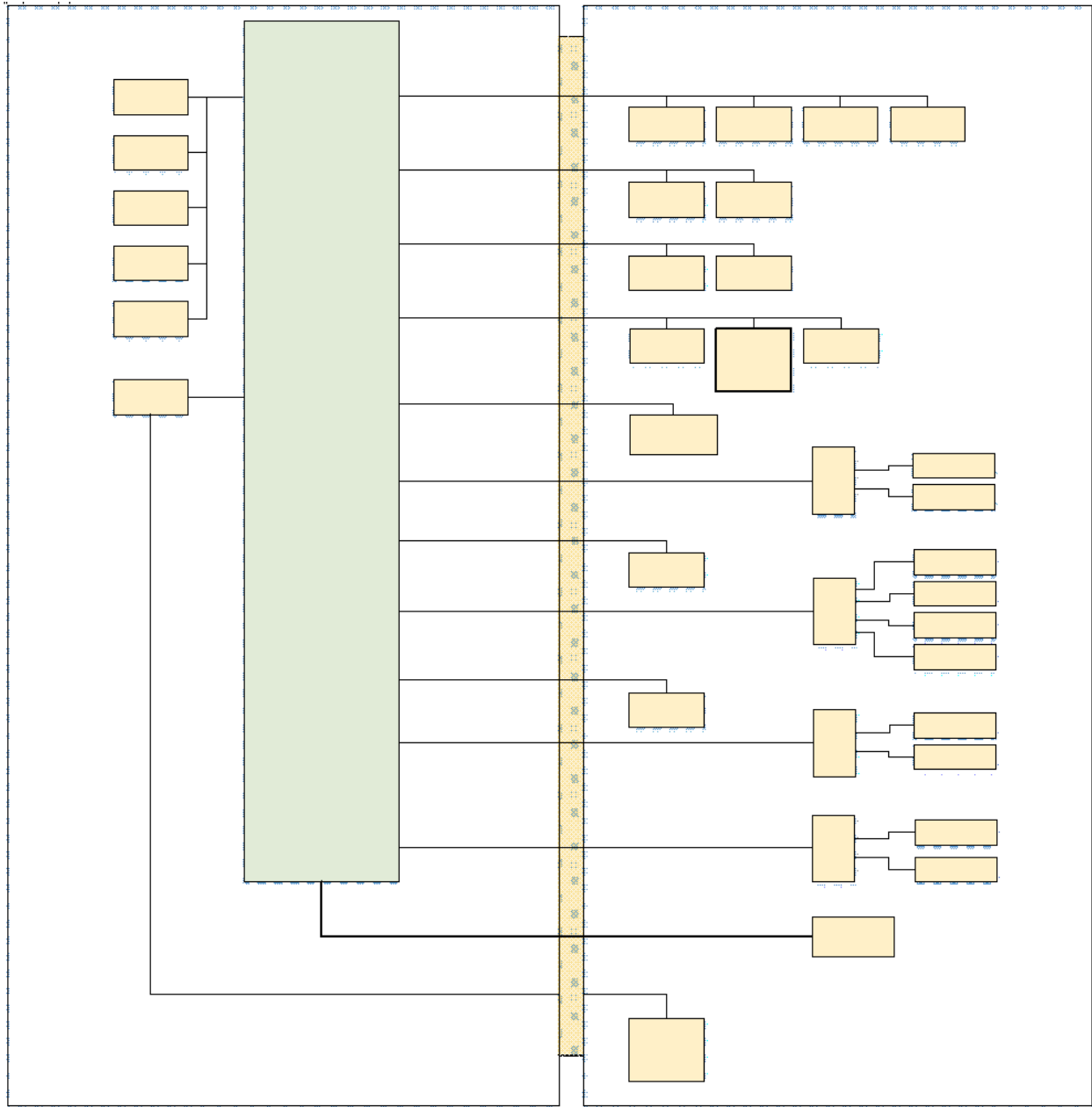


Figure 34: I2C Example Block Diagram

2.4.5 I3C

The DC-SCI supports four I3C buses. These are intended to enable future uses of I3C for HPM features. 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.

An example block diagram demonstrating the BMC low voltage I3C interface to DDR5 SPD is shown in Figure 35. Note that I3C supports multiple initiators on the same bus, but optional muxes can be added to eliminate secondary initiator negotiation.

Specific example use cases for I3C bus topology are purposefully excluded as there are no hard constraints

2.4.6 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.

An example block diagram is shown in Figure 36. The example includes an optional RoT for attestation of BMC and BIOS flash to demonstrate one of the potential security aspects of DC-SCM.

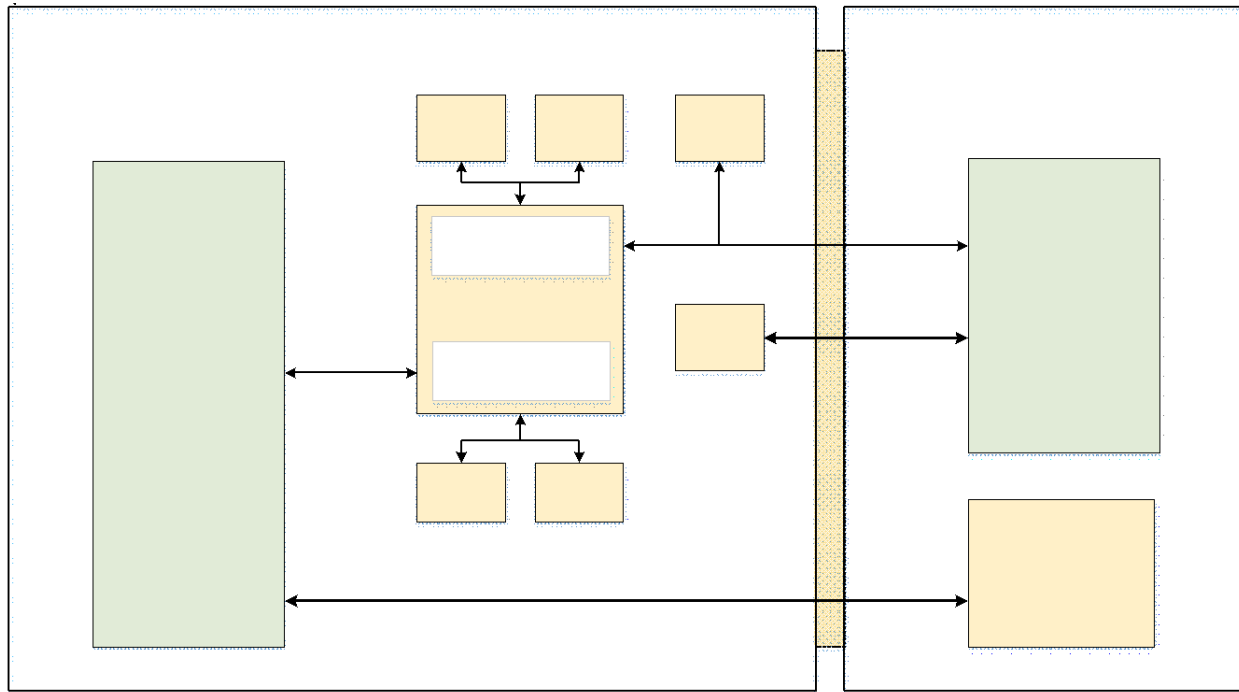


Figure 36: SPI Example Block Diagram

2.4.7 USB

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

- USB2_HPM_SCM – This is typically used to support USB 2.0 connection between the HPM and the BMC. The HPM is the initiator.
- USB2_SCM_HPM – Second USB 2.0 interface. The initiator is the BMC, and the responders are typically expansion devices within the chassis.
- GPIO/USB2_SCM_HPM_2 – potential third USB 2.0 interface where the BMC is the initiator.
- PCIE_SCM_HPM*/USB3_SCM_HPM* – This is the reserved management interface to expansion devices for future use. USB3_HPM_SCM*/PCIE_HPM_SCM*<1> - These pins are shared between single and dual node design. USB3 is used for single node and PCIE is used for dual node.

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 **Error! Reference source not found..** An example block diagram demonstrating typical USB DC-SCM/HPM architecture is shown in **Error! Reference source not found..**

Table 15: USB Signal Descriptions

Function	I/O	Voltage(V)	Description
USB2_SCM_HPM_DN			USB 2.0 between DC-SCM BMC and HPM expansion device
USB2_SCM_HPM_DP			USB 2.0 between DC-SCM BMC and HPM expansion device

USB2_HPM_SCM_DN			USB 2.0 between HPM SOC and DC-SCM BMC
USB2_HPM_SCM_DP			USB 2.0 between HPM SOC and DC-SCM BMC
GPIO/USB2_SCM_HPM_2_DN			
GPIO/USB2_SCM_HPM_2_DP			
USB3_HPM_SCM_TX_DN/PCIE_HPM_SCM_TX_DN<1>			
USB3_HPM_SCM_TX_DP/PCIE_HPM_SCM_TX_DP<1>			
USB3_HPM_SCM_RX_DN/PCIE_HPM_SCM_RX_DN<1>			
USB3_HPM_SCM_RX_DP/PCIE_HPM_SCM_RX_DP<1>			
PCIE_SCM_HPM_TX_DN/USB3_SCM_HPM_TX_DN			
PCIE_SCM_HPM_TX_DP/USB3_SCM_HPM_TX_DP			
PCIE_SCM_HPM_RX_DN/USB3_SCM_HPM_RX_DN			
PCIE_SCM_HPM_RX_DP/USB3_SCM_HPM_RX_DP			

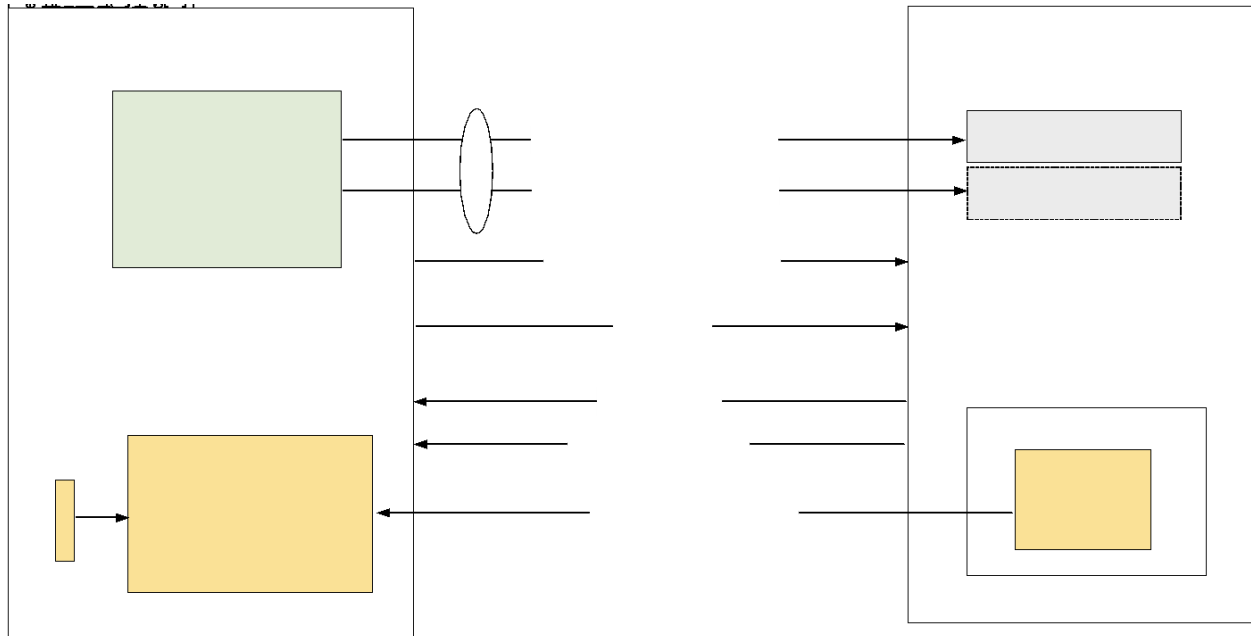


Figure 37: USB Block Diagram

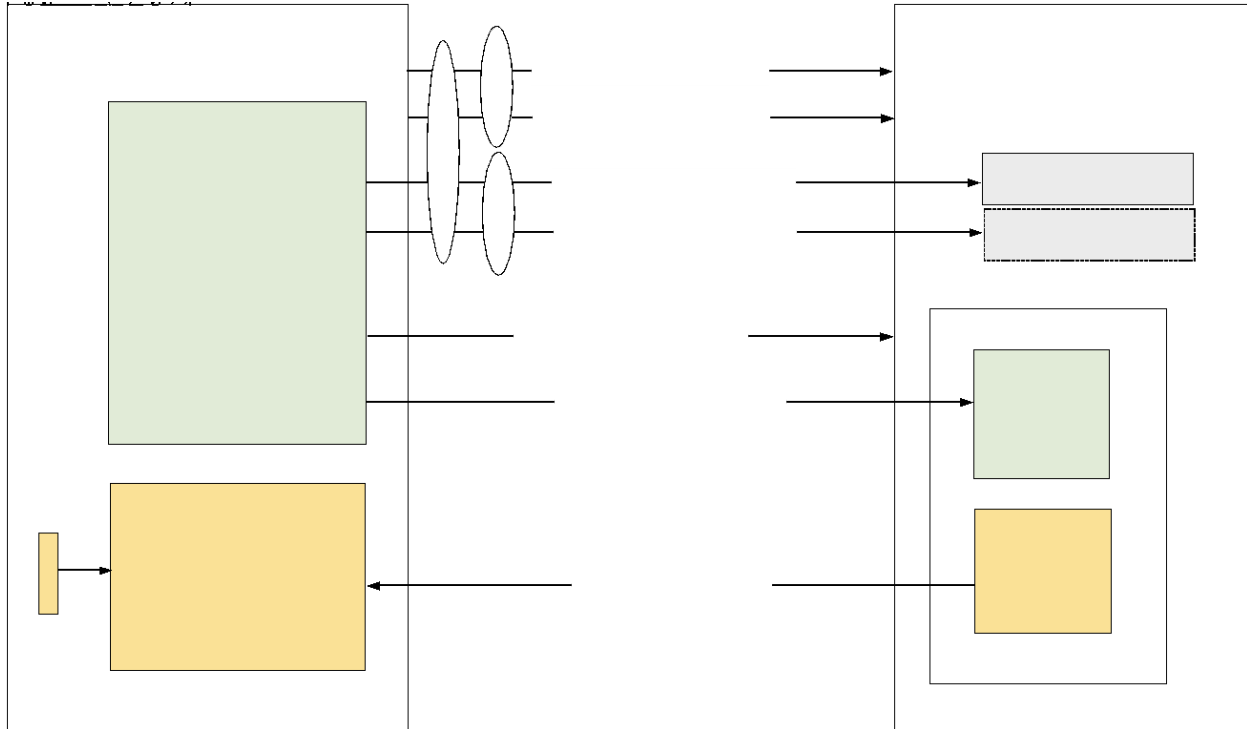
2.4.8 PCIe

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

- PCIe Gen 2.0 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 **Error! Reference source not found..**
- USB3.1 / PCIe Gen 2.0 x1 dual function Interface – These pins are connected as the second PCIe from the host to BMC for a dual node system. This interface can be used as USB3.1 for a single node design.
- PCIe Gen 2.0 x1 / USB3.1 Interface – This is reserved for the future management interface that is being defined for expansion devices.
- PCIe Gen 5.0 capable x4 Interface – This 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 **Error! Reference source not found..** CD-SCM 2.0 extended the usage model of this interface to allow bifurcation. This interface shall also allow 2 x2 lanes or 4 x1 lanes.

The DC-SCI supports one PCIe Gen 5.0 capable clock signal from the HPM to the DC-SCM. A description of the signals is shown in **Error! Reference source not found..** When both PCIe Gen 2.0 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. PCIe reset can be sourced from RST_PLTRST_BUF_N signal supported over DC-SCI as described in Table 23.

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.



2.4.9 PECI

The DC-SCI supports an optional 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. Note that the PECI interface requires its own voltage supplied by the HPM.

2.4.10 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 **Error! Reference source not found..** Note that the TRST_N (TAP reset) and SRST_N (Target system reset) if used, should be provisioned over the Serial GPIO bus.

An example block diagram demonstrating typical JTAG DC-SCM/HPM architecture is shown in **Error! Reference source not found..** The MUX on the HPM must default to selecting the JTAG channel to the HPM programmable device (HPM FPGA), by means of resistor strapping on the HPM and/or usage of the HPM_FW_RECOVERY signal described in Table 26, in order to ensure that the BMC 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.

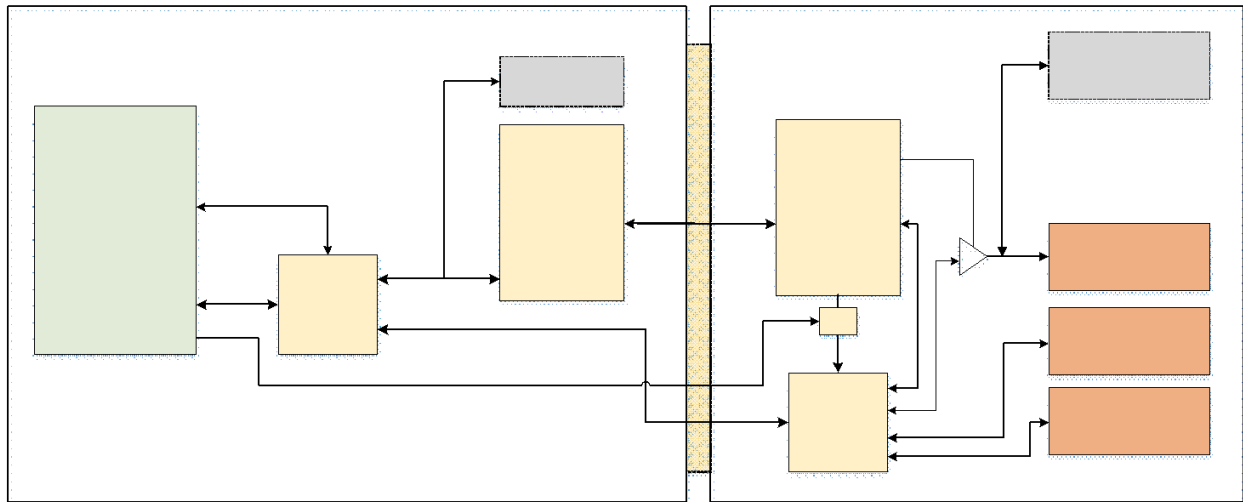


Figure 38: JTAG Example Block Diagram

2.4.11 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 21.

Table 21: 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 39. 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.

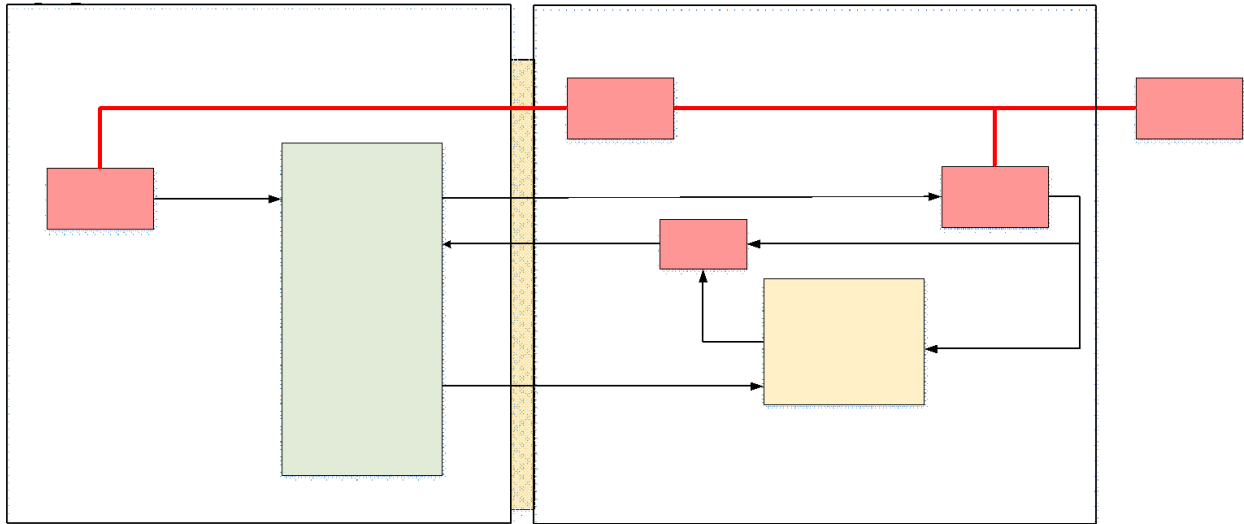


Figure 39: DC-SCM STBY Sequencing Signals Block Diagram

An example power-on and boot sequence diagram is shown in Figure 40. 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.



2.4.12 Battery Voltage

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

Table 22: 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 if 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.

2.4.13 Miscellaneous Signals

Table 23, Table 24 and Table 25 below list the RoT, Debug and Interrupt signals provisioned on the DC-SCI respectively.

Table 23: 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 25: Interrupts via DC-SCI

Signal Name	I/O	Voltage(V)	Description
SPI1_IRQ0_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 SPI1 random access or LTPI interface. Same thing with RSM_RST_N/AUXPWROK, SYS_PWROK, SYS_PWRBTN_N,

Any PSU power status signals if used, should be provisioned over the SPI1 Random Access or LTPI bus.

CATERR_N can be provisioned over either interface as well, by ensuring that any decoding based on signal timing is done in the HPM FPGA before serializing. For example, CATERR may be decoded by HPM FPGA and only IERR and MCERR be made available to the DC-SCM

Table 26 lists other miscellaneous IOs provisioned on the DC-SCI.

Table 26: Other Miscellaneous IOs via DC-SCI

Signal Name	I/O	Voltage(V)	Description
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

2 Note: Electrical Specifications

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

1.2 Input Voltage, Power, and Current

Table 27 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 27: Input Power Requirements

	Minimum	Nominal	Max
Input voltage	10V DC	12.3V DC	14V DC
Input Power	n/a	n/a	44W
Inrush Rise Time	5ms	n/a	200ms
*Input Current	n/a	n/a	4.4A

*Input current is based on 1.1A rating per pin, which is already derated. Total of four power pins on the DC-SCI.

New to DC-SCM2.0 is VCC_SCM_HPM_FRU, which is 1 DC-SCI pin sourced from the DC-SCM to the HPM specifically for powering the HPM FRU and optional circuits such as an authentication IC.

VCC_SCM_HPM_FRU must be +3.3VAUX +/- 5% and limited to 200mA maximum current. Note that this is limited for overall budget reasons and not by the pin current limit.

1.3 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 26 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 41 shows a typical presence detection and power protection implementation.

UPDATE diagram with

PRSNT0_SCM_HPM_N = B58

PRSNT1_HPM_SCM_N = A7

Change efuse to FET and align power rail names.

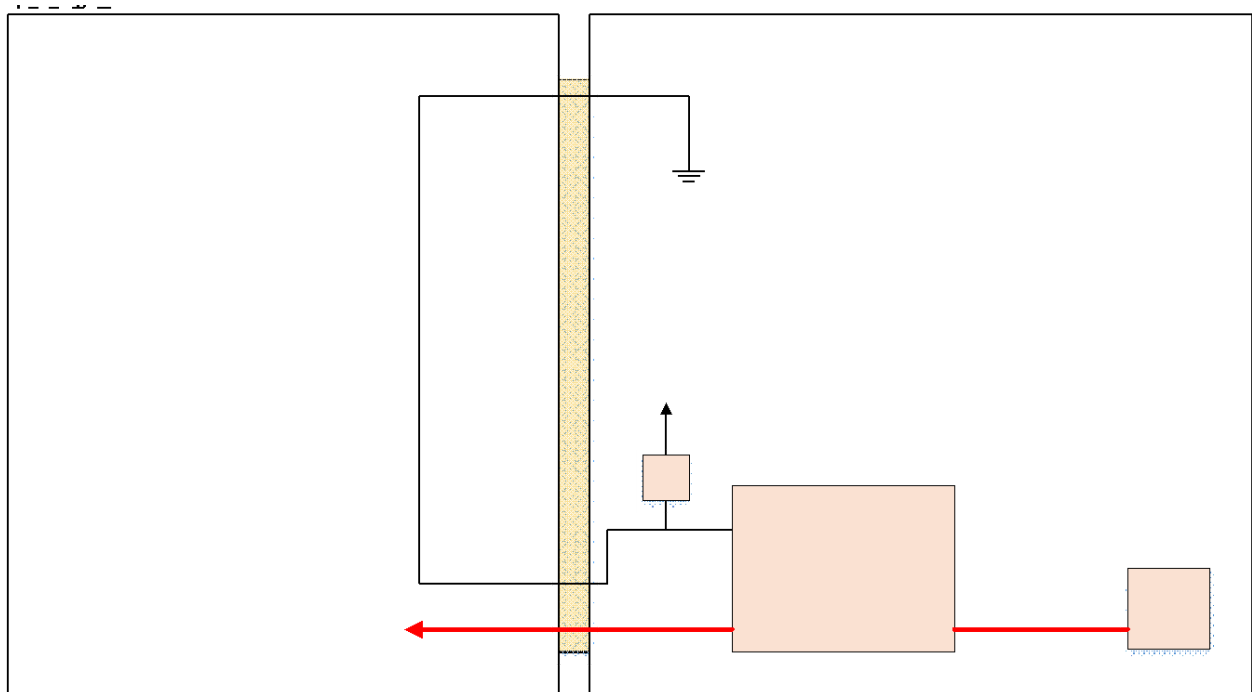


Figure 41: DC-SCM Presence Detection and Power Protection

3 Routing Guidelines and Signal Integrity

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 $\pm 15\%$ 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 42 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.

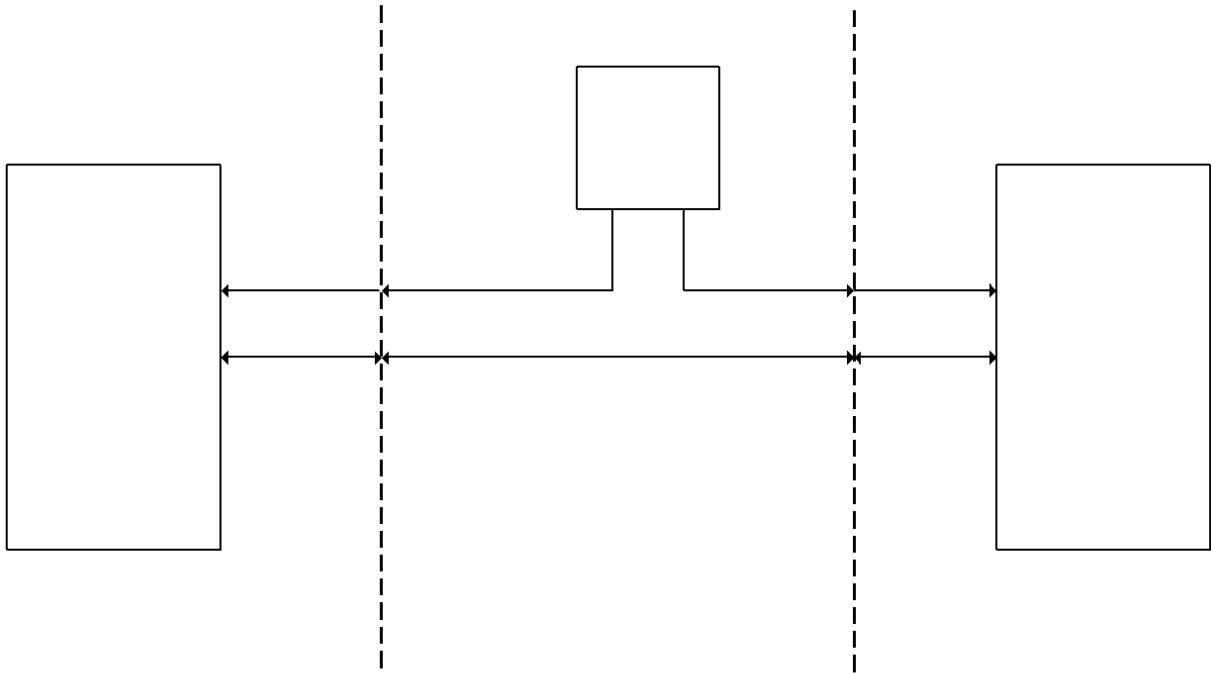


Figure 42: NC-SI Clock and Data Path Timing Delay Topology

Table 28 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 28: 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

3.1.1 NC-SI Data Timing

Based on the values in Table 28 , 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.

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

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 42 . Considering the connector propagation delays, the following requirement shall be met for the total propagation delay:

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

The Table 29 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 28.

Table 29: NC-SI Board Timing Budget

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

3.1.2 NC-SI Clock Timing

The maximum clock skew ($T_{SKEW[max]}$) between the reference clocks, as specified in DSP0222, is noted in Table 28. The critical delays are shown in Figure 42 as T1, T2, T3, and T4. The following equation summarizes the skew requirement.

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

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

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

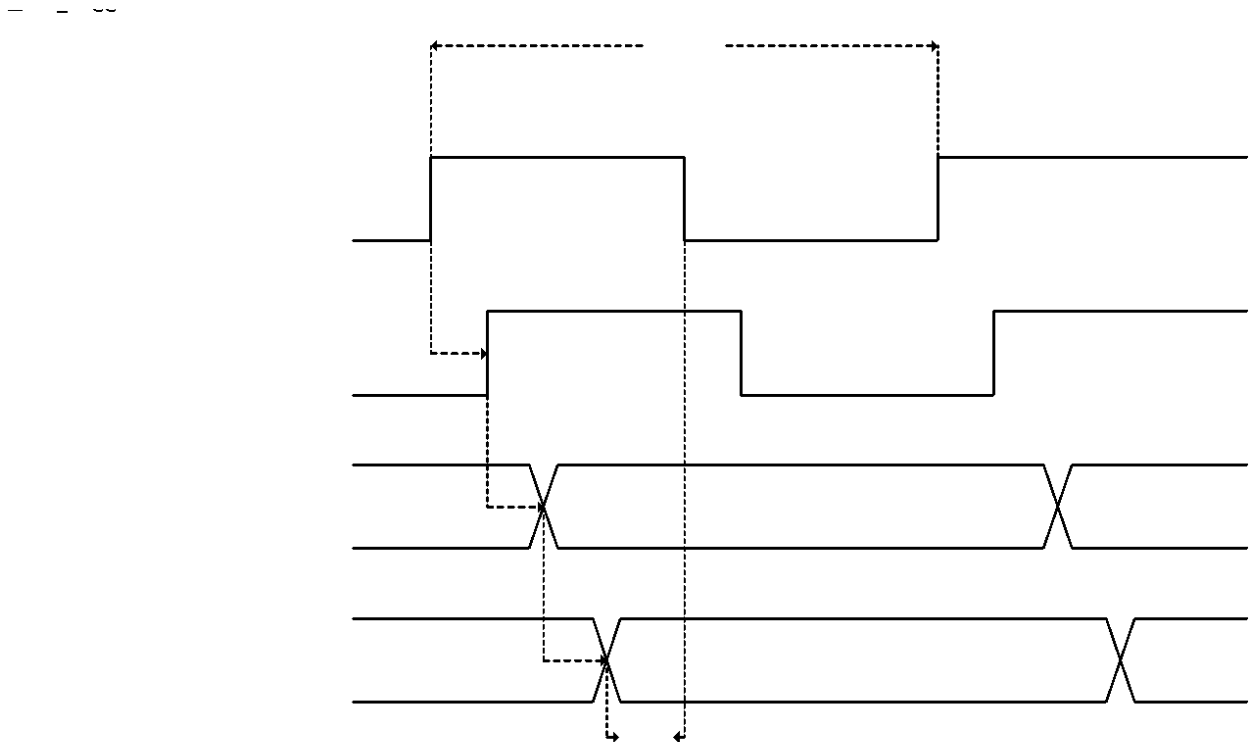


Figure 43: SGPIO Data Input Timing

Table 30 describes the timing parameters.

Table 30: 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,

$$t_{PD_SCLK} + 8 \text{ ns} + t_{PD_RX} + 1 \text{ ns} + 0.25 \text{ ns} \leq \frac{T_{SCLK}}{2}$$

$$2\text{ ns} + 8\text{ ns} + 2\text{ ns} + 1\text{ ns} + 0.25\text{ ns} = 13.25\text{ ns}$$

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.

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.

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.

4 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 31 outlines the required and optional interfaces through the DC-SCI and the expected termination on HPM when unused in the system.

Table 31: Platform Interoperability

Interface Name	Required? (Y/N)	HPM termination if un-used
NC-SI	N	No
ESPI/SSIF	N	No
I2C[1:3], I2C[5:12]	N	10K Pull-up to 3.3V STBY level
I2C[0]	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

5 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