Project Tahoe DC-SCM 2.0

Revision 0.91
October 15, 2023

Authors
Axiado: Raghu Kondapalli, Mani Gopal, Vijay Khemka, Narasimha Mangipudi, Steve Rhodes

Table of Contents

Table of Contents

1. License

1.1 OPTION B: Open Web Foundation (OWF) CLA

Contributions to this Specification are made under the terms and conditions set forth in Modified OWF-CLA-1.0.2 (As of June 1, 2023) (“Contribution License”) by:

Axiado Corporation

Usage of this Specification is governed by the terms and conditions set forth in Modified OWFa1.0.2 Final Specification Agreement (FSA) (As of June 1, 2023) (“Specification License”).

You can review the Contributor License(s) for this Specification on the OCP website at:

https://www.opencompute.org/legal-documents

For actual executed copies of either agreement, please contact OCP directly.

Notes:

The above license does not apply to the Appendix or Appendices. The information in the Appendix or Appendices is for reference only and non-normative in nature.

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

1.2 Acknowledgements

The contributors of this specification would like to acknowledge the following companies for their input:

Axiado Corporation

2. Compliance with OCP Tenets

2.1 Openness

The Project Tahoe Data Center Secure Control Module (DC-SCM) is an open-source design that adheres to the DC-SCM 2.0 specification. The deliverable includes reference design files and associated software required to recreate the design.

2.2 Efficiency

The Project Tahoe board is an energy efficient design consuming less than 20W when plugged into the PCIe slot of a server.

2.3 Impact

The Project Tahoe board fully conforms to the DC-SCM specification and introduces the single-chip AX3000 Trusted Compute Unit (TCU). The processor incorporates a built-in security co-processor that implements a Zero Trust Architecture, Hardware Root-of-Trust, Baseboard Management Control (BMC), and Trusted Platform Module (TPM). The board employs various attack mitigation strategies for infrastructure elements like servers, base stations, and network appliances through its patent-pending technologies.

The Project Tahoe board contains the following main elements:

- CPU complex incorporating four 64-bit ARM A53 cores.
- Secure Vault™ that provides secure address space and includes a Physically Unclonable Function (PUF).
- Secure AI™ with four Neural Network Processors (NNP).
- Hardware-based Firewall that accelerates network policies, traffic volume rules, and security isolation rules in hardware.
- Header and Crypto processing that provides classification, security protocol processing, and cryptographic algorithm acceleration.

The Project Tahoe board can be deployed across a multitude of Host Power Management (HPM) implementations. The only requirement for the HPM implementation is that is complies with the DC-SCM specification.

2.4 Scale

The multiple on-chip processing elements and wide variety of external interfaces make the Project Tahoe board ideal for large scale implementations. It enables the design and deployment of the HPM and DC-SCM with increased efficiency for time to market.

2.5 Sustainability

The Project Tahoe board is a modular design that is lead-free and RoHS compliant. It can work with any HPM implementation that complies with the DC-SCM specification. By following the DC-SCI pinout and definition, the common server management, security, and control features can be used across multiple platforms of the same generation and across platforms of different generations.

3. Version History

Date	Version Number	Author	Description
10/2/2023	0.90	Axiado	Draft release of Project Tahoe DC-SCM specification.
10/15/2023	0.91	Axiado	Incorporated DC-SCM management committee feedback. Added Keep-Out Zone figures.

4. Scope

The Project Tahoe board is a DC-SCM 2.0 compliant module based on the OCP DC-SCM Rev2.0 Ver1.0 Base Specification. This document can be found at:

https://www.opencompute.org/documents/ocp-dc-scm-2-0-ver-1-0-pdf

This document defines the Project Tahoe board, its functionality, and compliance with the DC-SCM specification. Strict adherence to the DC-SCM specification allows the Project Tahoe board to compatibly interface to a variety of HPM implementations that use the DC-SCI.

5. Glossary of Terms

The following terms are referenced throughout this document.

Table 1. Glossary of Terms

Term	Definition
AES	Advanced Encryption Standard
AI	Artificial Intelligence
AMD	Advanced Micro Devices
ANSI	American National Standards Institute
ARM	Advanced Risc Machines
BIOS	Basic Input Output System
BMC	Baseboard Management Controller
CBC	Cipher Block Chaining
CCM	Counter with Cipher block chaining Message authentication code; counter with CBC-MAC
CFB	Cipher Feedback
CLA	Contributor License Agreement
CMAC	Cipher-based Message Authentication Code
CPU	Central Processing Unit
CTR	Counter mode
DC-SCI	Data Center - Secure Control Interface
DC-SCM	Data Center - Secure Control Module
DRAM	Dynamic Random Access Memory
ECB	Electronic Code Book
ECDSA	Elliptic Curve Digital Signature Algorithm
EFF	External Form Factor
ESD	Electrostatic Discharge
eSPI	Enhanced Serial Peripheral Interface
FIFO	First In First Out
FET	Field Effect Transistor
FPGA	Field Programmable Gate Array
FRU	Field Replaceable Unit
FSA	Final Specification Agreement
GCM	Gallois Counter Mode
GMAC	Gallois Message Authentication Code
GPIO	General Purpose Input Output
HPM	Host Power Management
HDMI	High Definition Multimedia Interface
HWRoT	Hardware Root of Trust
IEEE	Institute of Electrical and Electronics Engineers
I2C	Inter-Integrated Circuit
JTAG	Joint Test Action Group
LTPI	Low-voltage differential signaling Tunneling Protocol & Interface
LVDS	Low-Voltage Differential Signaling
MAC	Message Authentication Code
ML	Machine Learning
NC-SI	Network Controller Sideband Interface
NNP	Neural Network Processor
OCP	Open Compute Project
OOB	Out Of Bound
OTP	One Time Programmable
OWF	Open Web Foundation
PCIe	Peripheral Connect Interface Express
PFR	Platform Firmware Resilience
PRoT	Platform Root of Trust
PUF	Physically Unclonable Function
QSPI	Quad Serial Peripheral Interface
RMII	Reduced Media Independent Interface
RoHS	Restriction of Hazardous Substances
ROM	Read Only Memory
SerDes	Serializer Deserializer
SGMII	Serial Gigabit Media Independent Interface
SGPIO	Serial General Purpose Input Output
SHA	Secure Hash Algorithm
SMBUS	System Management Bus
SPI	Serial Peripheral Interface
SRAM	Static Random Access Memory
SVT	Secure Vault
TCU	Trusted Compute Unit
TPM	Trusted Platform Module
UART	Universal Asynchronous Receiver Transmitter
UEFI	Unified Extensible Firmware Interface
USB	Universal Serial Bus
XTS	XEX-based Tweaked-codebook mode with ciphertext Stealing

6. Overview

The Project Tahoe board is based on the OCP DC-SCM Rev2.0 Ver1.0 Base Specification.

At the heart of the system is the AX3000 Trusted Compute Unit (TCU) processor which, when loaded with a compatible OpenBMC firmware, provides an environment that allows for remote server management.

The Project Tahoe board contains the following elements:

- A Hardware Root of Trust (HWRoT) and Platform Firmware Resiliency (PFR) solution providing secure firmware authentication, firmware recovery, and firmware update capability.
- An on-chip System Manager which controls resets, power enables, interrupts, SoC and platform alert power management. The Secure Vault within Tahoe exposes crypto services for authentication, measurements, etc.
- A built-in hardware Firewall:
  - Accelerates network policies, traffic volume rules, security isolation rules in hardware.
  - Detects and take actions on known vulnerabilities for traffic across interfaces like Ethernet.
  - Detects malicious intent by monitoring activity that is out of the ordinary on a per-user basis.
- An on-board Artificial Intelligence (AI) engine that detects specific traffic patterns from certain interfaces. The engine contains four Machine Learning (ML) islands operating at 1 GHz.
- The on-board Crypto Processing Unit incorporates up to four 1 Gbit Ethernet SGMII ports and provides classification, security protocol processing, and cryptographic algorithm acceleration required for the processing of network security for both wired and wireless protocols. The Crypto engine supports a wide variety of algorithms, including:
  - Kazumi F8/F9, SNOW3G, and ZUC wireless algorithms
  - Supports the AES-XTS (ANSI/IEEE Std P1619-2007) storage algorithm
  - Supports 3DES in ECB and CBC with (3x) 56-bit key
  - Supports AES in ECB, CBC, ICM, CTR, CFB and OFB128 mode with 128/192/256 bit keys, GCM, GMAC and CCM modes
- A separate Hash engine supports:
  - MD5 and SHA-1
  - SHA-2 with 224-bit, 256-bit digest
  - AES-CMAC, XCBC-MAC and CBC-MAC (for CCM)
- The Project Tahoe board incorporates an AMD Spartan 7 FPGA to support a variety of I/O interfaces, including LTPI, GPIO, I2C, UART, etc.
- The Project Tahoe board is implemented in the 1U vertical External Form Factor (EFF) design that plugs into the PCIe slots of a server.

7. Rack Compatibility

The Project Tahoe board is mechanically compatible within any system that has a DC-SCM 2.0 slot. The VFF definition, according to DC-SCM 2.0, incorporates servers that are 2U or taller. This specification expands the VFF definition to 1U servers.

8. Physical Specifications

8.1 Block Diagram

Figure 1 shows the block diagram for the Project Tahoe DC-SCM board.

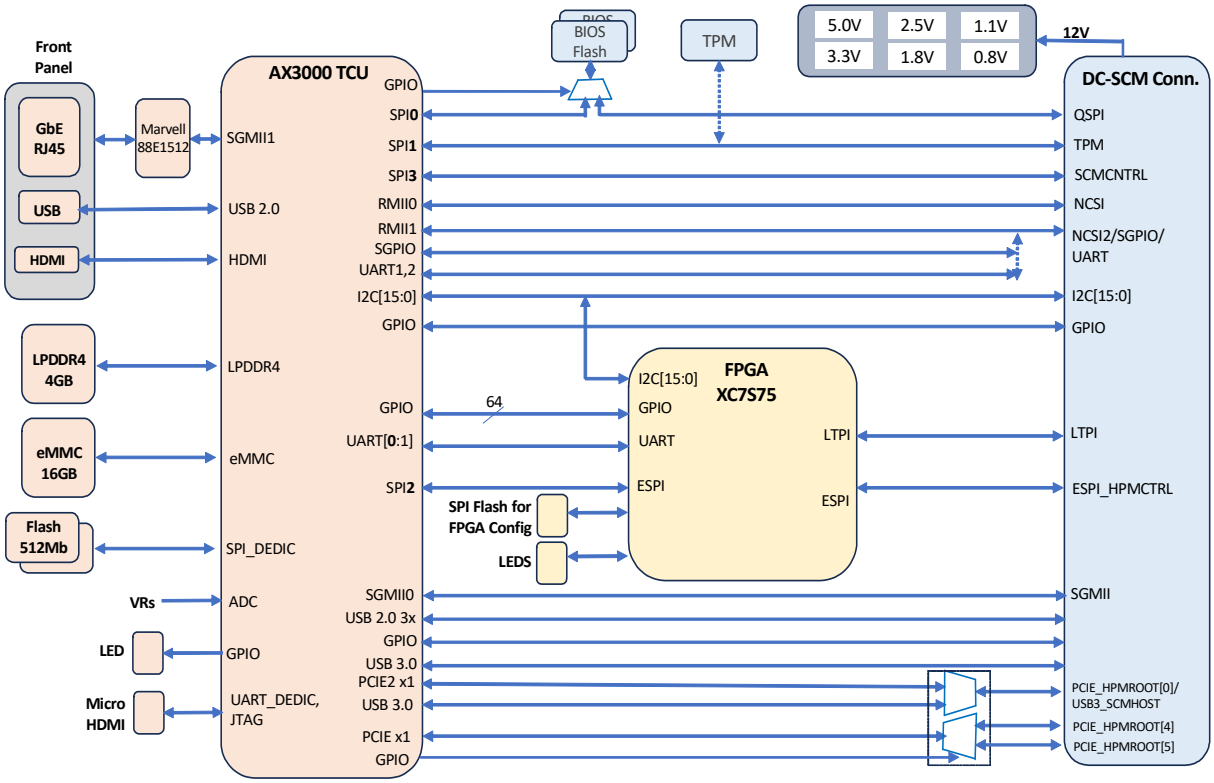

Figure 1. Project Tahoe DC-SCM Block Diagram

8.2 PCB Overview

8.2.1 Board Stack-up

PCB Stack Up							Impedance							
Layer	Type		Thickness (mil)			DK/DF	Single end				Differential			
Top side solder mask				0.70	mils	4.1/0.022	LINE(mil)	Reference	ohm	TheoryValue	Width / Space(mil)	Reference	ohm	TheoryValue
L1	TOP	Signal	copper+plating	1.1	mils		5.00	L2	50	49.92	5.50/5.30 5.00/5.20 4.20/6.80	L2 L2 L2	85 90 100	84.49 88.06 99.03
		TU-86P		3.06	mils	4/0.016								
L2		Signal(GND)	copper	0.7	mils									
		TU-862	core	3	mils	3.97/0.016								
L3		Signal	copper	0.7	mils		2.80	L2/L4	50	47.5	3.60/8.40 3.30/8.25 2.60/8.50	L2/L4 L2/L4 L2/L4	85 90 100	83.3 86.96 97.29
		TU-86P		3.37	mils	4.14/0.015								
L4		Signal(GND)	copper	0.7	mils									
		TU-862	core	3	mils	3.97/0.016								
L5		Signal	copper	0.7	mils		2.80	L4/L6	50	47.97	3.60/8.40 3.30/7.80 2.60/8.95	L4/L6 L4/L6 L4/L6	85 100 90	84.13 87.58 98.33
		TU-86P		3.51	mils	4.14/0.015								
L6		Signal	copper	0.7	mils		2.80	L5/L7	50	47.97				
		TU-862	core	3	mils	3.97/0.016								
L7		Signal(GND)	copper	0.7	mils									
		TU-86P		3.58	mils	4.14/0.015								
L8		Signal(PWR)	copper	1.4	mils									
		TU-862	core	3	mils	3.97/0.016								
L9		Signal(PWR)	copper	1.4	mils									
		TU-86P		3.58	mils	4.14/0.015								
L10		Signal(GND)	copper	0.7	mils									
		TU-862	core	3	mils	3.97/0.016								
L11		Signal	copper	0.7	mils		2.80	L10/L12	50	47.97				
		TU-86P		3.51	mils	4.14/0.015								
L12		Signal	copper	0.7	mils		2.80	L11/L13	50	47.97	3.60/8.40 3.30/7.80 2.60/8.95	L11/L13 L11/L13 L11/L13	85 100 90	84.13 87.58 98.33
		TU-862	core	3	mils	3.97/0.016								
L13		Signal(GND)	copper	0.7	mils									
		TU-86P		3.37	mils	4.14/0.015								
L14		Signal	copper	0.7	mils		2.80	L13/L15	50	47.5	3.60/8.40 3.30/8.25 2.60/8.50	L13/L15 L13/L15 L13/L15	85 90 100	83.3 86.96 97.29
		TU-862	core	3	mils	3.97/0.016								
L15		Signal(GND)	copper	0.7	mils									
		TU-86P		3.06	mils	4/0.016								
L16	Bottom	Signal	copper+plating	1.1	mils		5.00	L15	50	49.92	5.50/5.30 5.00/5.20 4.20/6.80	L15 L15 L15	85 90 100	84.49 88.06 99.03
Bottom side solder mask				0.70	mils	4.1/0.022								
TOTAL				62.84 1.60	mils mm									

Figure 2. Board Stack-Up

8.2.2 Board Placement Top Side (TBD)

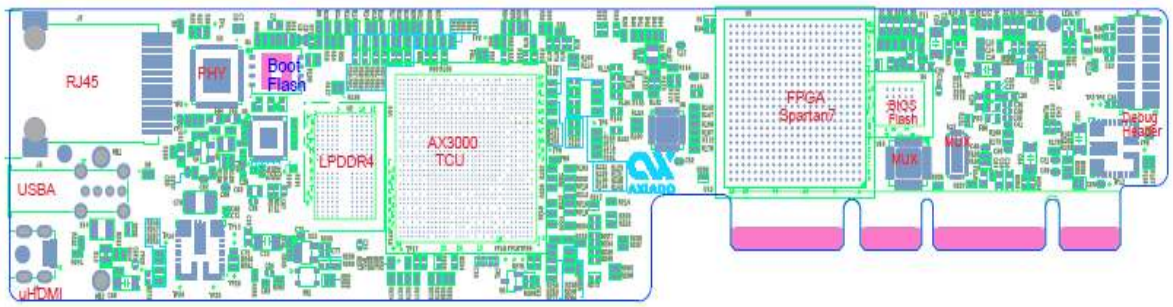

Figure 3. Board Placement — Top Side

8.2.3 Board Placement Bottom Side

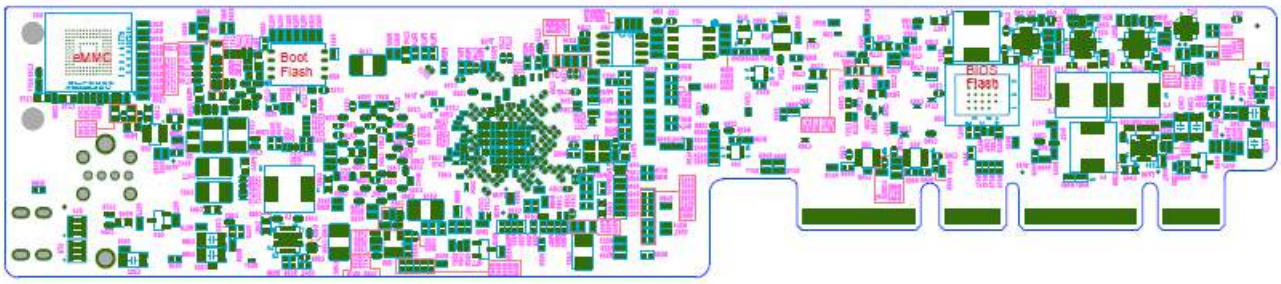

Figure 4. Board Placement — Bottom Side

8.2.4 Board Mechanical Dimensions

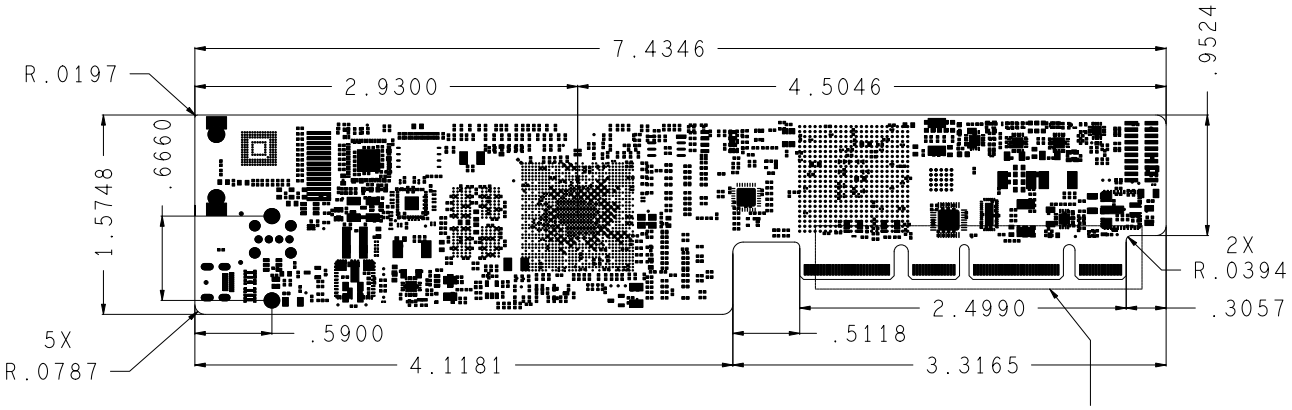

Figure 5. Tahoe Board Mechanical Dimensions

The 1U form factor height is defined as 44.45 mm. As shown in the above diagram, the overall height of the Project Tahoe board is 1.5748”, or 40 mm, which is within the maximum height defined by the specification.

9. Thermal Design Requirements

9.1 Sensor Locations on Board

The Project Tahoe DC-SCM board contains four ambient temperature sensors. These sensors are used to measure the inlet and outlet temperatures on the board. The Baseboard Management Control (BMC) firmware accesses these temperature sensors via the I2C bus. The sensors are located on the board as shown in Figure 6.

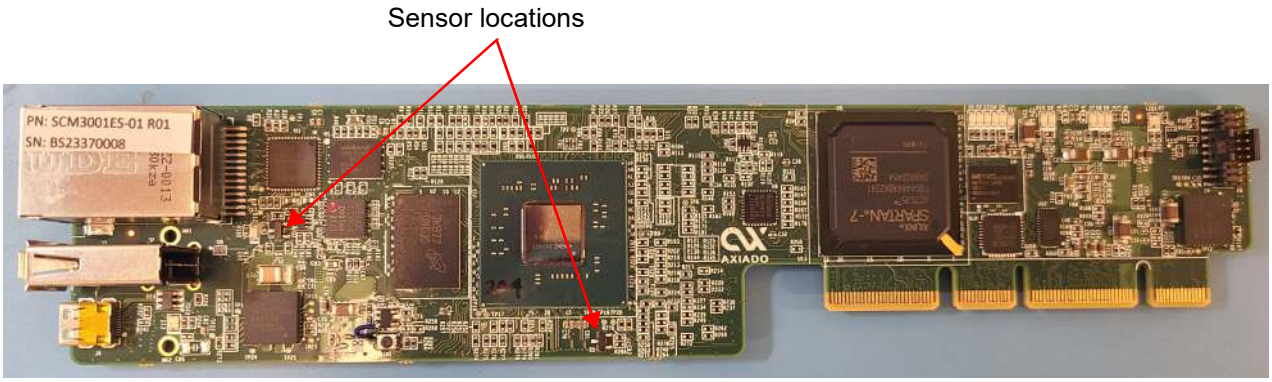

Figure 6. Sensor Locations — Top of Board

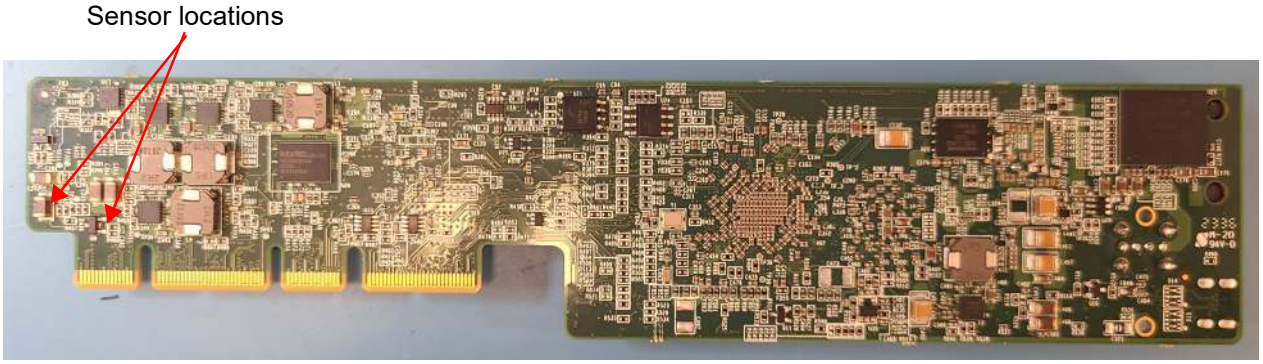

Figure 7. Sensor Locations — Bottom of Board

10. I/O System

10.1 DC-SCM Card Edge Connector Requirement

The DC-SCM card edge connector used on the Tahoe board complies with the OCP DC-SCM Rev2.0 Ver1.0 Base Specification. This connector is shown in Figure 8.

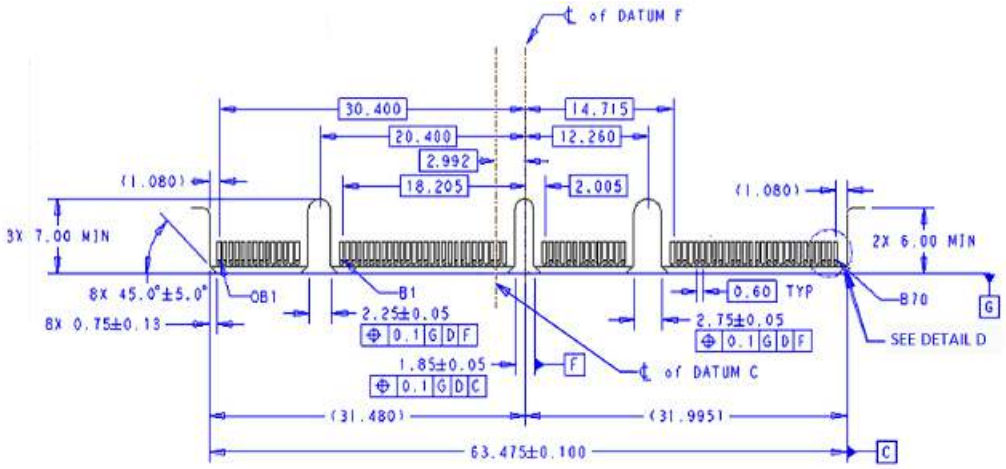

Figure 8. Card Edge Connector Dimensions – Top Side (“B” Pins)

10.2 Gold Finger Plating Requirement

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

10.3 HPM Connector Requirement

The Project Tahoe DC-SCM board is connected to the HPM through the connector shown in Figure 9. The connector is fastened to the board using two M2 screws.

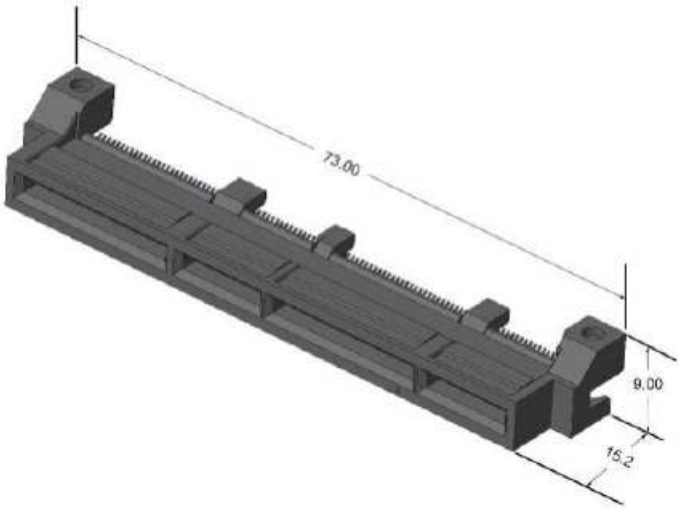

Figure 9. HPM Connector Dimensions (mm)

10.4 DC-SCI Pin Definitions

The Project Tahoe DC-SCM board DC-SCI pinout fully complies with the OCP DC-SCI Rev2.0 Ver1.0 Pin Definition. An overview of the interfaces supported by the Tahoe board is defined in Table 2 below.

Table 2. DC-SCI Pinout Overview

Function
12V Aux Power
Power Sequencing & Presence Detection
LTPI (LVDS)
2x BMC PCIe x1 End Point
3x BMC USB 2.0 Host or Endpoint
Up to 2x BMC USB 3.0 Host
eSPI (Single Node/CPU P0)
QSPI (Single Node/CPU P0)
SPI
10 x I2C/I3C @ 3.3V
5 x I2C/I3C @ 1.8V
2 x I2C/I3C @ 1.0V
Up to 26 GPIO's
SGPIO
Up to 2 UART ports
JTAG

The detailed pin assignments of the DC-SCI connector are captured in the following tables. Table 3 is the Side A pinout, and Table 4 is the Side B pinout. .

Table 3. Side A Pinout

Side A	Single Node Primary / Alternate Function (if applicable)	Voltage (Single/Dual)	Direction (DC-SCM View)	Tahoe Board DC-SCM 2.0
OA1	GND			GND
OA2	PCIE_HPMROOT_SCM_HPM_0_DN / USB3_SCMHOST2_SCM_HPM_DN		output / output	PCIE_HPMROOT_SCM_HPM_0_DN / USB3_SCMHOST2_SCM_HPM_DN
OA3	PCIE_HPMROOT_SCM_HPM_0_DP / USB3_SCMHOST2_SCM_HPM_DP		output / output	PCIE_HPMROOT_SCM_HPM_0_DP / USB3_SCMHOST2_SCM_HPM_DP
OA4	GND			GND
OA5	PCIE_HPMROOT_SCM_HPM_1_DN / LTPI2_SCM_HPM_CLK_DN / DISPLAYPORT_SCM_HPM_LANE0_DN	PCIe / LTPI / DP	output / output / output	NC
OA6	PCIE_HPMROOT_SCM_HPM_1_DP / LTPI2_SCM_HPM_CLK_DP / DISPLAYPORT_SCM_HPM_LANE0_DP	PCIe / LTPI / DP	output / output / output	NC
OA7	GND			GND
OA8	PCIE_HPMROOT_SCM_HPM_2_DN / SGMII_SCM_HPM_DN		output / output	SGMII_SCM_HPM_DN
OA9	PCIE_HPMROOT_SCM_HPM_2_DP / SGMII_SCM_HPM_DP		output / output	SGMII_SCM_HPM_DP
OA10	GND			GND
OA11	PCIE_HPMROOT_SCM_HPM_3_DN / LTPI2_SCM_HPM_DATA_DN / DISPLAYPORT_SCM_HPM_LANE1_DN	PCIe / LTPI / DP	output / output / output	NC
OA12	PCIE_HPMROOT_SCM_HPM_3_DP / LTPI2_SCM_HPM_DATA_DP / DISPLAYPORT_SCM_HPM_LANE1_DP	PCIe / LTPI / DP	output / output / output	NC
OA13	GND			GND
OA14	PECI_HPM_SCM / GPIO	0.85 - 1.21V	input / output	PECI_HPM_SCM / TCI GPIO
A1	P12V_AUX		input	P12V_AUX
A2	P12V_AUX		input	P12V_AUX
A3	P12V_AUX		input	P12V_AUX
A4	P12V_AUX		input	P12V_AUX
A5	GND			GND
A6	GND			GND
A7	PRSNT1_HPM_SCM_N	0V	input	PRSNT1_HPM_SCM_N / TCU GPIO
A8	JTAG_SCMCNTRL_TCK	3.3V	output	JTAG_SCMCNTRL_TCK / TCU GPIO
A9	JTAG_SCMCNTRL_TDI	3.3V	input	JTAG_SCMCNTRL_TDI / TCU GPIO
A10	JTAG_SCMCNTRL_TDO	3.3V	output	JTAG_SCMCNTRL_TDO / TCU GPIO
A11	JTAG_SCMCNTRL_TMS	3.3V	output	JTAG_SCMCNTRL_TMS / TCU GPIO
A12	JTAG_SCMCNTRL_TRST_N	3.3V	output	JTAG_SCMCNTRL_TRST_N / TCU GPIO
A13	SCM_HPM_STBY_RST_N	3.3V	output	SCM_HPM_STBY_RST_N / TCU GPIO
A14	SCM_HPM_STBY_EN	3.3V	output	SCM_HPM_STBY_EN / TCU GPIO
A15	I2C_3V3_0_SCL	3.3V	input / output	I2C_3V3_0_SCL
A16	I2C_3V3_0_SDA	3.3V	input / output	I2C_3V3_0_SDA
A17	I2C_3V3_1_SCL	3.3V	input / output	I2C_3V3_1_SCL
A18	I2C_3V3_1_SDA	3.3V	input / output	I2C_3V3_1_SDA

Table 3. Side A Pinout (Continued)

Side A	Single Node Primary / Alternate Function (if applicable)	Voltage (Single/Dual)	Direction (DC-SCM View)	Tahoe Board DC-SCM 2.0
A19	GND			GND
A20	LTPI_SCM_HPM_DATA_DN		output	LTPI_SCM_HPM_DATA_DN
A21	LTPI_SCM_HPM_DATA_DP		output	LTPI_SCM_HPM_DATA_DP
A22	GND			GND
A23	LTPI_SCM_HPM_CLK_DN		output	LTPI_SCM_HPM_CLK_DN
A24	LTPI_SCM_HPM_CLK_DP		output	LTPI_SCM_HPM_CLK_DP
A25	GND			GND
A26	I2C_3V3_2_SCL	3.3V	input / output	I2C_3V3_2_SCL
A27	I2C_3V3_2_SDA	3.3V	input / output	I2C_3V3_2_SDA
A28	PCIE_HPM_SCM_PERST_N	3.3V	input	PCIE_HPM_SCM_PERST_N
A29	GND			GND
A30	PCIE_HPMROOT_SCM_HPM_4_DN		output	PCIE_HPMROOT_SCM_HPM_4_DN
A31	PCIE_HPMROOT_SCM_HPM_4_DP		output	PCIE_HPMROOT_SCM_HPM_4_DP
A32	GND			GND
A33	PCIE_SCMROOT_SCM_HPM_DN / USB3_SCMHOST1_SCM_HPM_DN		output / output	USB3_SCMHOST1_SCM_HPM_DN
A34	PCIE_SCMROOT_SCM_HPM_DP / USB3_SCMHOST1_SCM_HPM_DP		output / output	USB3_SCMHOST1_SCM_HPM_DP
A35	GND			GND
A36	PCIE_HPM_SCM_CLK_100M_0_DN		input	AX20x_PCIEX1_100M_CLKn
A37	PCIE_HPM_SCM_CLK_100M_0_DP		input	AX20x_PCIEX1_100M_CLKp
A38	GND			GND
A39	I2C_I3C_1V0_18_SCL / FSI_1V2_0_SCL	1.0/1.2V	input / output	I2C_I3C_1V0_18_SCL
A40	I2C_I3C_1V0_18_SCL / FSI_1V2_0_SDA	1.0/1.2V	input / output	I2C_I3C_1V0_18_SDA
A41	I2C_I3C_1V0_19_SCL / FSI_1V2_1_SCL	1.0/1.2V	input / output	I2C_I3C_1V0_19_SCL
A42	I2C_I3C_1V0_19_SCL / FSI_1V2_1_SDA	1.0/1.2V	input / output	I2C_I3C_1V0_19_SDA
A43	I2C_3V3_3_SCL	3.3V single 1.8V dual	input / output	I2C_3V3_3_SCL
A44	I2C_3V3_3_SDA	3.3V single 1.8V dual	input / output	I2C_3V3_3_SDA
A45	I2C_3V3_4_SCL	3.3V single 1.8V dual	input / output	I2C_3V3_4_SCL
A46	I2C_3V3_4_SDA	3.3V single 1.8V dual	input / output	I2C_3V3_4_SDA
A47	I2C_3V3_5_SCL	3.3V single 1.8V dual	input / output	I2C_3V3_5_SCL
A48	I2C_3V3_5_SDA	3.3V single 1.8V dual	input / output	I2C_3V3_5_SDA
A49	I2C_3V3_6_SCL	3.3V single 1.8V dual	input / output	I2C_3V3_6_SCL
A50	I2C_3V3_6_SDA	3.3V single 1.8V dual	input / output	I2C_3V3_6_SDA
A51	I2C_I3C_1V8_16_SCL	1.8V	input / output	I2C_I3C_1V8_16_SCL
A52	I2C_I3C_1V8_16_SDA	1.8V	input / output	I2C_I3C_1V8_16_SDA
A53	GND			GND

Table 3. Side A Pinout (Continued)

Side A	Single Node Primary / Alternate Function (if applicable)	Voltage (Single/Dual)	Direction (DC-SCM View)	Tahoe Board DC-SCM 2.0
A54	SPI_HPMCNTRL_TPM_CLK / I2C_I3C_1V8_10_SCL	1.8V	input / input/output	SPI_HPMCNTRL_TPM_CLK
A55	SPI_HPMCNTRL_TPM_CS_N / I2C_I3C_1V8_10_SDA / QSPI_HPMCNTRL_TPM_CS_N	1.8V	input / input/output / output	SPI_HPMCNTRL_TPM_CS_N
A56	SPI_HPMCNTRL_TPM_MOSI / I2C_I3C_1V8_11_SCL	1.8V	input / input/output	SPI_HPMCNTRL_TPM_MOSI
A57	SPI_HPMCNTRL_TPM_MISO / I2C_I3C_1V8_11_SDA	1.8V	output / input/output	SPI_HPMCNTRL_TPM_MISO
A58	I2C_I3C_1V8_12_SCL	1.8V	input/output	I2C_I3C_1V8_12_SCL
A59	I2C_I3C_1V8_12_SDA	1.8V	input/output	I2C_I3C_1V8_12_SDA
A60	GPI / SPI_SCMCNTRL_IRQ0_N	1.8V	input	GPI / SPI_SCMCNTRL_IRQ0_N / TCU GPIO
A61	I2C_I3C_1V8_13_SCL	1.8V	input/output	I2C_I3C_1V8_13_SCL
A62	I2C_I3C_1V8_13_SDA	1.8V	input/output	I2C_I3C_1V8_13_SDA
A63	UART0_HPM_SCM_DATA / GPIO	3.3V	input / input/output	UART0_HPM_SCM_DATA / PCIE_SCM_HPM_PERST_N
A64	GND			GND
A65	PCIE_HPMROOT_SCM_HPM_5_DN		output	PCIE_HPMROOT_SCM_HPM_5_DN
A66	PCIE_HPMROOT_SCM_HPM_5_DP		output	PCIE_HPMROOT_SCM_HPM_5_DP
A67	GND			GND
A68	PCIE_HPM_SCM_CLK_100M_1_S0_DN / PCIE_HPM_SCM_CLK_100M_1_S5_DN		input / input	AX20x_PCIEX2_100M_CLKn
A69	PCIE_HPM_SCM_CLK_100M_1_S0_DP / PCIE_HPM_SCM_CLK_100M_1_S5_DP		input / input	AX20x_PCIEX2_100M_CLKp
A70	GND			GND

Table 4. Side B Pinout

Side B	Single Node Primary / Alternate Function (if applicable	Voltage (Single/Dual)	Direction (DC-SCM View)	Project Tahoe DC-SCM 2.0
OB1	GND			GND
OB2	PCIE_HPMROOT_HPM_SCM_0_DN / USB3_SCMHOST2_HPM_SCM_DN		input / input	PCIE_HPMROOT_HPM_SCM_0_DN / USB3_SCMHOST2_HPM_SCM_DN
OB3	PCIE_HPMROOT_HPM_SCM_0_DP / USB3_SCMHOST2_HPM_SCM_DP		input / input	PCIE_HPMROOT_HPM_SCM_0_DP / USB3_SCMHOST2_HPM_SCM_DP
OB4	GND			GND
OB5	PCIE_HPMROOT_HPM_SCM_1_DN / LTPI2_HPM_SCM_CLK_DN / DISPLAYPORT_AUX_DN	PCIe / LTPI / DP	input / input / input / output	PCIE_HPMROOT_HPM_SCM_1_DN
OB6	PCIE_HPMROOT_HPM_SCM_1_DP / LTPI2_HPM_SCM_CLK_DP / DISPLAYPORT_AUX_DP	PCIe / LTPI / DP	input / input / input / output	PCIE_HPMROOT_HPM_SCM_1_DP
OB7	GND			GND
OB8	PCIE_HPMROOT_HPM_SCM_2_DN / SGMII_HPM_SCM_DN		input / input	SGMII_HPM_SCM_DN
OB9	PCIE_HPMROOT_HPM_SCM_2_DP / SGMII_HPM_SCM_DP		input / input	SGMII_HPM_SCM_DP
OB10	GND			GND

Table 4. Side B Pinout (Continued)

Side B	Single Node Primary / Alternate Function (if applicable	Voltage (Single/Dual)	Direction (DC-SCM View)	Project Tahoe DC-SCM 2.0
OB11	PCIE_HPMROOT_HPM_SCM_3_DN / LTPI2_HPM_SCM_DATA_DN / USB2_SCMHOST3_DN	PCIe / LTPI / DP	input / input / input / output	USB2_SCMHOST3_DN
OB12	PCIE_HPMROOT_HPM_SCM_3_DP / LTPI2_HPM_SCM_DATA_DP / USB2_SCMHOST3_DP	PCIe / LTPI / DP	input / input / input / output	USB2_SCMHOST3_DP
OB13	GND			GND
OB14	PECI_VREF_HPM_SCM / GPI	0.85 - 1.21V	input	DC_SCM_OB14_GPI
B1	ESPI_HPMCNTRL_CLK	1.8V	input	ESPI_HPMCNTRL_CLK
B2	ESPI_HPMCNTRL_CS0_N	1.8V	input	ESPI_HPMCNTRL_CS0_N
B3	ESPI_HPMCNTRL_RESET_N	1.8V	input	ESPI_HPMCNTRL_RESET_N
B4	ESPI_HPMCNTRL_IO_0	1.8V	input / output	ESPI_HPMCNTRL_IO_0
B5	ESPI_HPMCNTRL_IO_1	1.8V	input / output	ESPI_HPMCNTRL_IO_1
B6	ESPI_HPMCNTRL_IO_2	1.8V	input / output	ESPI_HPMCNTRL_IO_2
B7	ESPI_HPMCNTRL_IO_3	1.8V	input / output	ESPI_HPMCNTRL_IO_3
B8	ESPI_HPMCNTRL_ALERT0_N	1.8V	output	ESPI_HPMCNTRL_ALERT0_N
B9	I2C_I3C_1V8_17_SCL / ESPI0_HPMCNTRL_CS1_N	1.8V	input / output input	I2C_I3C_1V8_17_SCL / ESPI0_HPMCNTRL_CS1_N
B10	I2C_I3C_1V8_17_SDA / ESPI0_HPMCNTRL_ALERT1_N	1.8V	input / output input	I2C_I3C_1V8_17_SDA / ESPI0_HPMCNTRL_ALERT1_N
B11	GND			GND
B12	QSPI_HPMCNTRL_CLK	1.8V	input	QSPI_HPMCNTRL_CLK
B13	QSPI_HPMCNTRL_CS0_N	1.8V	input	QSPI_HPMCNTRL_CS0_N
B14	QSPI_HPMCNTRL_IO_0	1.8V	input / output	QSPI_HPMCNTRL_IO_0
B15	QSPI_HPMCNTRL_IO_1	1.8V	input / output	QSPI_HPMCNTRL_IO_1
B16	QSPI_HPMCNTRL_IO_2	1.8V	input / output	QSPI_HPMCNTRL_IO_2
B17	QSPI_HPMCNTRL_IO_3	1.8V	input / output	QSPI_HPMCNTRL_IO_3
B18	QSPI_HPMCNTRL_CS1_N / GPI	1.8V	input / input	QSPI_HPMCNTRL_CS1_N / GPI
B19	GND			GND
B20	LTPI_HPM_SCM_DATA_DN		input	LTPI_HPM_SCM_DATA_DN
B21	LTPI_HPM_SCM_DATA_DP		input	LTPI_HPM_SCM_DATA_DP
B22	GND			GND
B23	LTPI_HPM_SCM_CLK_DN		input	LTPI_HPM_SCM_CLK_DN
B24	LTPI_HPM_SCM_CLK_DP		input	LTPI_HPM_SCM_CLK_DP
B25	GND			GND
B26	HPM_SCM_STBY_RDY	3.3V	input	HPM_SCM_STBY_RDY / TCU GPIO
B27	HPM_SCM_INTRUSION_N	3.3V / BAT	input	HPM_INTRUSION_BMC_N / TCU GPIO
B28	P3V0_HPM_SCM_BAT	3.0V / BAT	input	NC
B29	GND			GND
B30	PCIE_HPMROOT_HPM_SCM_4_DN		input	PCIE_HPMROOT_HPM_SCM_TX_DN
B31	PCIE_HPMROOT_HPM_SCM_4_DP		input	PCIE_HPMROOT_HPM_SCM_TX_DP
B32	GND			GND
B33	PCIE_SCMROOT_HPM_SCM_DN / USB3_SCMHOST1_HPM_SCM_DN		output / output	USB3_SCMHOST1_HPM_SCM_DN

Table 4. Side B Pinout (Continued)

Side B	Single Node Primary / Alternate Function (if applicable	Voltage (Single/Dual)	Direction (DC-SCM View)	Project Tahoe DC-SCM 2.0
B34	PCIE_SCMROOT_HPM_SCM_DP / USB3_SCMHOST1_HPM_SCM_DP		output / output	USB3_SCMHOST1_HPM_SCM_DP
B35	GND			GND
B36	USB2_SCMHOST1_DN / USB2_HPMHOST1_DN / GPIO		input / output input / output input / output	USB2_SCMHOST1_DN / USB2_HPMHOST1_DN / GPIO
B37	USB2_SCMHOST1_DP / USB2_HPMHOST1_DP / GPIO		input / output input / output input / output	USB2_SCMHOST1_DP / USB2_HPMHOST1_DP / GPIO
B38	GND			GND
B39	I2C_I3C_1V8_14_SCL	1.8V	input / output	I2C_I3C_1V8_14_SCL
B40	I2C_I3C_1V8_14_SDA	1.8V	input / output	I2C_I3C_1V8_14_SDA
B41	I2C_I3C_1V8_15_SCL	1.8V	input / output	I2C_I3C_1V8_15_SCL
B42	I2C_I3C_1V8_15_SDA	1.8V	input / output	I2C_I3C_1V8_15_SDA
B43	NCSI_HPM_SCM_CLK / GPIO	3.3V	input	NCSI_HPM_SCM_CLK / GPIO
B44	NCSI_HPM_SCM_CRS_DV / GPIO	3.3V	input	NCSI_HPM_SCM_CRS_DV / GPIO
B45	NCSI_SCM_HPM_TX_EN / GPIO	3.3V	output	NCSI_SCM_HPM_TX_EN / GPIO
B46	NCSI_SCM_HPM_D0 / GPIO	3.3V	output	NCSI_SCM_HPM_D0 / GPIO
B47	NCSI_SCM_HPM_D1 / GPIO	3.3V	output	NCSI_SCM_HPM_D1 / GPIO
B48	NCSI_HPM_SCM_D0 / GPIO	3.3V	input	NCSI_HPM_SCM_D0 / GPIO
B49	NCSI_HPM_SCM_D1 / GPIO	3.3V	input	NCSI_HPM_SCM_D1 / GPIO
B50	VCC_SCM_HPM_FRU	3.3V	output	VCC_SCM_HPM_FRU / TCU GPIO
B51	UART0_SCM_HPM_DATA / PCIE_SCM_HPM_PERST_N / GPO / NCSI2_SCM_HPM_TX_EN	3.3V	output / output / output / output	UART0_SCM_HPM_DATA / PCIE_SCM_HPM_PERST_N / GPO / NCSI2_SCM_HPM_TX_EN
B52	I2C_3V3_7_SCL / SGPIO_CLK / NCSI2_HPM_SCM_CLK	3.3V	input / output output / output	I2C_3V3_7_SCL / SGPIO_CLK / NCSI2_HPM_SCM_CLK
B53	I2C_3V3_7_SDA / SGPIO_LD / NCSI2_HPM_SCM_CRS_DV /	3.3V	input / output output / output	I2C_3V3_7_SDA / SGPIO_LD / NCSI2_HPM_SCM_CRS_DV /
B54	I2C_3V3_8_SCL / SGPIO_DATAOUT / NCSI2_SCM_HPM_D0	3.3V	input / output output / input / output	I2C_3V3_8_SCL / SGPIO_DATAOUT / NCSI2_SCM_HPM_D0
B55	I2C_3V3_8_SDA / SGPIO_DATAIN / NCSI2_SCM_HPM_D1	3.3V	input / output input / input / output	I2C_3V3_8_SDA / SGPIO_DATAIN / NCSI2_SCM_HPM_D1
B56	I2C_3V3_9_SCL / UART1_SCM_HPM_DATA / NCSI2_HPM_SCM_D0	3.3V	input / output output / input / output	I2C_3V3_9_SCL / UART1_SCM_HPM_DATA / NCSI2_HPM_SCM_D0
B57	I2C_3V3_9_SDA / UART1_HPM_SCM_DATA / NCSI2_HPM_SCM_D1	3.3V	input / output input / input / output	I2C_3V3_9_SDA / UART1_HPM_SCM_DATA / NCSI2_HPM_SCM_D1
B58	PRSNT0_SCM_HPM_N	0V	output	PRSNT0_SCM_HPM_N
B59	SPI_SCMCNTRL_CS1_N / GPIO	3.3V	output / input / output	SPI_SCMCNTRL_CS1_N / GPIO
B60	SPI_SCMCNTRL_CLK	3.3V	output	SPI_SCMCNTRL_CLK
B61	SPI_SCMCNTRL_MISO	3.3V	input	SPI_SCMCNTRL_MISO

Table 4. Side B Pinout (Continued)

Side B	Single Node Primary / Alternate Function (if applicable	Voltage (Single/Dual)	Direction (DC-SCM View)	Project Tahoe DC-SCM 2.0
B62	SPI_SCMCNTRL_MOSI	3.3V	output	SPI_SCMCNTRL_MOSI
B63	SPI_SCMCNTRL_CS0_N	3.3V	output	SPI_SCMCNTRL_CS0_N
B64	GND			GND
B65	PCIE_HPMROOT_HPM_SCM_5_DN		output	PCIE_HPMROOT_HPM_SCM_5_DN
B66	PCIE_HPMROOT_HPM_SCM_5_DP		output	PCIE_HPMROOT_HPM_SCM_5_DP
B67	GND			GND
B68	USB2_SCMHOST2_DN / USB2_HPMHOST2_DN / GPIO	3.3V	input / output input / output input / output	USB2_SCMHOST2_DN / USB2_HPMHOST2_DN / GPIO
B69	USB2_SCMHOST2_DP / USB2_HPMHOST2_DP / GPIO	3.3V	input / output input / output input / output	USB2_SCMHOST2_DP / USB2_HPMHOST2_DP / GPIO
B70	GND			GND

10.5 Project Tahoe Board External Interfaces

10.5.1 LTPI Interface Block Diagram

The current silicon revision of the AX3000 TCU does not natively support LTPI and requires an external CPLD/FPGA.

The LTPI interface combines several channels of GPIO, UART, I2C, and application specific interfaces as shown in Figure 10 and transmits/receives over a single high-speed LVDS path.

When transmitting a frame, the signals are multiplexed by the mux engine shown below. The multiplexed data is then assembled into frames by the Framer block before being encoded by the 8b/10b block and driven out onto the wire.

When receiving a frame, the incoming data arrives over the wire and is decoded by the 10b/8b block. The frame is deconstructed by the Deframer block and then demultiplexed by the Demux block into its original data stream and driven onto the associated interfaces shown in Figure 10. The master and slave can be on either end of the interface in a particular configuration.

The LTPI specification defines training, capability, and configuration of the LTPI channel, as well as the data frame format used by the Framer block. The LTPI interface uses configuration registers to create and configure the interface. The AXB20x LTPI implementation is OCP DC-SCM spec 2.0 compliant.

NOTE: The LTPI standard requires that the configurable logic described above exist at both ends of the interface to support a flexible implementation.

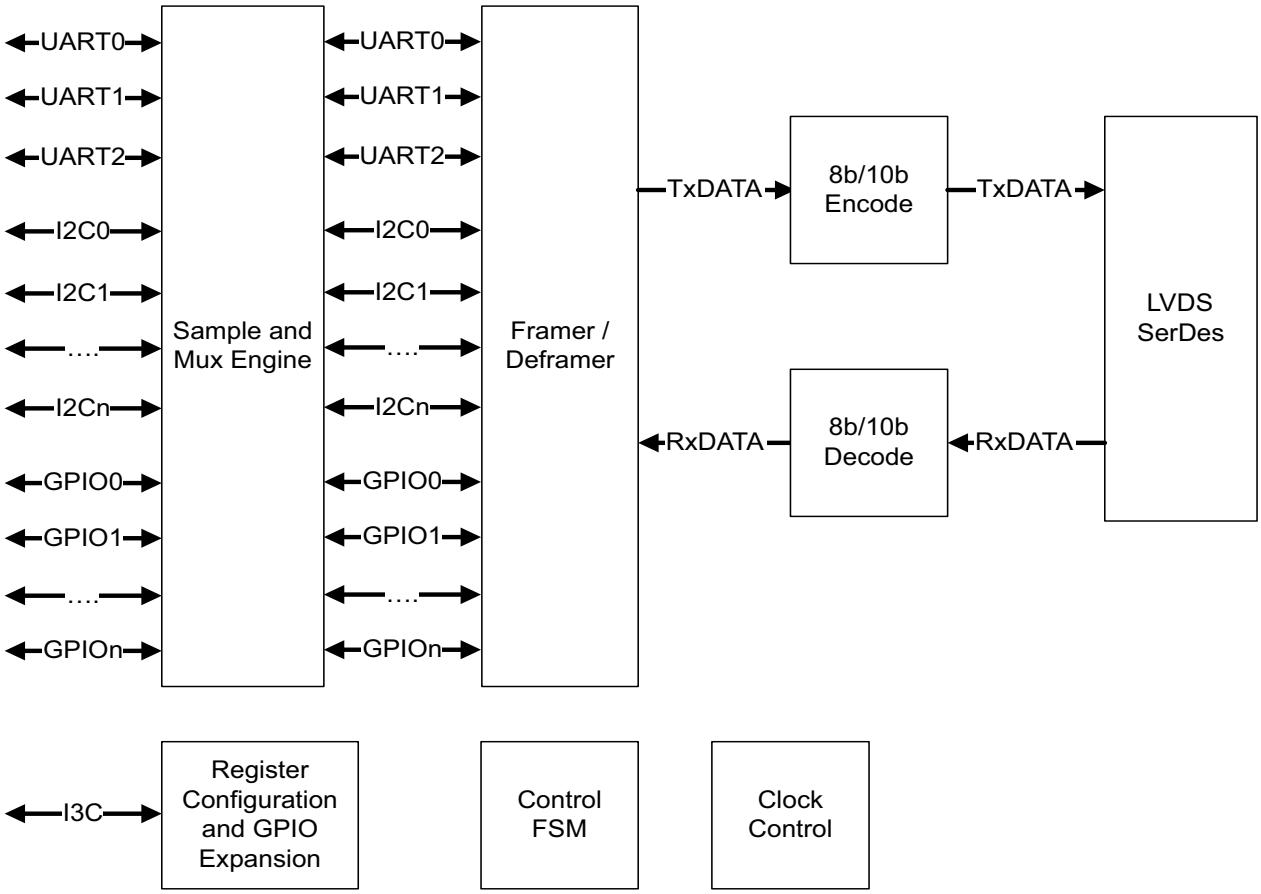

Figure 10. LTPI Block Diagram

10.5.2 LTPI SerDes

The SerDes is implemented in the LVDS GPIOs of the FPGA. For a two channel LTPI, 16 total LVDS pins are required. The ingress to the SerDes will be 10-bit symbols that are then serialized out at the SerDes clock rate. The egress from the SerDes will be framed to a 10-bit symbol and passed upstream via ingress FIFO.

Figure 11 shows a block diagram of the LTPI SerDes interface.

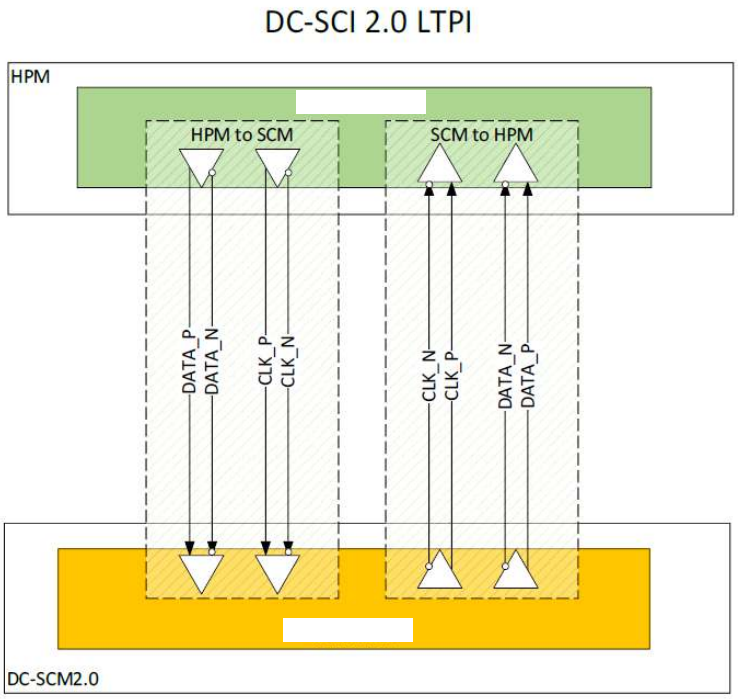

Figure 11. LTPI SerDes Interface

Table 5. LTPI Signal Definitions

Function	HPM CPLD LVDS I/O	SCM FPGA LVDS I/O
LTPI_HPM_SCM_DATA_DN	TX Data Negative	RX Data Negative
LTPI_HPM_SCM_DATA_DP	TX Data Positive	RX Data Positive
LTPI_HPM_SCM_CLK_DN	TX Clock Negative	RX Clock Negative
LTPI_HPM_SCM_CLK_DP	TX Clock Positive	RX Clock Positive
LTPI_SCM_HPM_DATA_DN	RX Data Negative	TX Data Negative
LTPI_SCM_HPM_DATA_DP	RX Data Positive	TX Data Positive
LTPI_SCM_HPM_CLK_DN	RX Clock Negative	TX Clock Negative
LTPI_SCM_HPM_CLK_DP	RX Clock Positive	TX Clock Positive

10.5.3 SGPIO

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

10.5.4 I2C/I3C

The Project Tahoe DC-SCM board supports a total of 16 x I2C/I3C ports from the DC-SCI to the HPM.

10.5.5 eSPI

Project Tahoe DC-SCM board supports single node configurations with 1 x HPM to DC-SCM eSPI bus defined. The SPI_SS and SPI_ALERT signals should be used for the AX3000 TCU.

There is no LPC support in Project Tahoe. Host to HPM details when eSPI is unavailable are beyond the scope of this document.

10.5.6 QSPI and SPI

The Project Tahoe DC_SCM board supports configures the four SPI interfaces as follows:

Table 6. SPI Interface Distribution

SPI Interface	SPI Configuration	From	To
0	QSPI	AX3000 TCU	DC-SCI Connector
1	TPM	AX3000 TCU	DC-SCI Connector
2	eSPI	AX3000 TCU	XC7S75 FPGA
3	SCMCTRL	AX3000 TCU	DC-SCI Connector

10.5.7 USB

The Project Tahoe DC-SCM board supports three USB 2.0 ports and two USB 3.0 ports. One USB 2.0 port is located on the front faceplate. The USB signal (USB2_HPMHOST1_x) comes directly from the host CPU through the DC-SCI connector.

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

Table 7. DC-SCI USB Pin Assignments

AX3000 Pin Name	DC-SCI Pin Number	DC-SCI
USB2P0_0_DM USB2P0_0_DP	B36/B37	USB2_HPMHOST1_DN/ USB2_HPMHOST1_DP
USB2P0_1_DM USB2P0_1_DP	B68/B69	USB2_HPMHOST2_DN/ USB2_HPMHOST2_DP
USB2P0_2_DM USB2P0_2_DP	OB11/OB12	USB2_HPMHOST3_DN/ USB2_HPMHOST3_DP
USB3P0_0_DM USB3P0_0_DP	A33/A34	USB3_HPMHOST1_DN/ USB3_HPMHOST1_DP
USB3P0_1_DM USB3P0_1_DP	OB2/OB3	USB3_HPMHOST2_DN/ USB3_HPMHOST2_DP

10.5.8 JTAG

The Project Tahoe DC-SCM board supports a Joint Test Action Group (JTAG) interface using GPIO pins. This interface can be used for system debug, as well as for programming various devices such as an HPM CPLD or other PCIe based add-in cards.

Table 8. DC-SCI JTAG Pin Assignments

AX3000 Pin Name	DC-SCI Pin Number	DC-SCI
GPIO_148	A8	HPM_JTAG_TCK

Table 8. DC-SCI JTAG Pin Assignments (Continued)

AX3000 Pin Name	DC-SCI Pin Number	DC-SCI
GPIO_149	A9	HPM_JTAG_TDI
GPIO_150	A10	HPM_JTAG_TDO
GPIO_151	A11	HPM_JTAG_TMS
GPIO_152	A12	HPM_JTAG_TRST_N

10.5.9 NC-SI

Project Tahoe DC-SCM board supports an RMII/NC-SI interface that is connected to the DC-SCI. The description of the signals is shown in Table 9.

Table 9. DC-SCI NC-SI Pin Assignments

AX3000 Pin Name	DC-SCI Pin Number	DC-SCI
RMII0_REFCLK	B43	NCSI_CLK
RMII0_RXDV	B44	NCSI_CRS_DV
RMII0_TXEN	B45	NCSI_TXEN
RMII0_TXD0	B46	NCSI_TXD0
RMII0_TXD1	B47	NCSI_TXD1
RMII0_RXD0	B48	NCSI_RXD0
RMII0_RXD1	B49	NCSI_RXD1

10.5.10 UART

The Project Tahoe DC-SCM board supports two UART ports on the DC-SCI.

Table 10. DC-SCI UART Pin Assignments

AX3000 Pin Name	DC-SCI Pin Number	DC-SCI
UART_1_RXD	A63	UART0_HPM_SCM_DATA
UART_1_TXD	B51	UART0_SCM_HPM_DATA
UART_2_RXD	B56	UART1_TX_SCM_HPM_DATA
UART_2_TXD	B57	UART1_RX_HPM_SCM_DATA

10.6 Power States and Boot Sequence

The Project Tahoe DC-SCM board power states adhere to the OCP DC-SCM Rev2.0 Ver1.0 Base Specification power states. The supported power states are shown in Table 12.

The DC-SCM specification does not specifically support hot insertion or removal. However, circuitry should exist on the HPM to protect the circuits from damage due to faulty connector pins.

Table 11. DC-SCI Discovery/Sequencing Pin Assignments

DC-SCM Side	DC-SCI Pin Number	DC-SCI Pin Name
SCM board	A7	PRSNT1_N
SCM board	B58	PRSNT0_N
GPIO_144	A14	HPM_STBY_EN
GPIO_143	B26	HPM_STBY_RDY

Table 11. DC-SCI Discovery/Sequencing Pin Assignments (Continued)

DC-SCM Side	DC-SCI Pin Number	DC-SCI Pin Name
GPIO_145	A13	PFR_HPM_STBY_RST_N

Table 12. Power States, Boot, and Discovery Sequence

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

10.6.1 Virtual Re-seat

The Project Tahoe DC-SCM board supports the virtual re-seat function. This is accomplished by de-asserting the HPM_STBY_EN signal (pin A14 on the DC-SCI connector). Asserting this pin places the system in the Pre-STBY power state defined in Table 12. In this state, all power rails on the HPM interface are removed completely. The power rails continue in this state as long as HPM_STBY_EN remains de-asserted. When the HPM_STBY_EN signal is again asserted, the system transitions to the STBY power state and the HPM power rails are automatically restored.

10.7 Platform Root of Trust (PRoT)

The Project Tahoe DC-SCM board implements the Root-of-Trust (RoT) in hardware and thus forms an immutable RoT, which is referred to as Hardware Root of Trust (HWRoT). The HWRoT extends to provide the Platform Root-of-Trust (PRoT). The platform firmware images such as UEFI, BMC, along with the images for Tahoe are stored in onboard flash. As Tahoe boots it first authenticates and measures its own image, before authenticating and measuring the platform images.

After a successful authentication of the platform images Tahoe will release the Host and its associated circuitry out of reset. This whole process establishes the PRoT. Platform Firmware Resiliency (PFR) additionally protects platform firmware from malicious attacks, prevents platform firmware corruption, and recovers the platform if the firmware were to be corrupted, in accordance with recommendation published in *National Institutes of Standards and Technology (NIST) Special Publication 800-193: Platform Firmware Resiliency Guidelines*.

PFR can further be hardened by including physical security features like screws and interlock mechanisms.

The main features of the PRoT and PFR include:

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

The AX3000 Trusted Compute Unit (TCU) contains a built-in RISC-V execution engine which, along with the One Time Programmable (OTP) memory, Secure Vault (SVT), Read Only Memory (ROM), and Physically Unclonable Function (PUF) blocks, forms the Hardware Root-of-Trust (HWRoT). A block diagram of the HWRoT is shown in Figure 12.

The execution engine boots from the ROM, copies code from the off-chip Flash to the on-chip SRAM, then authenticates the code using the SVT block. The PUF provides a seed for the secret keys, while the OTP provides on-board persistent storage for the secure HWRoT configuration data.

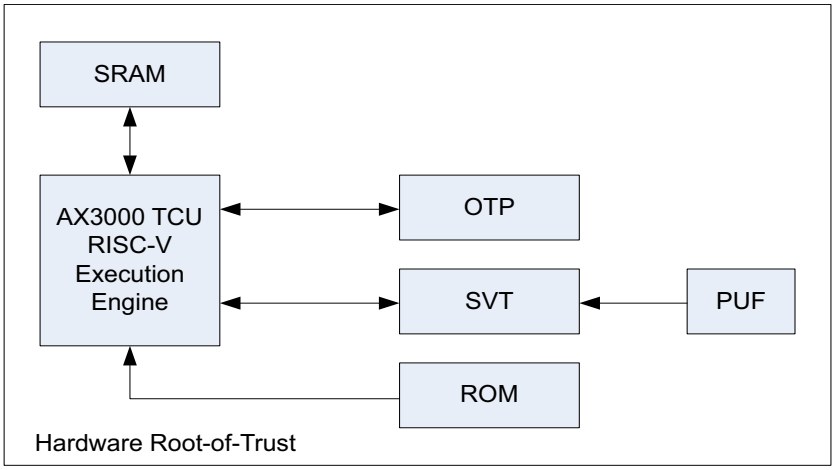

Figure 12. AX3000 RoT Block Diagram

10.8 DC-SCM FPGA

The Project Tahoe DC-SCM board uses an AMD Spartan 7 as the DC-SCM FPGA and is critical in enabling a variety of key features of the board.

10.8.1 Secure Boot and Dual Boot

The current version of the Project Tahoe board does not support Secure boot and Dual boot for SCM FPGA.

10.8.2 LTPI

The DC-SCM LTPI architecture complies with the OCP DC-SCM 2.0 LVDS Tunneling Protocol & Interface Specification.

The Project Tahoe DC-SCM board LTPI interface supports:

- Low Latency (LL) — up to 32 GPIO (16 GPI and 16 GPO)
- Normal Latency (NL) — up to 32 GPIO (16 GPI and 16 GPO)
- I2C — up to 6 over LTPI
- UART — up to 2

Table 13 shows the GPIO to LTPI mapping. In this table:

- GPIO Type LL = Low Latency
- GPIO Type NL = Normal Latency

Table 13. SCM FPGA GPIO to LTPI Mapping

Number	TCU Pin Name	TCU Ball Number	FPGA Pin	Direction	GPIO Type
0	TCU_GPIO_25	AJ32	L4	Input	LL
1	TCU_GPIO_26	AJ30	K4	Input	LL
2	TCU_GPIO_27	AK31	L8	Input	LL
3	TCU_GPIO_28	AJ31	K8	Input	LL
4	TCU_GPIO_29	AE28	M8	Input	LL
5	TCU_GPIO_30	AE27	R4	Input	LL
6	TCU_GPIO_31	AF28	M4	Input	LL
7	TCU_GPIO_54	AF27	L5	Input	LL
8	TCU_GPIO_55	AJ29	L1	Input	LL
9	TCU_GPIO_56	AH28	K1	Input	LL
10	TCU_GPIO_57	AG27	M2	Input	LL
11	TCU_GPIO_58	AJ23	M1	Input	LL
12	TCU_GPIO_59	AH27	N4	Input	LL
13	TCU_GPIO_60	AG26	T21	Input	LL
14	TCU_GPIO_61	AK24	T22	Input	LL
15	TCU_GPIO_62	AL26	V21	Input	LL
0	TCU_GPIO_63	AP30	W22	Output	LL
1	TCU_GPIO_123	E26	A19	Output	LL
2	TCU_GPIO_124	F24	E17	Output	LL
3	TCU_GPIO_125	F25	E18	Output	LL
4	TCU_GPIO_202	AJ10	U22	Output	LL
5	TCU_GPIO_203	AP6	V22	Output	LL
6	TCU_GPIO_204	AN6	W21	Output	LL
7	TCU_GPIO_205	AG11	Y21	Output	LL
8	TCU_GPIO_206	AP5	U20	Output	LL
9	TCU_GPIO_207	AM5	V20	Output	LL

Table 13. SCM FPGA GPIO to LTPI Mapping (Continued)

Number	TCU Pin Name	TCU Ball Number	FPGA Pin	Direction	GPIO Type
10	TCU_GPIO_208	AH8	U18	Output	LL
11	TCU_GPIO_209	AP4	U19	Output	LL
12	TCU_GPIO_210	AM4	P15	Output	LL
13	TCU_GPIO_211	AN4	P16	Output	LL
14	TCU_GPIO_212	AH7	P17	Output	LL
15	TCU_GPIO_213	AK4	R18	Output	LL
0	TCU_GPIO_214	AN3	T17	Input	NL
1	TCU_GPIO_215	AP2	U17	Input	NL
2	TCU_GPIO_216	AM3	R16	Input	NL
3	TCU_GPIO_217	AJ5	R17	Input	NL
4	TCU_GPIO_218	AG8	R19	Input	NL
5	TCU_GPIO_219	AG7	R20	Input	NL
6	TCU_GPIO_220	AF8	T19	Input	NL
7	TCU_GPIO_221	AM2	T20	Input	NL
8	TCU_GPIO_222	AL2	Y20	Input	NL
9	TCU_GPIO_223	AL3	AA20	Input	NL
10	TCU_GPIO_234	AN2	Y22	Input	NL
11	TCU_GPIO_235	AN1	AA22	Input	NL
12	TCU_GPIO_236	AK3	W18	Input	NL
13	TCU_GPIO_237	AM1	Y19	Input	NL
14	TCU_GPIO_238	AK1	AA21	Input	NL
15	TCU_GPIO_239	AJ4	AB21	Input	NL
0	TCU_GPIO_240	AJ2	AB19	Output	NL
1	TCU_GPIO_241	AJ1	AB20	Output	NL
2	TCU_GPIO_242	AH6	V18	Output	NL
3	TCU_GPIO_243	AG6	V19	Output	NL
4	TCU_GPIO_244	AH5	T16	Output	NL
5	TCU_GPIO_245	AJ3	A21	Output	NL
6	TCU_GPIO_246	AG5	F17	Output	NL
7	TCU_GPIO_247	AH4	F18	Output	NL
8	TCU_GPIO_248	AH2	H17	Output	NL
9	TCU_GPIO_249	AG1	G17	Output	NL
10	TCU_GPIO_250	AG4	J17	Output	NL
11	TCU_GPIO_251	AG2	H18	Output	NL
12	TCU_GPIO_252	AH3	H16	Output	NL
13	TCU_GPIO_253	AH1	G16	Output	NL
14	TCU_GPIO_254	AF3	K16	Output	NL
15	TCU_GPIO_255	AG3	J16	Output	NL

Table 13. SCM FPGA GPIO to LTPI Mapping (Continued)

Number	TCU Pin Name	TCU Ball Number	FPGA Pin	Direction	GPIO Type
0	TCU_UART_0_RXD	AH24	D20	Input	---
0	TCU_UART_0_TXD	AJ24	C20	Output	---
1	TCU_UART_1_RXD	AP22	B7	Input	---
1	TCU_UART_1_TXD	AN21	D8	Output	---
0	TCU_I2C_0_SCL	AJ27	J19	Input/Output	---
0	TCU_I2C_0_SDA	AH26	J20	Input/Output	---
1	TCU_I2C_1_SCL	AJ26	L18	Input/Output	---
1	TCU_I2C_1_SDA	AK28	L19	Input/Output	---
2	TCU_I2C_2_SCL	AN27	H19	Input/Output	---
2	TCU_I2C_2_SDA	AP28	G20	Input/Output	---
3	TCU_I2C_3_SCL	AK23	G21	Input/Output	---
3	TCU_I2C_3_SDA	AN26	G22	Input/Output	---
4	TCU_I2C_4_SCL	A18	C15	Input/Output	---
4	TCU_I2C_4_SDA	E17	C16	Input/Output	---
5	TCU_I2C_5_SCL	B18	B15	Input/Output	---
5	TCU_I2C_5_SDA	G18	B16	Input/Output	---

Table 14 shows the FPGA to DC-SCI pin mapping.

Table 14. SCM FPGA to DC-SCI Pin Mapping

FPGA Pin#	DC-SCI Pin Name	DC-SCI Pin#
U15	LTPI_SCM_HPM_DATA_DN	A20
T14	LTPI_SCM_HPM_DATA_DP	A21
Y17	LTPI_SCM_HPM_CLK_DN	A23
W17	LTPI_SCM_HPM_CLK_DP	A24
V15	LTPI_HPM_SCM_DATA_DN	B20
V14	LTPI_HPM_SCM_DATA_DP	B21
AB14	LTPI_HPM_SCM_CLK_DN	B23
AA14	LTPI_HPM_SCM_CLK_DP	B24
P7	ESPI_HPMCNTRL_IO_0	B4
N7	ESPI_HPMCNTRL_IO_1	B5
R7	ESPI_HPMCNTRL_IO_2	B6
R6	ESPI_HPMCNTRL_IO_3	B7
R5	ESPI_HPMCNTRL_RESET_N	B3
M7	ESPI_HPMCNTRL_CLK	B1
R3	ESPI_HPMCNTRL_CS0_N	B2
C8	I2C_I3C_1V8_17_SCL / ESPI0_HPMCNTRL_CS1_N	B9
N3	ESPI_HPMCNTRL_ALERT0_N	B8

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

This section is not applicable for this version of the Project Tahoe DC-SCM board.

12. Mechanical

12.1 General Overview

The Project Tahoe DC-SCM board supports the vertical External Form Factor configuration that complies with the OCP DC-SCM Rev2.0 Ver1.0 Base Specification.

- External Form Factor (EFF). This form factor is used in servers where the Project Tahoe DC-SCM board is installed vertically at the front/rear of the server.

12.2 Keep-out Zones

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

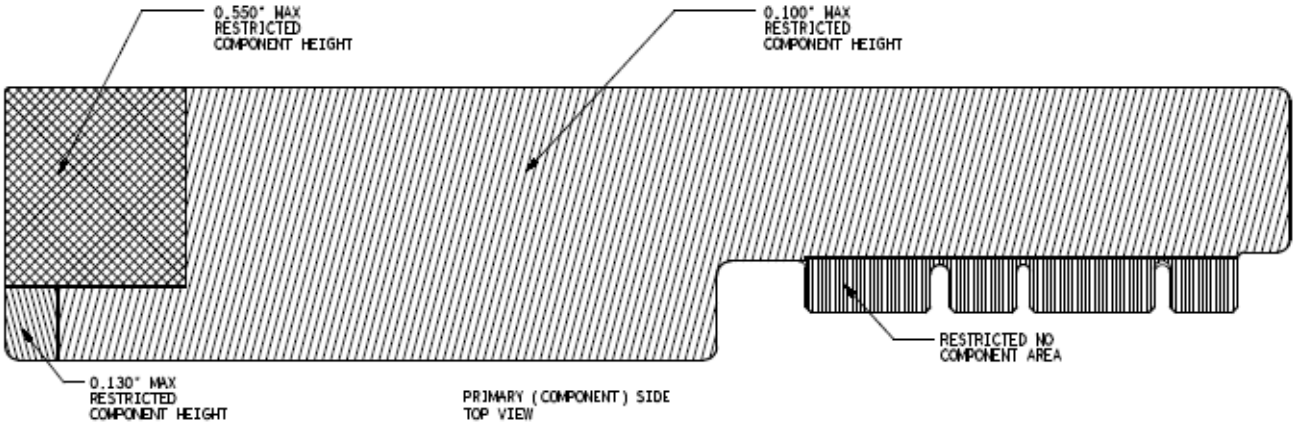

Figure 13. Keep-out Zones — Top Side

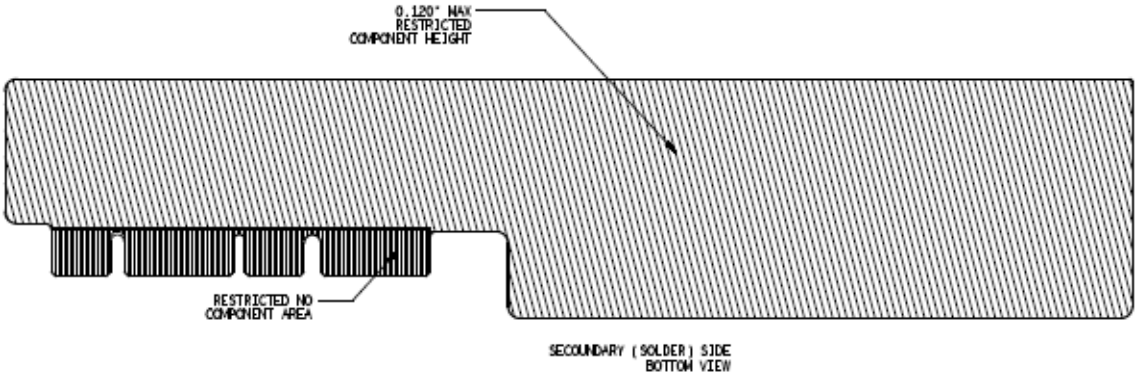

Figure 14. Keep-out Zones — Bottom Side

12.3 I/O Faceplate Bracket Subassembly

The I/O faceplate bracket is shown in Figure 15.

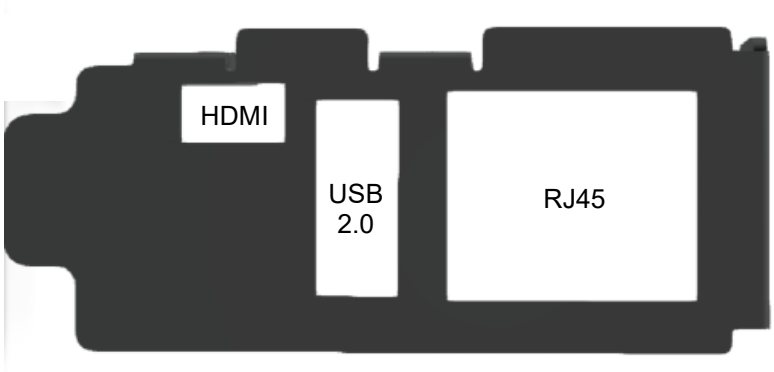

Figure 15. Faceplate Bracket Subassembly

12.4 Module Assembly Overview

The module assembly is shown Figure 16 below.

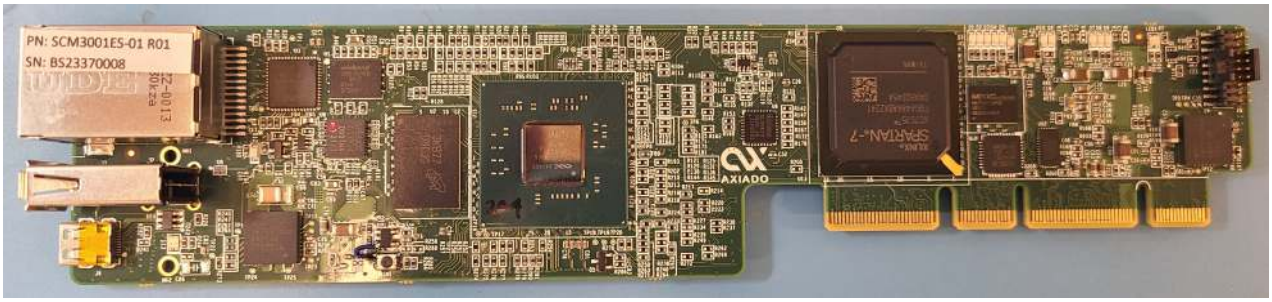

Figure 16. Module Assembly Overview

12.5 Front Panel Definition

The Project Tahoe DC-SCM board contains the following user accessible ports:

- One 1G RJ-45 Ethernet port
- One USB Type A port
- One micro-HDMI connector

12.5.1 1G RJ-45 Ethernet Port

The Project Tahoe DC-SCM board incorporates one 1G Ethernet port via an RJ-45 jack to provide Ethernet connectivity with the AX3000 TCU processor.

12.5.2 USB Interface

The Project Tahoe DC-SCM board contains one customer-visible type-A USB port. The main use case for this port is for a locally attached keyboard or mouse. If a keyboard or mouse is locally attached, the AX3000 TCU shall detect this and proxy the inputs from these devices to the HPM. The board also supports interfacing to an external USB hub if the system requires multiple USB devices.

12.5.3 HDMI Connector

The Project Tahoe DC-SCM board provides a micro-HDMI connector that can be used as a host graphics interface.

13. Onboard Power System

The power topology for Project Tahoe DC-SCM board is shown in Figure 17.

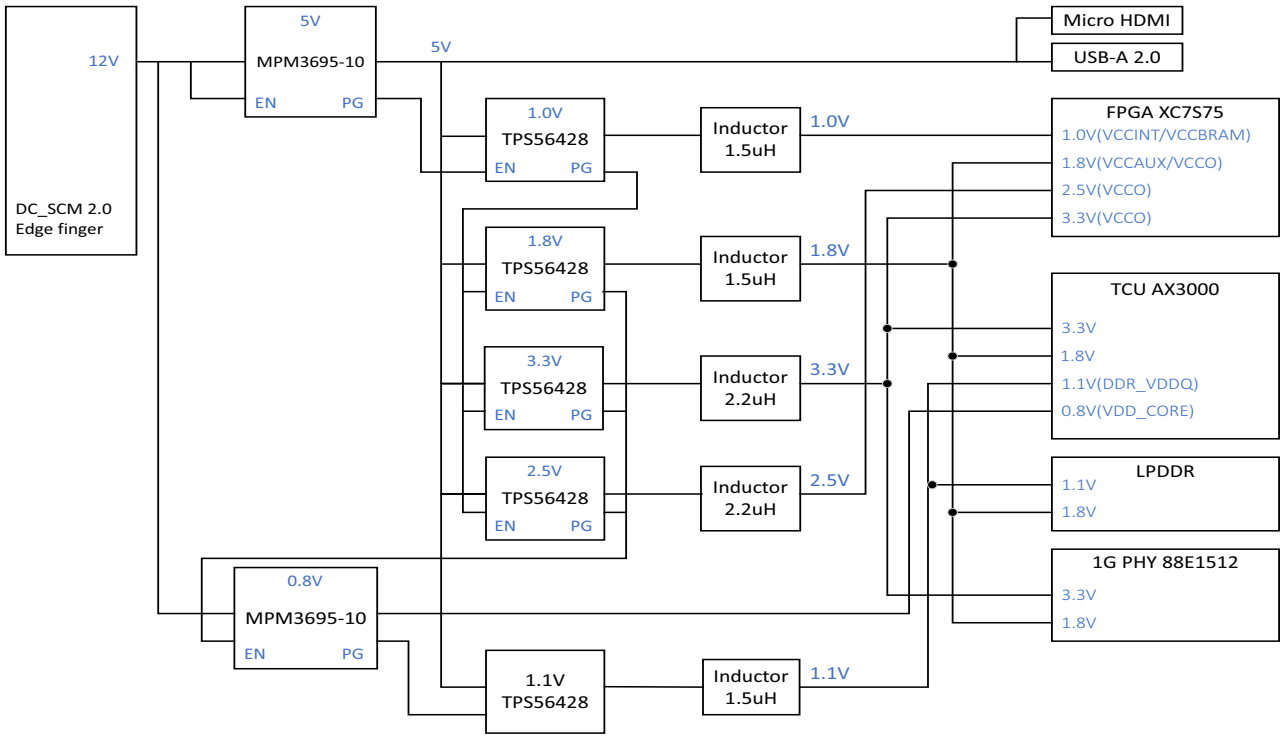

Figure 17. Power Delivery Block Diagram

14. Environmental Regulations/Environmental Requirements

Table 15. Environmental Regulations

Target Category	Applicable Specification
Immunity (ESD)	EN 55035 2017, and IEC 61000-4-2 2008 for ESD. EN 55024 may alternatively be reported. Required ±4 kV contact discharge and ±8 kV air discharge. Note: EN55024 is scheduled to be superseded by EN55035. Project Tahoe DC-SCM 2.0 implementers are encouraged to test to EN55035 to avoid recertifying their product when EN55024 is withdrawn.
REMI (Radiation test)	Radiation testing for ANSI C63.4/CISPR 32. Required -5dB based on Class A regulatory limits.
CEMI (conduction test)	Conduction testing for ANSI C63.4/CISPR 32. Required -5dB based on Class A regulatory limits.
Immunity	EN 55035 2017, and IEC 61000-4-6 for CS. Required 3 Vrms, Criteria.
(Conducted Immunity, CS)	A
Immunity (Electrical Fast Transient, EFT)	EN 55035 2017, and IEC 61000-4-4 for EFT. Required +/-1 kV, Criteria B on Mains and +/-0.5 kV, Criteria B on I/O.
Operating Condition	Operating Altitude: Sea level to 5000 feet. Operating relative humidity: 8 - 85%.
Environmental	RoHS Directive 2011/65/EU and Amendment (EU) 2015/863. European Commission Regulation Number 1907/2006 concerning the Registration, Evaluation, Authorization and Restriction of Chemicals (REACH).

15. Prescribed Materials

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

16. Software Support (recommended)

This section is not applicable to this version of the Project Tahoe DC-SCM board.

17. System Firmware

This section is not applicable to this version of the Project Tahoe DC-SCM board.

18. Hardware Management

- The Project Tahoe DC-SCM board includes a dedicated RJ45 jack with 1GbE port for Baseboard Management Controller (BMC) Out Of Bound (OOB) manageability via embedded PHY controller.
- The Baseboard Management Controller (BMC) has 1GB DRAM and 128MB Flash for firmware storage.
- Firmware for the BMC, BIOS, and SCM FPGA can be updated online. Axiado supports OpenBMC version 2.12.
- Supports monitoring of 12V AUX input and other voltage rails.

19. Security (only for Platform Boards and Systems)

This section is not applicable to this version of the Project Tahoe DC-SCM board.

20. Interoperability and FRU Requirements

20.1 HPM FRU Requirements

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

Table 16. HPM FRU Requirements

Offset	Field Length	Field	Value	Notes
0	1	Record Type ID	0xC1	
1	1	7:7 - End of list 6:4 - Reserved, write as 000b 3:0 - Record Format version		
2	1	Record Type ID		
3	1	Record Checksum (zero checksum)		
4	1	Header Checksum (zero checksum)		
5	3	Manufacture ID	0x7F 0xA6 0x00	OCP INIA assigned ID 0x00A67F (LSB first)
8	1	OCP DC-SCM 2.0 FRU OEM Record Version	0x00 - Reserved 0x01 - OCP DC-SCM 2.0 card FRU record released with version 1.0	
9	2	DC-SCM Revision 15:8 Major number 7:0 Minor number	0x02 0x00	Revision 2.0
11	1	DC-SCM version 7:4 Major number 3:0 Minor number	0x1 0x0	Version 1.0
12	2	LTPI Revision 15:8 - Major number 7:0 - Minor number	0x1 0x0	Version 1.0
14	1	LTPI Version 7:4 - Major number 3:0 - Minor number	0x1 0x0	Version 1.0
15	1	DC-SCM type	0x00 - not any defined type 0x01 - 0xFF Reserved	
16	16	Reserved	Reserved set to 0xFF	
31	32	OEM		Board ID, type, etc.

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

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

Table 17. Approval Checklist

Item	Status Details	Link to Detailed Explanation
Is this contribution entered into the OCP Contribution Portal?	Yes/No	If no, please state reason.
Was it approved in the OCP Contribution Portal?		If no, please state reason.
Is there a Supplier(s) that is building a product based on this Spec? (Supplier must be an OCP Solution Provider)		
Will Supplier(s) have the product available for GENERAL AVAILABILITY within 120 days?		