Express-ID7/R

User's Guide

intel

COM Express®

Revision: Rev. 1.2
Date: 2024-08-26
Part Number: 50M-72137-1020

ADLINK
LEADING EDGE COMPUTING

Revision History

Revision	Description	Date	Author
1.0	Initial release	2022-06-14	CC
1.1	BIOS info added	2024-05-20	AL
1.2	SKUs added	2024-08-26	AL

Preface

Disclaimer

Information in this document is provided in connection with ADLINK products. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in ADLINK´s Terms and Conditions of Sale for such products, ADLINK assumes no liability whatsoever, and ADLINK disclaims any express or implied warranty, relating to sale and/or use of ADLINK products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. If you intend to use ADLINK products in or as medical devices, you are solely responsible for all required regulatory compliance, including, without limitation, Title 21 of the CFR (US), Directive 2007/47/EC (EU), and ISO 13485 & 14971, if any. ADLINK may make changes to specifications and product descriptions at any time, without notice.

Environmental Responsibility

ADLINK is committed to fulfil its social responsibility to global environmental preservation through compliance with the European Union's Restriction of Hazardous Substances (RoHS) directive and Waste Electrical and Electronic Equipment (WEEE) directive. Environmental protection is a top priority for ADLINK. We have enforced measures to ensure that our products, manufacturing processes, components, and raw materials have as little impact on the environment as possible. When products are at their end of life, our customers are encouraged to dispose of them in accordance with the product disposal and/or recovery programs prescribed by their nation or company.

California Proposition 65 Warning: This product can expose you to chemicals including acrylamide, arsenic, benzene, cadmium, Tris(1,3-dichloro-2-propyl)phosphate (TDCPP), 1,4-Dioxane, formaldehyde, lead, DEHP, styrene, DINP, BBP, PVC, and vinyl materials, which are known to the State of California to cause cancer, and acrylamide, benzene, cadmium, lead, mercury, phthalates, toluene, DEHP, DIDP, DnHP, DBP, BBP, PVC, and vinyl materials, which are known to the State of California to cause birth defects or other reproductive harm. For more information go to www.P65Warnings.ca.gov.

Trademarks

Product names mentioned herein are used for identification purposes only and may be trademarks / registered trademarks of respective companies.

Copyright © 2024 ADLINK Technology Incorporated

Safety Instructions

For user safety, please read and follow all Instructions, **WARNING**s, **CAUTION**s, and **NOTE**s marked in this manual and on the associated equipment before handling/operating the equipment.

Read these safety instructions carefully.

- Keep this manual for future reference.
- Read the specifications section of this manual for detailed information on the operating environment of this equipment.
- Turn off power and unplug any power cords/cables when installing/mounting or un-installing/removing equipment.
- To avoid electrical shock and/or damage to equipment:
- Keep equipment away from water or liquid sources;
- Keep equipment away from high heat or high humidity;
- Keep equipment properly ventilated (do not block or cover ventilation openings);
- Make sure to use recommended voltage and power source settings;
- Always install and operate equipment near an easily accessible electrical socket outlet;
- Secure the power cord (do not place any object on/over the power cord);
- Only install/attach and operate equipment on stable surfaces and/or recommended mountings;
- If the equipment will not be used for long periods of time, turn off the power source and unplug the equipment.

Conventions

The following conventions may be used throughout this manual, denoting special levels of information

Note: This information adds clarity or specifics to text and illustrations.

Caution: This information indicates the possibility of minor physical injury, component damage, data loss, and/or program corruption.

Warning: This information warns of possible serious physical injury, component damage, data loss, and/or program corruption.

Getting Service

Ask an Expert: https://www.adlinktech.com/en/Askanexpert

ADLINK Technology, Inc.
No. 66, Huaya 1st Rd., Guishan District, Taoyuan City 333411, Taiwan
Tel: +886-3-216-5088
Fax: +886-3-328-5706
Email: service@adlinktech.com

Ampro ADLINK Technology, Inc.
6450 Via Del Oro, San Jose, CA 95119-1208, USA
Tel: +1-408-360-0200
Toll Free: +1-800-966-5200 (USA only)
Fax: +1-408-600-1189
Email: info@adlinktech.com

ADLINK Technology (China) Co., Ltd.
300 Fang Chun Rd., Zhangjiang Hi-Tech Park, Pudong New Area, Shanghai, 201203, China
Tel: +86-21-5132-8988
Fax: +86-21-5132-3588
Email: market@adlinktech.com

ADLINK Technology GmbH
Hans-Thoma-Strasse 11, D-68163 Mannheim, Germany
Tel: +49-621-43214-0
Fax: +49-621 43214-30
Email: emea@adlinktech.com

Please visit the Contact page at www.adlinktech.com for information on how to contact the ADLINK regional office nearest you.

Table of Contents

List of Figures

1. Introduction

The Express-ID7 is the first **COM Express® COM.0 R3.1 Basic Size Type 7** module based on the new generation and longevity, future-focused Intel® Xeon-D processors (formerly "Ice Lake D-1700") supporting up to 10 cores, extended operating temperature range for selected SKUs, and integrated 10G Ethernet connectivity, making it highly suited for mission-critical applications. Its 10 cores at 70 watts TDP combined with Intel® AVX-512 Vector Neural Network Instructions (VNNI) can optimize AI inferencing performance at the edge. Industries in need of such high performance, low power consumption, and high bandwidth connectivity include industrial automation and control, intelligent surveillance, video storage analytics, 5G infrastructure at the edge, and more.

The Express-ID7 features Intel® Virtualization Technology (including VT-x, VT-d), Intel® Hyper-Threading Technology, Intel® Trusted Execution Technology, Intel® AES-NI Technology, and up to 4 SO-DIMMs supporting a maximum of 128GB DDR4 ECC (or non-ECC) memory capacity with triple-channel memory design at up to 2933 MT/s (dependent on processor SKU) to provide excellent overall performance.

An integrated Intel® 10G Ethernet controller supports four 10GBASE-KR interfaces, with relevant sideband signals effectively reducing hardware and firmware complexity for system integration. The Express-ID7 is designed to serve customers requiring optimized computing capability per watt and high speed connectivity requirements who want to outsource the custom core logic of their systems for reduced development time.

Input/output features include 16 PCIe Gen4 lanes, 16 PCIe Gen3 lanes, a single onboard Gigabit Ethernet port with NC-SI, 4x USB 3.0/2.0 ports, and 2x SATA 6 Gb/s ports. Support for SMBus and I^2C is also provided. The module is equipped with SPI AMI EFI BIOS with CMOS backup, supporting embedded features such as remote console, hardware monitor, and watchdog timer.

2. Specifications

2.1. Core System

CPU

Intel® Xeon® D-1700 Processor (formerly "Ice Lake D")

- Intel(R) Xeon(R) D-1848TER 2.0/3.1GHz, 15MB, 57W (10C/20T, eTEMP) (up to 2667MT/s)
- Intel(R) Xeon(R) D-1813NT 2.2/2.4GHz, 10MB, 42W (4C/8T) (up to 2400MT/s)
- Intel® Xeon® D-1746TER 2.0/3.1GHz, 15MB, 67W (10C/20T, eTEMP) (up to 2667 MT/s)
- Intel® Xeon® D-1735TR 2.2/3.4GHz, 15MB, 59W (8C/16T) (up to 2933 MT/s)
- Intel® Xeon® D-1732TE 1.9/3.0GHz, 15MB, 52W (8C/16T, eTEMP) (up to 2667 MT/s)
- Intel® Xeon® D-1715TER 2.4/3.5GHz, 10MB, 50W (4C/8T, eTEMP) (up to 2667 MT/s)
- Intel® Xeon® D-1712TR 2.0/3.1GHz, 10MB, 40W (4C/8T) (up to 2400 MT/s)

Note: Other non-IOTG SKUs (D-1748TE, D-1718T) and non-IOTG SKUs with Intel® QAT feature (D-1749NT, D-1747NTE, D-1736NT, D-1733NT, D-1734NT, D-1713NTE, D-1713NT) may be available by project basis.

Supporting: Intel® VT (including VT-x, VT-d, VT-x with Extended Page Tables), Intel® HT Technology, Intel® SSE4.2, Intel® 64 Architecture, Intel® Turbo Boost Technology 2.0, Intel® AVX512-VNNI, Intel® TSX-NI, Intel® Platform Protection Technology with Intel® TXT and Execute Disable Bit, Intel® Data Protection Technology with Intel® Secure Key and Intel® AES-NI (availability of features may vary between processor SKUs)

Memory

Up to 128GB DDR4, three memory channel in total four SODIMM sockets, maximum 32GB per socket, ECC or non-ECC

Up to 2933 MT/s memory speed (dependent on SKUs and 1DPC/2DPC usage)

Four SODIMM sockets supported by build option and project basis

Cache

15MB: D-1848TER, D-1746TER, D-1735TR, D-1732TE

10MB: D-1813NT, D-1715TER, D-1712TR

Embedded BIOS

AMI Aptio V UEFI with CMOS backup in 32 MB SPI BIOS, dual BIOS by build option

2.2. Expansion Busses

16 PCI Express Gen4: Lane 16-31 (four controllers, configurable to 1 x16, 2 x8, or 4 x4)
Refer to Ch. 4 Pinout and Signal Descriptions for details on Gen4 clock, PCIE_CK_REF1 (pin B29/B30)

8 PCI Express Gen3: Lanes 0-7 (four controllers, configurable to 1 x8, 2 x4, 4 x2/x1)

8 PCI Express Gen3: Lane 8-15 (four controllers, configurable to 1 x8, 2 x4, 4 x2/x1)

Note: Additional PCIe x1 at Lane 1 and Lane 5 are supported by build option and project basis.
PCIE_CK_REF (A88/A89) for Lane 16-31 (with up to Gen3 speed) is supported by build option and project basis.
Combined HSIO has a bandwidth up to the equivalent of 16 PCIe Gen3 lanes; PCIe lane 0-15, SATA, GbE and USB SSTX/RX are sourced from HSIO.

Other: SMBus (system), I^2C (user), LPC bus

2.3. 10G-KR Ethernet

Intel® Ethernet Controller integrated on SoC

Four 10GBASE-KR and sideband signals

PHY on carrier and ID EEPROM and PHY firmware are required for 10G SFP+ and/or Copper 10GBASE-T applications

The recommended PHY for SFP+ is C827, for 10GBASE-T is X557-AT4. The enablement of other PHY may require platform supplier support.

10G Ethernet Controller firmware is combined with BIOS code and stored on the same SPI ROM

10G Ethernet Controller firmware for 10K-KR backplane usage is different than that for 10G SFP+/10GBASE-T usage.

10G SFP+/10GBASE-T use the same firmware and are supported by default while 10G-KR backplane firmware is supported by build option and project basis.

Note: For detailed information about circuit design between the Ethernet controller, Optical Fiber/Copper PHY and firmware, please contact your local ADLINK representative
40GBASE-KR4 support requires the use of 4 KR lanes, which is supported by project basis (TBC).

2.4. GbE Ethernet

Intel® Ethernet Controller I210 Series

1000/100/10 Mbit/s connections

NC-SI and GBE0_SDP are supported on select SKU

2.5. Multi I/O and Storage

USB

4x USB 3.0/2.0/1.1 (USB 0, 1, 2, 3)

SuperSpeed, High-Speed, Full-Speed and Low-Speed USB signaling

USB_OC pins share the same source, from SOC

SATA

2x SATA 6Gb/s (SATA 0,1)

Note: Combined HSIO has a bandwidth up to the equivalent of 16 PCIe Gen3 lanes; PCIe lane 0-15, SATA, GbE and USB SSTX/RX are sourced from HSIO.

UART

Two UART interfaces SER0 and SER1 RX/TX on module
Console Redirection COM 1 or COM 2 selectable in BIOS

Up to 4 serial ports supported by standard BIOS, including Super I/O on carrier board

COM Port	Description	IRQ	Address	Console Redirection Support
COM 1	Supported by module (SER0, A98/A99), via embedded controller	4	0x3F8	Yes
COM 2	Supported by module (SER1, A101/A102), via embedded controller	3	0x2F8	Yes
COM 3	Supported by Super I/O (W83627DHG) on carrier board	5	0x240	Yes
COM 4	Supported by Super I/O (W83627DHG) on carrier board	7	0x248	Yes

SER0, SER1 from SoC HSUART are supported by BOM option and project basis

GPIO ~~or SD~~

4 GPO and 4 GPI (GPI with interrupt, TBC)

2.6. Trusted Platform Module (TPM)

Chipset: Infineon solution

Type: TPM 2.0 (SPI bus based)

2.7. SEMA Board Controller

Supports: Voltage/current monitoring, power sequence debug support, AT/ATX mode control, logistics and forensic information, flat panel control, general purpose I2C, failsafe BIOS (dual BIOS, opt. support), watchdog timer and fan control

2.8. Debug

30-pin flat cable connector for use with DB30 x86 debug module

Supports embedded controller access, SPI BIOS flashing, internal power rail test points, debug LEDs, and BIOS POST code LED

2.9. Power

Power Modes: AT and ATX mode (AT mode startup controlled by SEMA Board Controller)

Standard Voltage Input: AT: 12V±5% or ATX: 12V±5% / 5Vsb ±5%

Power Management: ACPI 5.0 compliant

Power States: C0-C3, S0, S5, S5 ECO mode (WoL S5)

ECO Mode support for deep S5 for 5Vsb power saving

Note: For ATX power source, a minimum interval of 10ms is required from SUS_S3# fall to VCC_12V fall.

Power Consumption
Please contact our ADLINK representative for the document "COM Express Module Power Consumption."

2.10. Mechanical and Environmental

Form Factor and specification

PICMG COM Express Rev 3.1 (COM.0 R3.1), Type 7, Basic size 125 x 95 mm

Operating Temperature

Standard	0°C to 60°C	Storage: -20°C to 80°C
Extreme Rugged	-40°C to 85°C	Storage: -40°C to 85°C (build option by project basis, selected SoC SKUs, TBC)

Humidity

5-90% RH operating, non-condensing, 5-95% RH storage (and operating with conformal coating)

Shock and Vibration

IEC 60068-2-64 and IEC-60068-2-27
MIL-STD-202F, Method 213B, Table 213-I, Condition A and Method 214A, Table 214-I, Condition D

HALT tested

Thermal Stress, Vibration Stress, Thermal Shock and Combined Test

3. Block Diagram

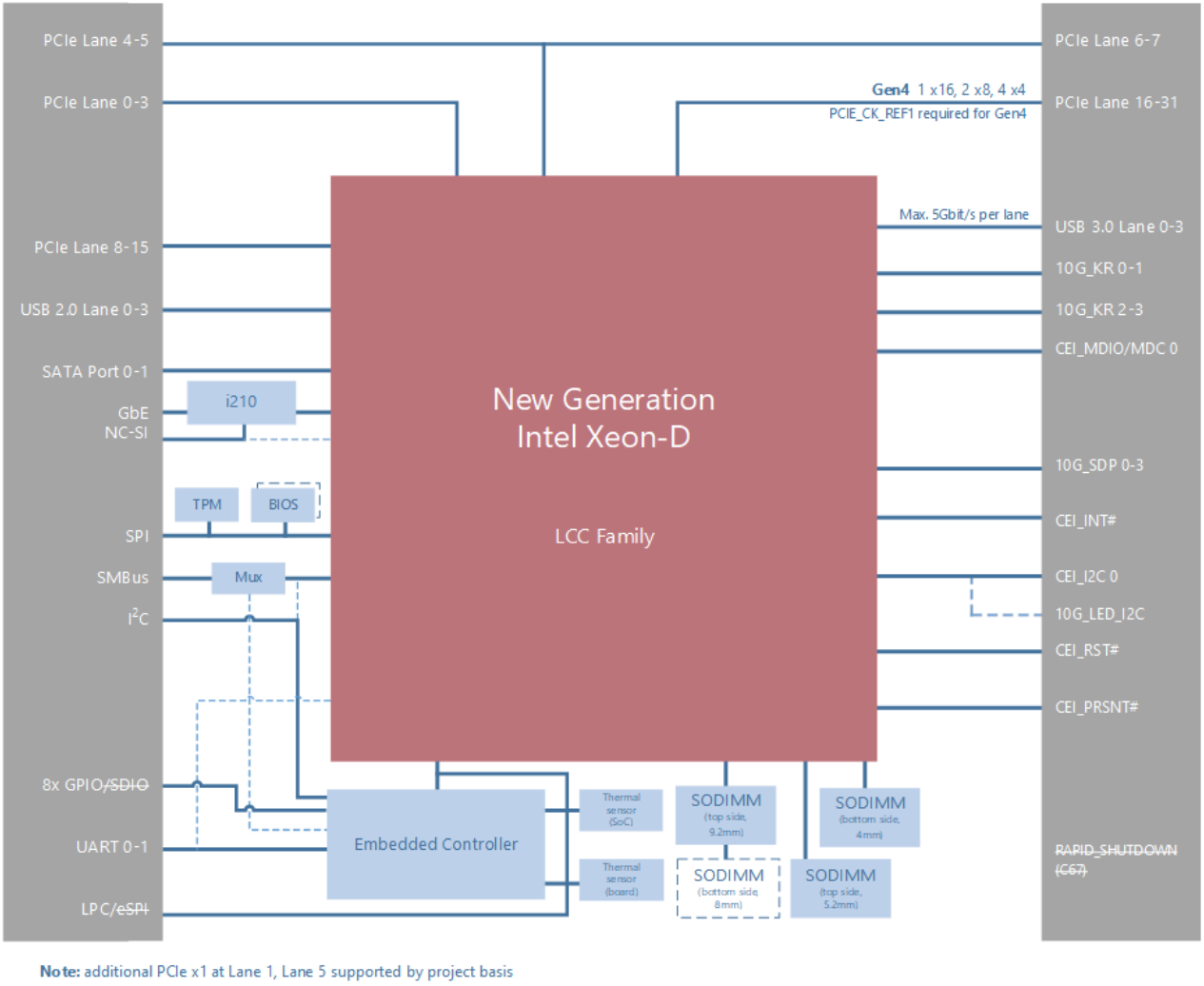


Figure 1 – Module functional block diagram

4. Pinout and Signal Descriptions

4.1. Pin Summary

The table below is a comprehensible list of all signal pins supported on the dual 220-pin COM Express connectors as defined for Type 7 in the PICMG COM.0 R3.1 specification. Signals described in the specification but not supported on the Express-ID7 are strikethrough ~~STRIKETHROUGH~~

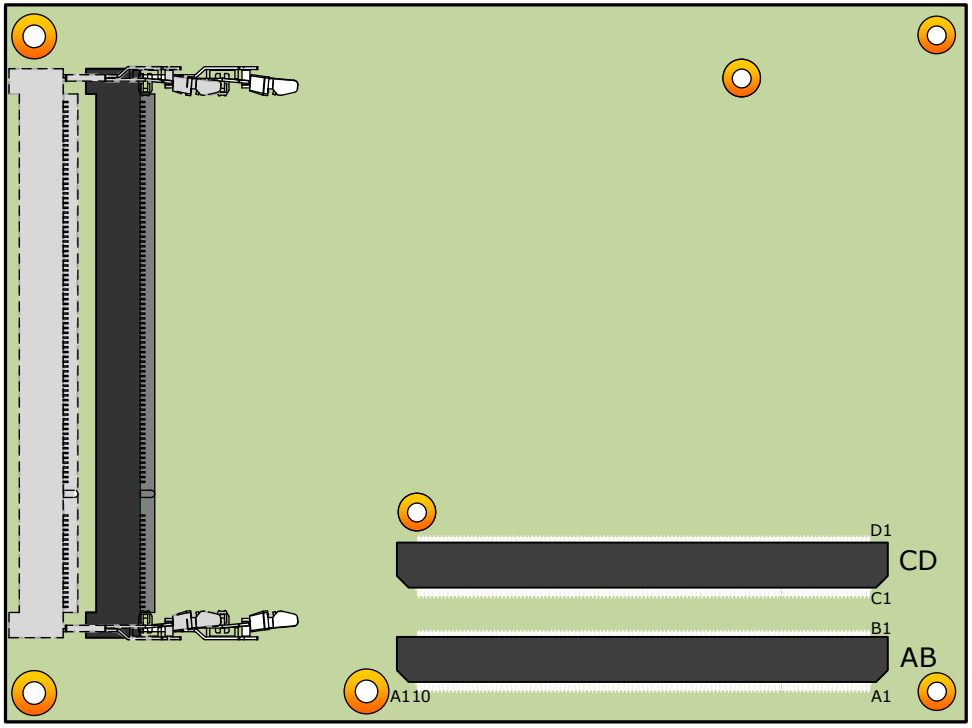


Figure 2 - Module rear side row and pin numbering

Note: The 4th SO-DIMM (grey color) is supported by build option.

Row A			Row B			Row C			Row D	
A1	GND (fixed)		B1	GND (fixed)		C1	GND (fixed)		D1	GND (fixed)
A2	GBE0_MDI3-		B2	GBE0_ACT#		C2	GND		D2	GND
A3	GBE0_MDI3+		B3	LPC_FRAME#		C3	USB_SSRX0-		D3	USB_SSTX0-
A4	GBE0_LINK100#		B4	LPC_AD0		C4	USB_SSRX0+		D4	USB_SSTX0+
A5	GBE0_LINK1000#		B5	LPC_AD1		C5	GND		D5	GND
A6	GBE0_MDI2-		B6	LPC_AD2		C6	USB_SSRX1-		D6	USB_SSTX1-
A7	GBE0_MDI2+		B7	LPC_AD3		C7	USB_SSRX1+		D7	USB_SSTX1+
A8	GBE0_LINK#		B8	~~LPC_DRQ0#~~		C8	GND		D8	GND
A9	GBE0_MDI1-		B9	~~LPC_DRQ1#~~		C9	USB_SSRX2-		D9	USB_SSTX2-
A10	GBE0_MDI1+		B10	LPC_CLK		C10	USB_SSRX2+		D10	USB_SSTX2+
A11	GND (fixed)		B11	GND (fixed)		C11	GND (fixed)		D11	GND (fixed)
A12	GBE0_MDI0-		B12	PWRBTN#		C12	USB_SSRX3-		D12	USB_SSTX3-
A13	GBE0_MDI0+		B13	SMB_CK		C13	USB_SSRX3+		D13	USB_SSTX3+
A14	GBE0_CTREF		B14	SMB_DAT		C14	GND		D14	GND
A15	SUS_S3#		B15	SMB_ALERT#		C15	~~10G_PHY_MDC_SCL3~~		D15	~~10G_PHY_MDIO_SDA3~~
A16	SATA0_TX+		B16	SATA1_TX+		C16	~~10G_PHY_MDC_SCL2~~		D16	~~10G_PHY_MDIO_SDA2~~
A17	SATA0_TX-		B17	SATA1_TX-		C17	10G_SDP2		D17	10G_SDP3
A18	SUS_S4#		B18	~~SUS_STAT#~~		C18	GND		D18	GND
A19	SATA0_RX+		B19	SATA1_RX+		C19	PCIE_RX6+		D19	PCIE_TX6+
A20	SATA0_RX-		B20	SATA1_RX-		C20	PCIE_RX6-		D20	PCIE_TX6-
A21	GND (fixed)		B21	GND (fixed)		C21	GND (fixed)		D21	GND (fixed)
A22	PCIE_TX15+		B22	PCIE_RX15+		C22	PCIE_RX7+		D22	PCIE_TX7+
A23	PCIE_TX15-		B23	PCIE_RX15-		C23	PCIE_RX7-		D23	PCIE_TX7-
A24	SUS_S5#		B24	PWR_OK		C24	~~10G_INT2~~		D24	~~10G_INT3~~
A25	PCIE_TX14+		B25	PCIE_RX14+		C25	GND		D25	GND
A26	PCIE_TX14-		B26	PCIE_RX14-		C26	10G_KR_RX3+		D26	10G_KR_TX3+
A27	BATLOW#		B27	WDT		C27	10G_KR_RX3-		D27	10G_KR_TX3-
A28	(S)ATA_ACT#		B28	**GND**		C28	GND		D28	GND
A29	RSVD		B29	**PCIE_CK_REF1+**		C29	10G_KR_RX2+		D29	10G_KR_TX2+
A30	RSVD		B30	**PCIE_CK_REF1-**		C30	10G_KR_RX2-		D30	10G_KR_TX2-
A31	GND (fixed)		B31	GND (fixed)		C31	GND (fixed)		D31	GND (fixed)
A32	RSVD		B32	SPKR		C32	~~10G_SFP_SDA3~~		D32	~~10G_SFP_SCL3~~
A33	RSVD		B33	I2C_CK		C33	~~10G_SFP_SDA2~~		D33	~~10G_SFP_SCL2~~
A34	BIOS_DIS0#		B34	I2C_DAT		C34	~~10G_PHY_RST_23~~		D34	~~10G_PHY_CAP_23~~
A35	THRMTRIP#		B35	THRM#		C35	~~10G_PHY_RST_01_/~~ **CEI_RST#**		D35	~~10G_PHY_CAP_01_/~~ **CEI_PRSNT#**

Row A			Row B			Row C			Row D	
A36	PCIE_TX13+		B36	PCIE_RX13+		C36	10G_LED_SDA *		D36	RSVD
A37	PCIE_TX13-		B37	PCIE_RX13-		C37	10G_LED_SCL *		D37	RSVD
A38	GND		B38	GND		C38	~~10G_SFP_SDA1~~		D38	~~10G_SFP_SCL1~~
A39	PCIE_TX12+		B39	PCIE_RX12+		C39	~~10G_SFP_SDA0 /~~ **CEI_SDA**		D39	~~10G_SFP_SCL0 /~~ **CEI_SCL**
A40	PCIE_TX12-		B40	PCIE_RX12-		C40	10G_SDP0		D40	10G_SDP1
A41	GND (fixed)		B41	GND (fixed)		C41	GND (fixed)		D41	GND (fixed)
A42	USB2-		B42	USB3-		C42	10G_KR_RX1+		D42	10G_KR_TX1+
A43	USB2+		B43	USB3+		C43	10G_KR_RX1-		D43	10G_KR_TX1-
A44	USB_2_3_OC#		B44	USB_0_1_OC#		C44	GND		D44	GND
A45	USB0-		B45	USB1-		C45	~~10G_PHY_MDC_SCL1~~		D45	~~10G_PHY_MDIO_SDA1~~
A46	USB0+		B46	USB1+		C46	~~10G_PHY_MDC_SCL0 /~~ **CEI_MDC**		D46	~~10G_PHY_MDIO_SDA0 /~~ **CEI_MDIO**
A47	VCC_RTC		B47	~~ESPI_EN#~~		C47	~~10G_INT0 /~~ **CEI_INT#**		D47	~~10G_INT1 /~~ **~~ETH0-3_PHY_INT#~~**
A48	RSVD		B48	~~USB0_HOST_PRSNT~~		C48	GND		D48	GND
A49	GBE0_SDP		B49	SYS_RESET#		C49	10G_KR_RX0+		D49	10G_KR_TX0+
A50	LPC_SERIRQ		B50	CB_RESET#		C50	10G_KR_RX0-		D50	10G_KR_TX0-
A51	GND (fixed)		B51	GND (fixed)		C51	GND (fixed)		D51	GND (fixed)
A52	PCIE_TX5+		B52	PCIE_RX5+		C52	PCIE_RX16+		D52	PCIE_TX16+
A53	PCIE_TX5-		B53	PCIE_RX5-		C53	PCIE_RX16-		D53	PCIE_TX16-
A54	GPI0		B54	GPO1		C54	TYPE0#		D54	RSVD
A55	PCIE_TX4+		B55	PCIE_RX4+		C55	PCIE_RX17+		D55	PCIE_TX17+
A56	PCIE_TX4-		B56	PCIE_RX4-		C56	PCIE_RX17-		D56	PCIE_TX17-
A57	GND		B57	GPO2		C57	TYPE1#		D57	TYPE2#
A58	PCIE_TX3+		B58	PCIE_RX3+		C58	PCIE_RX18+		D58	PCIE_TX18+
A59	PCIE_TX3-		B59	PCIE_RX3-		C59	PCIE_RX18-		D59	PCIE_TX18-
A60	GND (fixed)		B60	GND (fixed)		C60	GND (fixed)		D60	GND (fixed)
A61	PCIE_TX2+		B61	PCIE_RX2+		C61	PCIE_RX19+		D61	PCIE_TX19+
A62	PCIE_TX2-		B62	PCIE_RX2-		C62	PCIE_RX19-		D62	PCIE_TX19-
A63	GPI1		B63	GPO3		C63	RSVD		D63	RSVD
A64	PCIE_TX1+		B64	PCIE_RX1+		C64	RSVD		D64	RSVD
A65	PCIE_TX1-		B65	PCIE_RX1-		C65	PCIE_RX20+		D65	PCIE_TX20+
A66	GND		B66	WAKE0#		C66	PCIE_RX20-		D66	PCIE_TX20-
A67	GPI2		B67	WAKE1#		C67	~~RAPID_SHUTDOWN~~		D67	GND
A68	PCIE_TX0+		B68	PCIE_RX0+		C68	PCIE_RX21+		D68	PCIE_TX21+
A69	PCIE_TX0-		B69	PCIE_RX0-		C69	PCIE_RX21-		D69	PCIE_TX21-
A70	GND (fixed)		B70	GND (fixed)		C70	GND (fixed)		D70	GND (fixed)

Row A			Row B			Row C			Row D	
A71	PCIE_TX8+		B71	PCIE_RX8+		C71	PCIE_RX22+		D71	PCIE_TX22+
A72	PCIE_TX8-		B72	PCIE_RX8-		C72	PCIE_RX22-		D72	PCIE_TX22-
A73	GND		B73	GND		C73	GND		D73	GND
A74	PCIE_TX9+		B74	PCIE_RX9+		C74	PCIE_RX23+		D74	PCIE_TX23+
A75	PCIE_TX9-		B75	PCIE_RX9-		C75	PCIE_RX23-		D75	PCIE_TX23-
A76	GND		B76	GND		C76	GND		D76	GND
A77	PCIE_TX10+		B77	PCIE_RX10+		C77	RSVD		D77	RSVD
A78	PCIE_TX10-		B78	PCIE_RX10-		C78	PCIE_RX24+		D78	PCIE_TX24+
A79	GND		B79	GND		C79	PCIE_RX24-		D79	PCIE_TX24-
A80	GND (fixed)		B80	GND (fixed)		C80	GND (fixed)		D80	GND (fixed)
A81	PCIE_TX11+		B81	PCIE_RX11+		C81	PCIE_RX25+		D81	PCIE_TX25
A82	PCIE_TX11-		B82	PCIE_RX11-		C82	PCIE_RX25-		D82	PCIE_TX25-
A83	GND		B83	GND		C83	RSVD		D83	RSVD
A84	NCSI_TX_EN		B84	VCC_5V_SBY		C84	GND		D84	GND
A85	GPI3		B85	VCC_5V_SBY		C85	PCIE_RX26+		D85	PCIE_TX26+
A86	RSVD		B86	VCC_5V_SBY		C86	PCIE_RX26-		D86	PCIE_TX26-
A87	RSVD		B87	VCC_5V_SBY		C87	GND		D87	GND
A88	PCIE0_CK_REF+		B88	BIOS_DIS1#		C88	PCIE_RX27+		D88	PCIE_TX27+
A89	PCIE0_CK_REF-		B89	~~NSCI_RX_ER~~		C89	PCIE_RX27-		D89	PCIE_TX27-
A90	GND (fixed)		B90	GND (fixed)		C90	GND (fixed)		D90	GND (fixed)
A91	SPI_POWER		B91	NCSI_CLK_IN		C91	PCIE_RX28+		D91	PCIE_TX28+
A92	SPI_MISO		B92	NCSI_RXD1		C92	PCIE_RX28-		D92	PCIE_TX28-
A93	GPO0		B93	NCSI_RXD0		C93	GND		D93	GND
A94	SPI_CLK		B94	NCSI_CRS_DV		C94	PCIE_RX29+		D94	PCIE_TX29+
A95	SPI_MOSI		B95	NCSI_TXD1		C95	PCIE_RX29-		D95	PCIE_TX29-
A96	TPM_PP		B96	NCSI_TXD0		C96	GND		D96	GND
A97	TYPE10#		B97	SPI_CS#		C97	RSVD		D97	RSVD
A98	SER0_TX		B98	NCSI_ARB_IN		C98	PCIE_RX30+		D98	PCIE_TX30+
A99	SER0_RX		B99	NCSI_ARB_OUT		C99	PCIE_RX30-		D99	PCIE_TX30-
A100	GND (fixed)		B100	GND (fixed)		C100	GND (fixed)		D100	GND (fixed)
A101	SER1_TX		B101	FAN_PWMOUT		C101	PCIE_RX31+		D101	PCIE_TX31+
A102	SER1_RX		B102	FAN_TACHIN		C102	PCIE_RX31-		D102	PCIE_TX31-
A103	~~LID#~~		B103	~~SLEEP#~~		C103	GND		D103	GND
A104	VCC_12V		B104	VCC_12V		C104	VCC_12V		D104	VCC_12V
A105	VCC_12V		B105	VCC_12V		C105	VCC_12V		D105	VCC_12V

Row A			Row B			Row C			Row D	
A106	VCC_12V		B106	VCC_12V		C106	VCC_12V		D106	VCC_12V
A107	VCC_12V		B107	VCC_12V		C107	VCC_12V		D107	VCC_12V
A108	VCC_12V		B108	VCC_12V		C108	VCC_12V		D108	VCC_12V
A109	VCC_12V		B109	VCC_12V		C109	VCC_12V		D109	VCC_12V
A110	GND (fixed)		B110	GND (FIXED)		C110	GND (FIXED)		D110	GND (FIXED)

Note:

1. 10G SFP+ or 10GBASE-T support is based on CEI mode (sideband signal arrangement related) and requires PHY (C827 or X557-AT4) along with on-carrier firmware, for SFP+ or 10GBASE-T applications. A reference design will be offered. Please contact our ADLINK representative for availability.
2. Another PCIe clock (PCIE_CK_REF1) for up to Gen4 usage is required for PCIe lane 16-31. Check pin B28, B29, B30. To stay at PCIE_CK_REF and only needing up to Gen3 at PCIe lane 16-31, a build option on module to re-route the clock for lane 16-31 is supported by project basis.
3. 10G_LED_I2C (C36, C37) is a build option supported by project basis.
4. USB_0_1_OC# (B44) and USB_2_3_OC# (A44) share the same source, from Ice Lake D.

4.2. Signal Terminology Descriptions

Meaning of the terms used for signal description tables

Term	Description
I	Input to the module
O	Output from the module
I/O	Bi-directional Input / Output
OD	Open drain output from the module
I 3.3V	Input 3.3V tolerant
I 5V	Input 5V tolerant
O 3.3V	Output 3.3V signal level
O 5V	Output 5V signal level
I/O 3.3V	Bi-directional signal 3.3V tolerant
I/O 5V	Bi-directional signal 5V tolerant
I/O $3.3V_{SB}$	Input or output 3.3V tolerant active in standby state
DDC	Display Data Channel
PCIE	PCI Express compatible differential signal
PEG	PCI Express Graphics
SATA	Serial ATA specification Revision 2.6 and 3
LVDS	Low Voltage Differential Signal - 330 mV nominal; 450 mV maximum differential signal
P	Power Input / Output
REF	Reference voltage output. May be sourced from a Module power plane.
PDS	Pull-down strap. A Module output pin that is either tied to GND or is not connected. Used to signal Module capabilities to the Carrier Board.
PU	PU (pull-up) resistor on module
PD	PD (pull-down) resistor on module

4.3. AB Connector Signal Descriptions

4.3.1 Network Controller Sideband Interface (NC-SI)

Name	Pin #	Description	I/O	PU / PD	Comment
NCSI_CLK_IN	B91	Clock reference for receive, transmit and control interface	I 3.3VSB	PD 10K	
NCSI_RXD[1:0]	B92 B93	Receive Data (from NC to BMC)	O 3.3VSB	PU 10K 3.3VSB	PU 10K that aligns with LAN chip specification
NCSI_TXD[1:0]	B95 B96	Transmit Data (from BMC to NC)	I 3.3VSB	PU 10K 3.3VSB	
NCSI_CRS_DV	B94	Carrier Sense/Receive Data valid to MC, indicating that the transmitted data from NC to BMC is valid	O 3.3VSB	PD 10K	PU 10K that aligns with LAN chip specification
NCSI_TX_EN	A84	Transmit enable	I 3.3VSB	PD 10K	
~~NCSI_RX_ER~~	~~B89~~	~~Receive error~~	~~O~~ ~~3.3VSB~~		Not supported
NCSI_ARB_IN	B98	Network Controller hardware arbitration input	I 3.3VSB		Left floating on module, that aligns with LAN chip specification
NCSI_ARB_OUT	B99	Network Controller hardware arbitration output	O 3.3VSB		

Note: NC-SI source from Intel® Ethernet Controller I210.

4.3.2 Gigabit Ethernet

Name	Pin #	Description	I/O	PU / PD	Comment
GBE0_MDI0+ GBE0_MDI0- GBE0_MDI1+ GBE0_MDI1- GBE0_MDI2+ GBE0_MDI2- GBE0_MDI3+ GBE0_MDI3-	A13 A12 A10 A9 A7 A6 A3 A2	Gigabit Ethernet Controller 0: Media Dependent Interface Differential Pairs 0, 1, 2, 3. The MDI can operate in 1000, 100, and 10Mbit/sec modes. Some pairs are unused in some modes according to the following: **1000 / 100 / 10** MDI[0]+/- B1_DA+/- TX+/- TX+/- MDI[1]+/- B1_DB+/- RX+/- RX+/- MDI[2]+/- B1_DC+/- MDI[3]+/- B1_DD+/-	I/O Analog		Twisted pair signals for external transformer.
GBE0_ACT#	B2	Gigabit Ethernet Controller 0 activity indicator, active low.	OD 3.3VSB		
GBE0_LINK#	A8	Gigabit Ethernet Controller 0 link indicator, active low.	OD 3.3VSB		
GBE0_LINK100# *	A4	Gigabit Ethernet Controller 0 100Mbit/sec link indicator, active low.	OD 3.3VSB		
GBE0_LINK1000# *	A5	Gigabit Ethernet Controller 0 1000Mbit/sec link indicator, active low.	OD 3.3VSB		
GBE0_CTREF	A14	Reference voltage for Carrier Board Ethernet channel 1 and 2 magnetics center tap. The reference voltage is determined by the requirements of the Module PHY and may be as low as 0V and as high as 3.3V. The reference voltage output shall be current limited on the Module. In the case in which the reference is shorted to ground, the current shall be 250 mA or less.	REF GND min 3.3V max		Not supported
GBE0_SDP	A49	Gigabit Ethernet Controller 0 Software-Definable Pin. Can also be used for IEEE1588 support such as 1pps signal.	IO 3.3VSB	PU 10K 3.3VSB	Depends on the selection of LAN controller

Note: GBE0_ACT# and GBE0_LINK# share the same pin from LAN controller.

4.3.3 SATA

Name	Pin #	Description	I/O	PU / PD	Comment
SATA0_TX+ SATA0_TX-	A16 A17	Serial ATA channel 0, Transmit Output differential pair.	O SATA		AC coupled on Module
SATA0_RX+ SATA0_RX-	A19 A20	Serial ATA channel 0, Receive Input differential pair.	I SATA		AC coupled on Module
SATA1_TX+ SATA1_TX-	B16 B17	Serial ATA channel 1, Transmit Output differential pair.	O SATA		AC coupled on Module
SATA1_RX+ SATA1_RX-	B19 B20	Serial ATA channel 1, Receive Input differential pair.	I SATA		AC coupled on Module
(S)ATA_ACT#	A28	ATA (parallel and serial) or SAS activity indicator, active low.	O 3.3V	PU 4.7K 3.3V	

4.3.3.1. PCH HSIO Lane Assignments

Name	HSIO name on SOC	Comment
SATA0	HSIO 17	
SATA1	HSIO 19	

4.3.4 PCI Express

Name	Pin #	Description	I/O	PU / PD	Comment
PCIE_TX0+ PCIE_TX0-	A68 A69	PCI Express channel 0, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX0+ PCIE_RX0-	B68 B69	PCI Express channel 0, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX1+ PCIE_TX1-	A64 A65	PCI Express channel 1, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX1+ PCIE_RX1-	B64 B65	PCI Express channel 1, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX2+ PCIE_TX2-	A61 A62	PCI Express channel 2, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX2+ PCIE_RX2-	B61 B62	PCI Express channel 2, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX3+ PCIE_TX3-	A58 A59	PCI Express channel 3, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX3+ PCIE_RX3-	B58 B59	PCI Express channel 3, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX4+ PCIE_TX4-	A55 A56	PCI Express channel 4, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX4+ PCIE_RX4-	B55 B56	PCI Express channel 4, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX5+ PCIE_TX5-	A52 A53	PCI Express channel 5, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX5+ PCIE_RX5-	B52 B53	PCI Express channel 5, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX8+ PCIE_TX8-	A71 A72	PCI Express channel 8, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX8+ PCIE_RX8-	B71 B72	PCI Express channel 8, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX9+ PCIE_TX9-	A74 A75	PCI Express channel 9, Transmit Output differential pair.	O PCIE		AC coupled on Module

Name	Pin #	Description	I/O	PU / PD	Comment
PCIE_RX9+ PCIE_RX9-	B74 B75	PCI Express channel 9, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX10+ PCIE_TX10-	A77 A78	PCI Express channel 10, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX10+ PCIE_RX10-	B77 B78	PCI Express channel 10, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX11+ PCIE_TX11-	A81 A82	PCI Express channel 11, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX11+ PCIE_RX11-	B81 B82	PCI Express channel 11, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX12+ PCIE_TX12-	A39 A40	PCI Express channel 12, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX12+ PCIE_RX12-	B39 B40	PCI Express channel 12, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX13+ PCIE_TX13-	A36 A37	PCI Express channel 13, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX13+ PCIE_RX13-	B36 B37	PCI Express channel 13, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX14+ PCIE_TX14-	A25 A26	PCI Express channel 14, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX14+ PCIE_RX14-	B25 B26	PCI Express channel 14, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX15+ PCIE_TX15-	A22 A23	PCI Express channel 15, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX15+ PCIE_RX15-	B22 B23	PCI Express channel 15, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_CLK_REF+ PCIE_CLK_REF-	A88 A89	PCI Express Reference Clock output for all PCI Express and PCI Express Graphics Lanes.	O PCIE		
PCIE_CLK_REF1+ PCIE_CLK_REF1-	B29 B30		O PCIE		

Note: PCIE_CLK_REF1 (B29, B30) and GND (B28) are used for Gen4/3/2/1 speed at PCIe lane 16-31

PCI Express lane configuration as below

Lane 0-7								Lane 16-23								Lane 24-31								Lane 8-15							
-								x16																-							
x8								x8								x8								x8							
x4				x4				x4				x4				x4				x4				x4							
x2		x2		x2		x2		x2				x2				x2				x2				x2		x2					
x1		x1		x1		x1		x1				x1				x1				x1				x1		x1					

Compliant with PICMG definition

Additional configurations supported by Intel® Xeon® D platform.
Use caution when adopting these additional configurations.

Note: Additional PCIe x1 at Lane 1 and Lane 5 are by build option supported by project basis.

4.3.4.1. PCH HSIO Lane Assignments

Name	HSIO name on SOC	Comment
PCIE0	HSIO 0	
PCIE1	HSIO 1	
PCIE2	HSIO 2	
PCIE3	HSIO 3	
PCIE4	HSIO 4	
PCIE5	HSIO 5	
PCIE6	HSIO 6	
PCIE7	HSIO 7	
PCIE8	HSIO 8	
PCIE9	HSIO 9	
PCIE10	HSIO 10	
PCIE11	HSIO 11	
PCIE12	HSIO 12	
PCIE13	HSIO 13	
PCIE14	HSIO 14	
PCIE15	HSIO 15	

4.3.5 LPC Bus

Name	Pin #	Description	I/O	PU / PD	Comment
LPC_AD0 LPC_AD1 LPC_AD2 LPC_AD3	B4 B5 B6 B7	LPC multiplexed address, command and data bus	I/O 3.3VSB	PU 10K 3.3VSB	This Intel platform requires PU
LPC_FRAME#	B3	LPC frame indicates the start of an LPC cycle	O 3.3VSB	PU 10K 3.3VSB	This Intel platform requires PU
~~LPC_DRQ0#~~ ~~LPC_DRQ1#~~	~~B8~~ ~~B9~~	~~LPC serial DMA request~~	~~I 3.3V~~		Not supported
LPC_SERIRQ	A50	LPC serial interrupt	I/O 3.3VSB	PU 10K 3.3VSB	This Intel platform requires PU
LPC_CLK	B10	LPC clock output –33MHz nominal	O 3.3VSB	PD 10K	The LPC_CLK frequency is 24MHz on this platform

4.3.6 USB

Name	Pin #	Description	I/O	PU / PD	Comment
USB0+ USB0-	A46 A45	USB differential data pairs for Port 0	I/O 3.3VSB		USB 1.1/ 2.0 compliant
USB1+ USB1-	B46 B45	USB differential data pairs for Port 1	I/O 3.3VSB		USB 1.1/ 2.0 compliant
USB2+ USB2-	A43 A42	USB differential data pairs for Port 1	I/O 3.3VSB		USB 1.1/ 2.0 compliant
USB3+ USB3-	B43 B42	USB differential data pairs for Port 2	I/O 3.3VSB		USB 1.1/ 2.0 compliant
USB_0_1_OC#	B44	USB over-current sense, USB ports 0 and 1 (see *Note)	I 3.3VSB	PU 10K 3.3VSB	Do not pull high on carrier
USB_2_3_OC#	A44	USB over-current sense, USB ports 2 and 3 (see *Note)	I 3.3VSB	PU 10K 3.3VSB	Do not pull high on carrier
~~USB0_HOST_PRSNT~~	~~B48~~	~~Module USB client may detect the presence of a USB host on USB0. A high value indicates that a host is present.~~	~~I 3.3VSB~~		Not supported

***Note**: A pull-up for this line shall be present on the module. An open drain driver from a USB current monitor on the carrier board may drive this line low.

4.3.6.1. USB Root Segmentation

All USB interfaces are derived from the xHCI controller.

4.3.7 SPI Bus (BIOS only)

Name	Pin #	Description	I/O	PU / PD	Comment
SPI_CS#	B97	Chip select for Carrier Board SPI BIOS Flash.	O 3.3VSB	PU 10K 3.3VSB	
SPI_MISO	A92	Data in to module from carrier board SPI BIOS flash.	I 3.3VSB		
SPI_MOSI	A95	Data out from module to carrier board SPI BIOS flash.	O 3.3VSB		
SPI_CLK	A94	Clock from module to carrier board SPI BIOS flash.	O 3.3VSB		
SPI_POWER	A91	Power supply for Carrier Board SPI – sourced from Module – nominally 3.3V. The Module shall provide a minimum of 100mA on SPI_POWER. Carriers shall use less than 100mA of SPI_POWER. SPI_POWER shall only be used to power SPI devices on the Carrier	O P 3.3VSB		
BIOS_DIS0#	A34	Selection strap to determine the BIOS boot device.	I	PU 10K 3.3VSB	Carrier shall pull to GND or leave not connected.
BIOS_DIS1#	B88	Selection strap to determine the BIOS boot device.	I	PU 10K 3.3VSB	Carrier shall pull to GND or leave not connected

4.3.8 Miscellaneous

Name	Pin #	Description	I/O	PU / PD	Comment
~~SPKR~~	~~B32~~	~~Output for audio enunciator, the "speaker" in PC-AT systems~~	~~O 3.3V~~		Not supported
WDT	B27	Output indicating that a watchdog time-out event has occurred.	O 3.3V	PU 10K 3.3V	
THRM#	B35	Input from off-module temp sensor indicating an over-temp situation.	I 3.3VSB		
THRMTRIP#	A35	Active low output indicating that the CPU has entered thermal shutdown.	O 3.3VSB	PU 10K 3.3VSB	
FAN_PWMOUT	B101	Fan speed control. Uses the Pulse Width Modulation (PWM) technique to control the fan's RPM.	O OD 3.3V		There shall be PD on carrier board
FAN_TACHIN	B102	Fan tachometer input for a fan with a two-pulse output.	I OD 3.3V	PU 47K 3.3V	
TPM_PP	A96	Trusted Platform Module (TPM) Physical Presence pin. Active high. TPM chip has an internal pull down. This signal is used to indicate Physical Presence to the TPM.	I 3.3V	PD 100K	PD only when TPM on module. Modules implementing a TPM shall pull down

4.3.9 SMBus

Name	Pin #	Description	I/O	PU / PD	Comment
SMB_CK	B13	System Management Bus bidirectional clock line. Power sourced through 3.3V standby rail and main power rails.	I/O OD 3.3VSB	PU 2.2K 3.3VSB	Equivalent resistor is 2.2K
SMB_DAT#	B14	System Management Bus bidirectional data line. Power sourced through 3.3V standby rail and main power rails.	I/O OD 3.3VSB	PU 2.2K 3.3VSB	Equivalent resistor is 2.2K
SMB_ALERT#	B15	System Management Bus Alert – active low input can be used to generate an SMI# (System Management Interrupt) or to wake the system. Power sourced through 3.3V standby rail and main power rails.	I 3.3VSB	PU 10K 3.3VSB	

Note: SMBus source from SoC's SMBus is default setting. SMBus source from EC is by build option supported by project basis.

4.3.10 I2C Bus

Name	Pin #	Description	I/O	PU / PD	Comment
I2C_CK	B33	General purpose I^2C port clock output/input	I/O OD 3.3VSB	PU 2.2K 3.3VSB	Source SEMA BMC as default (chipset by BOM option)
I2C_DAT	B34	General purpose I^2C port data I/O line	I/O OD 3.3VSB	PU 2.2K 3.3VSB	Source SEMA BMC as default (chipset by BOM option)

4.3.11 General Purpose I/O (GPIO)

Name	Pin #	Description	I/O	PU / PD	Comment
GPO[0]	A93	General purpose output pins.	O 3.3V	PD 10K 3.3V	After hardware RESET output low
GPO[1]	B54	General purpose output pins.	O 3.3V	PD 10K 3.3V	After hardware RESET output low
GPO[2]	B57	General purpose output pins.	O 3.3V	PD 10K 3.3V	After hardware RESET output low
GPO[3]	B63	General purpose output pins.	O 3.3V	PD 10K 3.3V	After hardware RESET output low
GPI[0]	A54	General purpose input pins. Pulled high internally on the module.	I 3.3V	PU 10K 3.3V	
GPI[1]	A63	General purpose input pins. Pulled high internally on the module.	I 3.3V	PU 10K 3.3V	
GPI[2]	A67	General purpose input pins. Pulled high internally on the module.	I 3.3V	PU 10K 3.3V	
GPI[3]	A85	General purpose input pins. Pulled high internally on the module.	I 3.3V	PU 10K 3.3V	

4.3.12 Serial Interface Signals

Name	Pin #	Description	I/O	PU / PD	Comment
SER0_TX	A98	General purpose serial port transmitter	O CMOS 3.3V		Power rail tolerance 5V, 12V There shall be PD on carrier board
SER0_RX	A99	General purpose serial port receiver	I CMOS 3.3V	PU 8.2K 3.3V	Power rail tolerance 5V, 12V
SER1_TX	A101	General purpose serial port transmitter	O CMOS 3.3V		Power rail tolerance 5V, 12V There shall be PD on carrier board
SER1_RX	A102	General purpose serial port receiver	I CMOS 3.3V	PU 8.2K 3.3V	Power rail tolerance 5V, 12V

Note: SER0, SER1 source from EC is default setting. SER0, SER1 source from SoC's HSUART is by build option by supported by project basis. HSUART has driver support limitation.

4.3.13 Power and System Management

Name	Pin #	Description	I/O	PU / PD	Comment
PWRBTN#	B12	Power button to bring system out of S5 (soft off), active on falling edge.	I 3.3VSB	PU 10K 3.3VSB	
SYS_RESET#	B49	Reset button input. Active low request for module to reset and reboot. May be falling edge sensitive. For situations when SYS_RESET# is not able to reestablish control of the system, PWR_OK or a power cycle may be used.	I 3.3VSB	PU 10K 3.3VSB	
CB_RESET#	B50	Reset output from module to Carrier Board. Active low. Issued by module chipset and may result from a low SYS_RESET# input, a low PWR_OK input, a VCC_12V power input that falls below the minimum specification, a watchdog timeout, or may be initiated by the module software.	O 3.3V		
PWR_OK	B24	Power OK from main power supply. A high value indicates that the power is good. This signal can be used to hold off Module startup to allow carrier-based FPGAs or other configurable devices time to be programmed.	I 3.3VSB	PU 10K 3.3VSB	Should have weak pull up.
SUS_STAT#	B18	Indicates imminent suspend operation; used to notify LPC devices.	O 3.3VSB		
SUS_S3#	A15	Indicates system is in Suspend to RAM state. Active-low output. An inverted copy of SUS_S3# on the carrier board (also known as "PS_ON") may be used to enable the non-standby power on a typical ATX power supply.	O 3.3VSB		
SUS_S4#	A18	Indicates system is in Suspend to Disk state. Active low output.	O 3.3VSB		
SUS_S5#	A24	Indicates system is in Soft Off state.	O 3.3VSB		Connect to SUS_S4#
WAKE0#	B66	PCI Express wake up signal.	I 3.3VSB	PU 10K 3.3VSB	
WAKE1#	B67	General purpose wake-up signal. May be used to implement wake-up on PS/2 keyboard or mouse activity.	I 3.3VSB	PU 10K 3.3VSB	Connect to WAKE 0#
BATLOW#	A27	Battery low input. This signal may be driven low by external circuitry to signal that the system battery is low or may be used to signal some other external power-management event.	I 3.3VSB	PU 10K 3.3VSB	
~~LID#~~	~~A103~~	~~LID button. Low active signal used by the ACPI operating system for a LID switch.~~	~~I OD 3.3VSB~~		Not supported
~~SLEEP#~~	~~B103~~	~~Sleep button. Low active signal used by the ACPI operating system to bring the system to sleep state or to wake it up again.~~	~~I OD 3.3VSB~~		Not supported
~~RAPID_ SHUTDOWN~~	~~C67~~	~~Trigger for Rapid Shutdown. Must be driven to 5V though a <=50-ohm source impedance for ≥ 20 µs.~~	~~I CMOS 5VSB~~		Not supported

4.3.14 Power and Ground

Name	Pin #	Description	I/O	PU / PD	Comment
VCC_12V	A104, A105, A106, A107, A108, A109, B104, B105, B106, B107, B109	Primary power input supports wide range 5~ 20V input All available VCC_12V pins on the connector(s) shall be used.	P		12V ±5%
VCC_5V_SBY	B84, B85, B86, B87	Standby power input: +5.0V nominal. If VCC5_SBY is used, all available VCC_5V_SBY pins on the connector(s) shall be used. Only used for standby and suspend functions. May be left unconnected if these functions are not used in the system design.	P		5Vsb ±5%
VCC_RTC	A47	Real-time clock circuit-power input. Nominally +3.0V.	P		
GND	A1, A11, A21, A31, A41, A51, A57, A60, A66, A70, A80, A90, A100, A110, B1, B11, B28, B21, B31, B41, B51, B60, B70, B80, B90, B100, B110	Ground - DC power and signal and AC signal return path.	P		

4.4. CD Connector Signal Descriptions

4.4.1 USB 3.0 Extensions

Name	Pin #	Description	I/O	PU / PD	Comment
USB_SSRX0- USB_SSRX0+	C3 C4	Additional Receive signal differential pairs for the SuperSpeed USB data path on USB0	I PCIE		AC coupled off module
USB_SSTX0- USB_SSTX0+	D3 D4	Additional Transmit signal differential pairs for the SuperSpeed USB data path on USB0	O PCIE		AC coupled on module
USB_SSRX1- USB_SSRX1+	C6 C7	Additional Receive signal differential pairs for the SuperSpeed USB data path on USB1	I PCIE		AC coupled off module
USB_SSTX1- USB_SSTX1+	D6 D7	Additional Transmit signal differential pairs for the SuperSpeed USB data path on USB1	O PCIE		AC coupled on module
USB_SSRX2- USB_SSRX2+	C9 C10	Additional Receive signal differential pairs for the SuperSpeed USB data path on USB2	I PCIE		AC coupled off module
USB_SSTX2- USB_SSTX2+	D9 D10	Additional Transmit signal differential pairs for the SuperSpeed USB data path on USB2	O PCIE		AC coupled on module
USB_SSRX3- USB_SSRX3+	C12 C13	Additional Receive signal differential pairs for the SuperSpeed USB data path on USB3	I PCIE		AC coupled off module
USB_SSTX3- USB_SSTX3+	D12 D13	Additional Transmit signal differential pairs for the SuperSpeed USB data path on USB3	O PCIE		AC coupled on module

4.4.1.1. USB Root Segmentation

All USB interfaces are derived from the xHCI controller.

4.4.2 PCI Express

Name	Pin #	Description	I/O	PU / PD	Comment
PCIE_TX6+ PCIE_TX6-	D19 D20	PCI Express channel 6, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX6+ PCIE_RX6-	C19 C20	PCI Express channel 6, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX7+ PCIE_TX7-	D22 D23	PCI Express channel 7, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX7+ PCIE_RX7-	C22 C23	PCI Express channel 7, Receive Input differential pair.	I PCIE		AC coupled off Module

4.4.2.1. PCH HSIO Lane Assignments

Refer to section **4.3.4.1 PCH HSIO Lane Assignments** for detailed info.

4.4.3 10G-KR Ethernet

Name	Pin #	Description	I/O	PU / PD	Comment
10G_KR_RX0+ 10G_KR_RX0- 10G_KR_RX1+ 10G_KR_RX1-	C49 C50 C42 C43	10GBASE-KR ports, Receive Input differential pairs	I KR		AC coupled on Module
10G_KR_TX0+ 10G_KR_TX0- 10G_KR_TX1+ 10G_KR_TX1-	D49 D50 D42 D43	10GBASE-KR ports, Transmit Output differential pairs	O KR		AC coupled on Carrier
10G_KR_RX2+ 10G_KR_RX2- 10G_KR_RX3+ 10G_KR_RX3-	C29 C30 C26 C27	10GBASE-KR ports, Receive Input differential pairs	I KR		AC coupled on Module
10G_KR_TX2+ 10G_KR_TX2- 10G_KR_TX3+ 10G_KR_TX3-	D29 D30 D26 D27	10GBASE-KR ports, Transmit Output differential pairs	O KR		AC coupled on Carrier
~~10G_INT0 /~~ **CEI_INT#**	C47	Interrupt pin from Copper PHY or Optical SFP+ module to the 10GbE controller	I 3.3VSB	PU 10K 3.3VSB	This pin is used for CEI mode
~~10G_INT1~~ ~~10G_INT2~~ ~~10G_INT3~~	~~D47~~ ~~C24~~ ~~D24~~	~~Interrupt pin from Copper PHY or Optical SFP+ module to the 10GbE controller~~	~~I 3.3VSB~~		Not supported
~~10G_PHY_MDIO_SDA0 /~~ **CEI_MDIO**	D46	MDIO mode Management Data I/O Interface mode data signal for serial data transfers between the MAC and an external PHY ~~I2C mode~~ ~~I2C Data signal, of the 2-wire management interface used for serial data transfers between the MAC and the external PHY~~	I/O 3.3VSB	PU 1K 3.3VSB	This pin is used for CEI mode
~~10G_PHY_MDC_SCL0~~	C46	MDIO mode	O 3.3VSB	PU 1K	This pin is used for CEI mode

Name	Pin #	Description	I/O	PU / PD	Comment
~~/~~ **CEI_MDC**		Management Data I/O Interface mode clock signal for serial data transfers between the MAC and an external PHY ~~I2C mode~~ ~~I2C Data signal, of the 2-wire management interface used for serial data transfers between the MAC and the external PHY~~		3.3VSB	
~~10G_PHY_MDIO_SDA1~~ ~~10G_PHY_MDIO_SDA2~~ ~~10G_PHY_MDIO_SDA3~~	~~D45~~ ~~D16~~ ~~D15~~	~~MDIO mode~~ ~~Management Data I/O Interface mode data signal for serial data transfers between the MAC and an external PHY~~ ~~I2C mode~~ ~~I2C Data signal, of the 2-wire management interface used for serial data transfers between the MAC and the external PHY~~	~~O 3.3VSB~~ ~~I/O OD 3.3VSB~~		Not supported
~~10G_PHY_MDC_SCL1~~ ~~10G_PHY_MDC_SCL2~~ ~~10G_PHY_MDC_SCL3~~	~~C45~~ ~~C16~~ ~~C15~~	~~MDIO mode~~ ~~Management Data I/O Interface mode clock signal for serial data transfers between the MAC and an external PHY~~ ~~I2C mode~~ ~~I2C Data signal, of the 2-wire management interface used for serial data transfers between the MAC and the external PHY~~	~~O 3.3VSB~~ ~~I/O OD 3.3VSB~~		Not supported
10G_SDP0 10G_SDP1 10G_SDP2 10G_SDP3	C40 D40 C17 D17	Software-Definable Pins	I/O 3.3VSB	PU 20K 3.3VSB	This Intel platform requires PU
~~10G_SFP_SDA0 /~~ **CEI_SDA**	C39	I2C Data signal, of the 2-wire management interface used by 10GbE controller to access the management registers of an external Optical SFP+ module	I/O OD 3.3VSB	PU 10K 3.3VSB	This pin is used for CEI mode
~~10G_SFP_SCL0 /~~ **CEI_SCL**	D39	I2C Clock signal, of the 2-wire management interface used by 10GbE controller to access the management registers of an external Optical SFP+ module	I/O OD 3.3VSB	PU 10K 3.3VSB	This pin is used for CEI mode
~~10G_SFP_SDA1~~ ~~10G_SFP_SDA2~~	~~C38~~ ~~C33~~	~~I2C Data signal, of the 2-wire management interface used by 10GbE controller to access the management registers of an~~	~~I/O OD 3.3VSB~~		Not supported

Name	Pin #	Description	I/O	PU / PD	Comment
~~10G_SFP_SDA3~~	~~C32~~	~~external Optical SFP+ module~~			
~~10G_SFP_SCL1~~ ~~10G_SFP_SCL2~~ ~~10G_SFP_SCL3~~	~~D38~~ ~~D33~~ ~~D32~~	~~I2C Clock signal, of the 2-wire management interface used by 10GbE controller to access the management registers of an external Optical SFP+ module~~	~~I/O OD 3.3VSB~~		Not supported
~~10G_PHY_RST_01 /~~ **CEI_RST#**	C35	Output signal that resets and Optical PHY on port 0 and port 1	O 3.3VSB	PD 10K	This pin is used for CEI mode
~~10G_PHY_RST_23~~	~~C34~~	~~Output signal that resets and Optical PHY on port 0 and port 1~~	~~O 3.3VSB~~		Not supported
~~10G_PHY_CAP_01 /~~ **CEI_PRSNT#**	D35	Phy mode capability pin: Indicates if the PHY for 10G lanes 0 and1 is capable of configuration by I2C. High indicates MDIO-only configuration, and low indicates configuration capability via I2C or MDIO. The actual protocol used for PHY configuration is determined by the module, in part based on this input. The actual protocol used is indicated over the dedicated I2C interface	I 3.3VSB	PU 10K 3.3VSB	This pin is used for CEI mode
~~10G_PHY_CAP_23~~	~~D34~~	~~Phy mode capability pin: Indicates if the PHY for 10G lanes 0 and1 is capable of configuration by I2C. High indicates MDIO-only configuration, and low indicates configuration capability via I2C or MDIO. The actual protocol used for PHY configuration is determined by the module, in part based on this input. The actual protocol used is indicated over the dedicated I2C interface~~	~~I 3.3VSB~~	~~PU 10K 3.3VSB~~	Not supported
10G_LED_SDA	C36	I2C Data signal, of the 2-wire that transfers all LED signals and additional Strapping signal for I2C or MDIO mode of Optical PHY	I/O OD 3.3VSB	PU 2.2K 3.3VSB	Build option by project basis
10G_LED_SCL	C37	I2C Clock signal, of the 2-wire that transfers all LED signals and additional Strapping signal for I2C or MDIO mode of Optical PHY	I/O OD 3.3VSB	PU 2.2K 3.3VSB	Build option by project basis

Note: For detailed information about circuit design between the Ethernet controller, Optical Fiber/Copper PHY and firmware, please contact your local ADLINK representative.

4.4.4 PCI Express

Name	Pin #	Description	I/O	PU / PD	Comment
PCIE_TX16+ PCIE_TX16-	D52 D53	PCI Express channel 16, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX16+ PCIE_RX16-	C52 C53	PCI Express channel 16, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX17+ PCIE_TX17-	D55 D56	PCI Express channel 17, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX17+ PCIE_RX17-	C55 C56	PCI Express channel 17, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX18+ PCIE_TX18-	D58 D59	PCI Express channel 18, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX18+ PCIE_RX18-	C58 C59	PCI Express channel 18, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX19+ PCIE_TX19-	D61 D62	PCI Express channel 19, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX19+ PCIE_RX19-	C61 C62	PCI Express channel 19, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX20+ PCIE_TX20-	D65 D66	PCI Express channel 20, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX20+ PCIE_RX20-	C65 C66	PCI Express channel 20, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX21+ PCIE_TX21-	D68 D69	PCI Express channel 21, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX21+ PCIE_RX21-	C68 C69	PCI Express channel 21, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX22+ PCIE_TX22-	D71 D72	PCI Express channel 22, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX22+ PCIE_RX22-	C71 C72	PCI Express channel 22, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX23+ PCIE_TX23-	D74 D75	PCI Express channel 23, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX23+ PCIE_RX23-	C74 C75	PCI Express channel 23, Receive Input differential pair.	I PCIE		AC coupled off Module

PCIE_TX24+ PCIE_TX24-	D78 D79	PCI Express channel 24, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX24+ PCIE_RX24-	C78 C79	PCI Express channel 24, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX25+ PCIE_TX25-	D81 D82	PCI Express channel 25, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX25+ PCIE_RX25-	C81 C82	PCI Express channel 25, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX26+ PCIE_TX26-	D85 D86	PCI Express channel 26, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX26+ PCIE_RX26-	C85 C86	PCI Express channel 26, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX27+ PCIE_TX27-	D88 D89	PCI Express channel 27, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX27+ PCIE_RX27-	C88 C89	PCI Express channel 27, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX28+ PCIE_TX28-	D91 D92	PCI Express channel 28, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX28+ PCIE_RX28-	C91 C92	PCI Express channel 28, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX29+ PCIE_TX29-	D94 D95	PCI Express channel 29, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX29+ PCIE_RX29-	C94 C95	PCI Express channel 29, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX30+ PCIE_TX30-	D98 D99	PCI Express channel 30, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX30+ PCIE_RX30-	C98 C99	PCI Express channel 30, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX31+ PCIE_TX31-	D101 D102	PCI Express channel 31, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX31+ PCIE_RX31-	C101 C102	PCI Express channel 31, Receive Input differential pair.	I PCIE		AC coupled off Module

Note: PCIE_CLK_REF1 (B29, B30) and GND (B28) are used for Gen4/3/2/1 speed at PCIe lane 16-31.
If up to Gen3 speed is required on PCIe lane 16-31 and would like to use PCIe clock from A88/A89, a build option on the module can be supported by project basis.

4.4.5 Module Type Definition

Name	Pin #	Description	I/O	PU / PD	Comment
TYPE0# TYPE1# TYPE2#	C54 C57 D57	The TYPE pins indicate to the Carrier Board the Pin-out Type that is implemented on the Module. The pins are tied on the Module to either ground (GND) or are no-connects (NC). For Pin-out Type 1 and Type 10 that lack a CD connector, these pins are not present (X) **TYPE2# TYPE1# TYPE0#** X X X Pinout Type 1 X X X Pinout Type 10 NC NC NC Pinout Type 2 NC NC GND Pinout Type 3 NC GND NC Pinout Type 4 NC GND GND Pinout Type 5 GND NC NC Pinout Type 6 GND NC GND Pinout Type 7 The Carrier Board ***should*** implement combinatorial logic that monitors the module TYPE pins and keeps power off (e.g deactivates the ATX_ON signal for an ATX power supply) if an incompatible module pin-out type is detected. The Carrier Board logic may also implement a fault indicator such as an LED.			Type 7
TYPE10#	A97	In case of a type 10 module this pin signal is tied to GND through a 47K resistor on the module.			No PD

4.4.6 Power and Ground

Name	Pin #	Description	I/O	PU / PD	Comment
VCC_12V	C104, C105, C106, C107, C108, C109, D104, D105, D106, D107, D108, D109	Primary power input supports wide range 5~ 20V input. All available VCC_12V pins on the connector(s) shall be used.	P		12V ±5%
GND	C1, C2, C5, C8, C11, C14, C21, C31, C41, C51, C60, C70, C73, C76, C80, C84, C87, C90, C93, C96, C100, C103, C110, D1, D2, D5, D8, D11, D14, D21, D31, D41, D51, D60, D67, D70, D73, D76, D80, D84, D87, D90, D93, D96, D100, D103, D110	Ground - DC power and signal and AC signal return path.	P		

5. Additional Features

This chapter describes connectors, LEDs, switches and additional items located on the module and not necessarily included in the PICMG standard specification. The locations of these items are shown below:

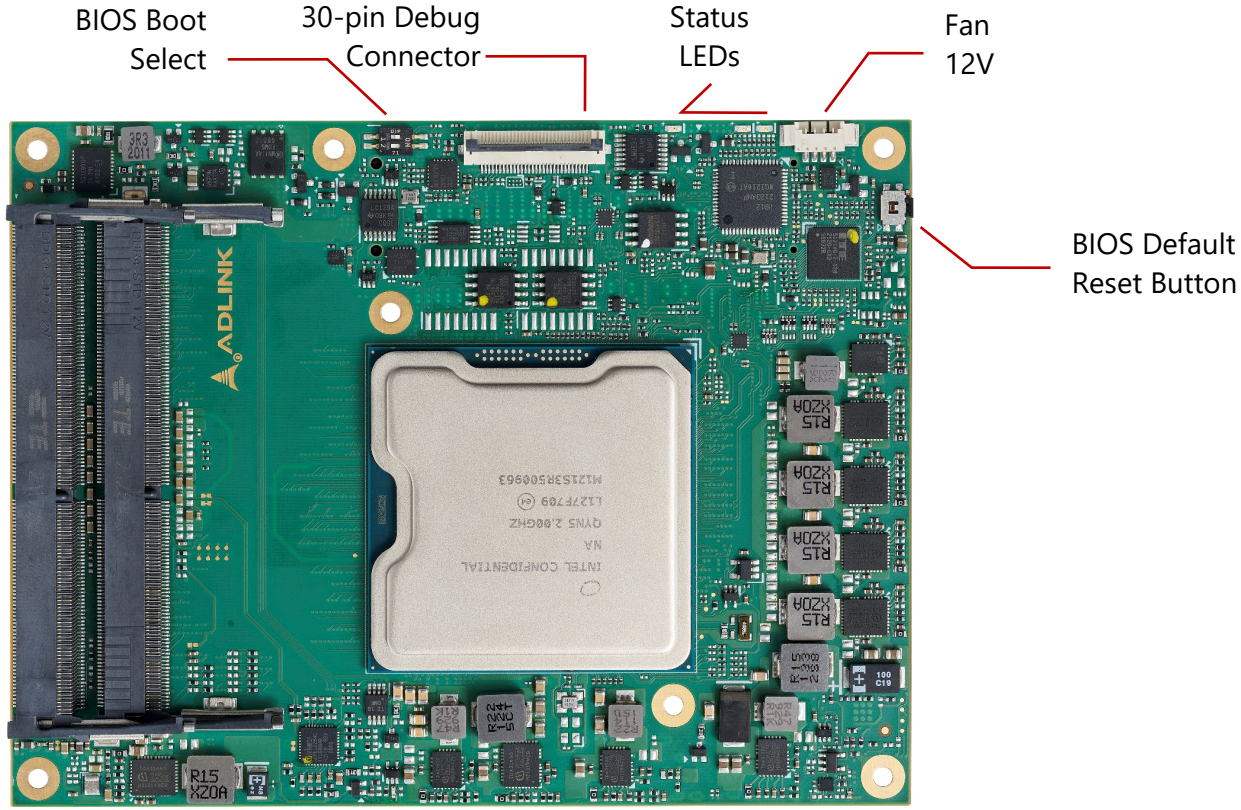


Figure 3 – Module feature locations

5.1. Debug Connector

This connector is particular useful during carrier design and bring up phase. It offers access to the following critical parts of the module:

- Test points measurement of internal power rails
- I2C bus for BIOS POST code readout
- SPI BIOS programming interface
- Embedded Controller programming interface

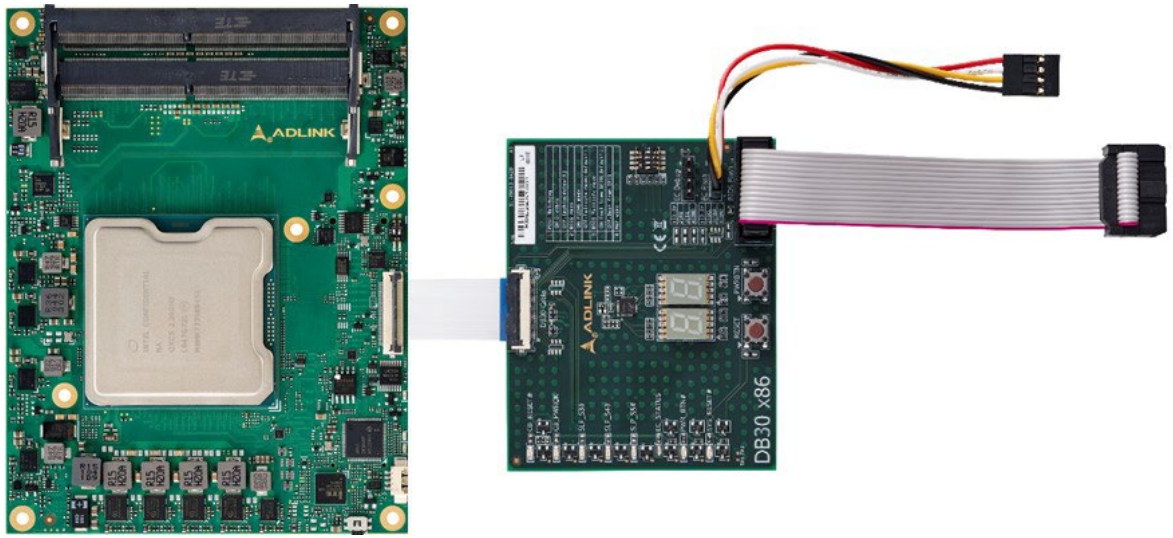


Figure 4 – Express-ID7 and Debug Module

5.2. Status LEDs

Status LED's are mounted on the module to facilitate easier maintenance.

Name	Color	Connection	Function
LED1	Blue	BMC output	Power Sequence Status Code (BMC) Power Changes, RESET (see Exception Codes below)
LED2	Green	Power Source 3Vcc	S0 LED ON S3/S4/S5 LED OFF ECO mode LED OFF
LED3	Red	BMC output and same signal as WDT (B27) on BtB connector	Module power up WD LED = LED OFF Watchdog counting WD LED = Keep Last State Watchdog timed out WD LED = LED ON Watchdog RESET WD LED = LED ON Rebooted after WD RESET WD LED = LED ON Rebooted after PWRBTN WD LED = LED OFF Rebooted after RESET BTN WD LED = LED OFF Note: Only a RESET not initiated by the BMC can clear the WD LED (user action)

5.3. Exception Codes

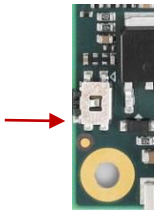
Exception Code	Error Message
0	NOERROR
2	NO_SUSCLK
3	NO_SLP_S5
4	NO_SLP_S4
5	NO_SLP_S3
6	BIOS_FAIL
7	RESET_FAIL
8	RESETIN_FAIL
9	NO_CB_PWROK
10	CRITICAL_TEMP
11	POWER_FAIL
12	VOLTAGE_FAIL
13	RSMRST_FAIL
14	NO_VDDQ_PG
15	NO_V1P05A_PG
16	NO_VCORE_PG
17	NO_SYS_GD
18	NO_V5SBY
19	NO_V3P3A
20	NO_V5_DUAL
21	NO_PWRSRC_GD
22	NO_P_5V_3V3_S0_PG
23	NO_SAME_CHANNEL
24	NO_PCH_PG

5.4. Fan Connector

Connector type: JVE 24W1125A-04M00

Name	Description
1	FAN_PWMOUT
2	FAN_TACHIN
3	GND
4	12V

5.5. BIOS Default Reset Button



To perform a hardware reset of BIOS default settings, perform the following steps:

1. Shut down the system.
2. Keep the BIOS Setup Defaults Reset Button pressed and boot up the system. You can release the button when the BIOS prompt screen appears
3. The BIOS prompt screen will display a confirmation that BIOS defaults have been reset and request that you reboot the system.

5.6. BIOS Boot Select

The module has two BIOS chips (BOM option) and BIOS operation can be configured to "PICMG" and dual-BIOS "Failsafe" modes using BIOS Select and Mode Configuration Switch, Pin 2.

Setting the module to PICMG mode will configure the BIOS chips on the module as SPI0 and SPI1. In PICMG mode, a BIOS chip cannot be placed in the SPI0 slot on the carrier.

In dual-BIOS Failsafe mode, both BIOS chips on the module are configured as SPI1. Only one of the two is connected to the SPI bus at any given time. In case of failure of the primary SPI1 BIOS, the system will reboot and switch to the secondary SPI1 BIOS on the module. In Failsafe mode, the SPI0 BIOS socket on the carrier can be populated.

In either mode, BIOS Select and Mode Configuration Switch Pin 1 is used to select whether to boot from SPI0 or SPI1.

Mode	Pin 1	Pin 2
Boot from SPI0 (default)	On	-
Boot from SPI1	Off	-
Set BIOS to PICMG mode (default)	-	On
Set BIOS to Failsafe BIOS mode	-	Off

6. System Resources

6.1. System Memory Map

Address Range (hex)	Description
22FFC000000-24FFFF1FFFF	PCI Express Root Complex
21FF0000000-21FFFF1FFFF	PCI Express Root Complex
20FFFA97000-20FFFA9AFFF	CDF ME HECI
20FFFA77000-20FFFA77FFF	SDA Standard Compliant SD Host Controller
20FFFA00000-20FFFA6FFFF	Intel USB 3.0 Host Controller
20FF0000000-20FFFA3FFFF	CDF PCIeRP
FEE00000-FFFFFFFF	PCI Express Root Complex
FF000000-FFFFFFFF	Motherboard resources
FED40000-FED44FFF	Trusted Platform Module 2.0
FED00000-FED003FF	High precision event timer
FEC00000-FECFFFFF	Advance programmable interrupt controller
FE200000-FE7FFFFF	Motherboard resources
FE010000-FE010FFF	PCI Express Root Complex
FD6F0000-FE01FFFF	Motherboard resources
FD6D0000-FD6EFFFF	Intel Serial IO Host Controller
FD6C0000-FD6CFFFF	Motherboard resources
FD6A0000-FD6AFFFF	Intel Serial IO Host Controller
FD000000-FD69FFFF	Motherboard resources
D8000000-FB7FFFFF	PCI Express Root Complex

Address Range (hex)	Description
B4000000-D7FFFFFF	PCI Express Root Complex
90000000-B3FFFFFF	PCI Express Root Complex
000C8000-000CFFFF	PCI Express Root Complex
000A0000-000BFFFF	PCI Express Root Complex

6.2. I/O Map

Hex Range	Device
00h - 0Fh	DMA controller
10h - 1Fh	Motherboard resources
20h – 2Dh	Programmable interrupt controller
2Eh - 2Fh 4Eh - 4Fh	LPC SIO (W83627DHGSEC / IT5121E) configuration index/data registers
30h – 3Dh	Programmable interrupt controller
40h - 43h	System Timer
50h - 53h	System Timer
60h and 64h	8742 equivalent (keyboard)
62h and 66h	ACPI-Compliant Embedded Controller
61h	System Speaker
70h - 77	Real Time Clock Controller
81h - 83h, 87h, 89h - 8Bh and 8Fh	DMA controller
A0h - B1h	Programmable interrupt controller
B2h – B3h	Motherboard resources

Hex Range	Device
B4h – BDh	Programmable interrupt controller
C0h – DFh	Direct memory access controller
F0h	Numeric data processor
240h - 247h	Serial port 3 (COM3)
248h - 24Fh	Serial port 4 (COM4)
2F8h – 2FFh	Serial port 2 (COM2)
3F8h - 3FFh	Serial port 1 (COM1)
400h - 41Fh	Motherboard resources
4D0h – 4D1h	Programmable interrupt controller
500h – A6Fh	Motherboard resources
CA2h – CA3h	Generic IPMI Compliant Device
CF9h	Reset Generator

6.3. Interrupt Request (IRQ) Lines

APIC Mode

IRQ#	Typical Interrupt Resource	Available
0	High precision even timer/System timer	No
1	Standard PS/2 Keyboard	No
3	Serial Port 2	No
4	Serial Port 1	No
5	Serial Port 3	No
7	Serial Port 4	No

IRQ#	Typical Interrupt Resource	Available
8	System CMOS/Real time clock	No
11	CDF ME:HECI	No
13	Numeric data processor	No
14	Serial IO GPIO Host Controller	No

6.4. PCI Configuration Space Map

Bus Number	Device Number	Function Number	Routing	Description
00h	00h	00h	Internal	Mesh2IIO MMAP/VT-D
00h	00h	01h	Internal	Mesh2IIO PMON
00h	00h	02h	Internal	Mesh2IIO RAS
00h	00h	03h	Internal	Mesh2IIO DFX
00h	00h	04h	Internal	Satellite IEH
00h	00h	05h	Internal	VMD
00h	01h	00h	Internal	CBDMA CH0
00h	01h	01h	Internal	CBDMA CH1
00h	01h	02h	Internal	CBDMA CH2
00h	01h	03h	Internal	CBDMA CH3
00h	01h	04h	Internal	CBDMA CH4
00h	01h	05h	Internal	CBDMA CH5
00h	01h	06h	Internal	CBDMA CH6
00h	01h	07h	Internal	CBDMA CH7
00h	02h	00h	Internal	PECI Out-Of-Band Management Services

Bus Number	Device Number	Function Number	Routing	Description
				Module (OOB-MSM)
00h	02h	01h	Internal	UBOX
00h	02h	02h	Internal	UBOX
00h	02h	04h	Internal	CPU Intel® Trace Hub
00h	06h	00h	Internal	Virtual Root Port (VRP) for Intel QAT v1.7
01h	00h	00h	Internal	Intel QAT v1.7 (Bus subordinate to S0 VRP is assigned by BIOS)
00h	09h	00h	Internal	PCH PCIe Cluster 0 Root Port 0
00h	0Eh	00h	Internal	SATA Controller
00h	0Fh	00h	Internal	Host SMBUS
00h	15h	00h	Internal	PCH PCIe Root Port
00h	18h	00h	Internal	Intel® ME - HECI
00h	18h	04h	Internal	Intel® ME - HECI
00h	1Ah	00h	Internal	HSUART 0
00h	1Ah	01h	Internal	HSUART 1
00h	1Ah	02h	Internal	HSUART 2
00h	1Ah	03h	Internal	Reserved
00h	1Dh	00h	Internal	Host Bridge
00h	1Eh	00h	Internal	USB xHCI Controller
00h	1Fh	00h	Internal	LPC/eSPI Controller
00h	1Fh	04h	Internal	Legacy SMBUS
00h	1Fh	05h	Internal	SPI Controller
00h	1Fh	07h	Internal	PCH Intel® Trace Hub

Bus Number	Device Number	Function Number	Routing	Description
01h	00h	00h	Internal	Intel Co-Processor
03h	00h	00h	External	Intel I210 Gigabit Network Connection
14h	00h	00h	Internal	Mesh2IIO MMAP/VT-D
14h	00h	01h	Internal	Mesh2IIO PMON
14h	00h	02h	Internal	Mesh2IIO RAS
14h	00h	03h	Internal	Mesh2IIO DFX
14h	00h	04h	Internal	Satellite IEH
F3h	00h	00h	Internal	Mesh2IIO MMAP/VT-D
F3h	00h	01h	Internal	Mesh2IIO PMON
F3h	00h	02h	Internal	Mesh2IIO RAS
F3h	00h	03h	Internal	Mesh2IIO DFX
F3h	00h	04h	Internal	Satellite IEH
F3h	04h	04h	Internal	Host Bridge
F4	00h	00h	Internal	Ethernet Controller(s) Exact number of functions will depend number of enabled ports (up to 8). Bus subordinate to S2 VRP is assigned by the BIOS.
F4h	00h	00h	Internal	UBOX - Global Events
F4h	00h	01h	Internal	UBOX
F4h	00h	02h	Internal	UBOX -DEC
F4h	00h	03h	Internal	Satellite IEH
FEh	0Bh	00h	Internal	SPD0_SMBUS
FEh	0Bh	01h	Internal	SPD1_SMBUS

Bus Number	Device Number	Function Number	Routing	Description
FEh	0Bh	02h	Internal	VPP_SMBUS
FEh	0Ch	00h	Internal	Mesh2IMC0
FEh	1Ah	00h	Internal	IMC0
FFh	00h	00h	Internal	CHA0_GRP1 - UNICAST_GROUP1_CHA
FFh	00h	01h	Internal	CHA1_GRP1 - UNICAST_GROUP1_CHA
FFh	00h	02h	Internal	CHA2_GRP1 - UNICAST_GROUP1_CHA
FFh	00h	03h	Internal	CHA3_GRP1 - UNICAST_GROUP1_CHA
FFh	00h	04h	Internal	CHA4_GRP1 - UNICAST_GROUP1_CHA
FFh	00h	05h	Internal	CHA5_GRP1 - UNICAST_GROUP1_CHA
FFh	00h	00h	Internal	CHA0_GRP0 - UNICAST_GROUP0_CHA
FFh	0Ah	01h	Internal	CHA1_GRP0 - UNICAST_GROUP0_CHA
FFh	0Ah	02h	Internal	CHA2_GRP0 - UNICAST_GROUP0_CHA
FFh	0Ah	03h	Internal	CHA3_GRP0 - UNICAST_GROUP0_CHA
FFh	0Ah	04h	Internal	CHA4_GRP0 - UNICAST_GROUP0_CHA
FFh	0Ah	05h	Internal	CHA5_GRP0 - UNICAST_GROUP0_CHA
FFh	1Dh	00h	Internal	CHAALL0 - Multicast DRAM Rules
FFh	1Dh	01h	Internal	CHAALL1 - Multicast MMIO Rules
FFh	1Eh	00h	Internal	PCU
FFh	1Eh	01h	Internal	PCU
FFh	1Eh	02h	Internal	PCU
FFh	1Eh	03h	Internal	PCU
FFh	1Eh	04h	Internal	PCU
FFh	1Eh	05h	Internal	PCU

Bus Number	Device Number	Function Number	Routing	Description
FFh	1Eh	06h	Internal	PCU
FFh	1Eh	07h	Internal	PCU

6.5. PCI Interrupt Routing Map

INT Line	PCI Express Port 0	Crystal Beach DMA Engine0	LPC Bridge	HECI #1 on PCH	SMBus controller on PCH	SATA Controller
Int0	INTA:16	INTA:16		INTA:16		INTA:16
Int1	INTB:17				INTB:17	
Int2	INTC:18		INTC:18			
Int3	INTC:19					

INT Line	XHCI Controller	Intel I210
Int0	INTA:16	INTA:16
Int1		
Int2		
Int3		

INT Line	PCIE Port1	PCIE Port 2	PCIE Port 3	PCIE Port 4	PCIE Port 5	PCIE Port 6	PCIE Port 7	PCIE Port 8
Int0	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Int1	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Int2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

INT Line	PCIE Port1	PCIE Port 2	PCIE Port 3	PCIE Port 4	PCIE Port 5	PCIE Port 6	PCIE Port 7	PCIE Port 8
Int3	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

6.6. SMBus Address Table

Device	Address
DDR4 Channel A(SO-DIMM1)	A0h
DDR4 Channel B(SO-DIMM2)	A4h
DDR4 Channel B(SO-DIMM3)	A2h
DDR4 Channel B(SO-DIMM4)	A8h
EC_I2C0_ALERT (SU1)	90h
EC_I2C0_ALERT (SU2)	92h
VNN_NAC(PU9)	CCh
VNN_PCH(PU6)	61h
VDDQ (PU12)	64h

7. BIOS Setup

7.1. Menu Structure

This section presents the six primary menus of the BIOS Setup Utility. Use the following table as a quick reference for the contents of the BIOS Setup Utility. The subsections in this section describe the submenus and setting options for each menu item. The default setting options are presented in **bold**, and the function of each setting is described in the right-hand column of the respective table.

Main	Advanced	Platform Configuration	Socket Configuration
BIOS Information System Information Board Information► System Date System Time	Serial Port Console Redirection► PCI Subsystem Settings► Power Management► System Management► Thermal Management► Watchdog Timer ► Super IO Configuration► Miscellaneous► Network Stack Configuration► Trusted Computing►	PCH-IO Configuration► Miscellaneous Configuration► Network Configuration► Server ME Configuration► iRC Firmware Information► System Event Log► Reserve Memory►	Processor Configuration► Common RefCode Configuration► Uncore Configuration► Memory Configuration► IIO Configuration► Advanced Power Management Configuration►

Security	Boot	Save & Exit
Password Description Secure Boot Menu	Boot Configuration	Save Options Default Options Boot Override

Note: Indicates a submenu

Gray text indicates info only.

7.2. Main

The Main Menu provides read-only information about your system and also allows you to set the System Date and Time. Refer to the tables below the screenshot of this menu for details of the submenus and settings.

7.2.1.1. BIOS Information

Feature	Options	Description
BIOS Vender	Info only	American Megatrends
BIOS Version	Info only	Display Core Version
Build Date	Info only	Display Compliancy Information
RC Version	Info only	Display Compliancy Information
ME FW Version	Info only	ADLINK BIOS Version.
BIOS Boot Source	Info only	SPI Boot Source

7.2.2 System Information

Board Information	Info only	Description
Project Name	Info only	Display Project Name
CPU Board Version	Info only	Display CPU Signature
CPU Brand String	Info only	Display CPU Brand Name
CPU Frequency	Info only	Display CPU Frequency
Total Memory	Info only	Display Installed Memory Size
Memory Frequency	Info only	Display Memory Frequency
PCH SKU	Info only	Display SOC SKU Name

7.2.3 Board Information

Board Information	Info only	Description
Serial Number	Read only	Display SMC serial number
Manufacturing Date	Read only	Display SMC manufacturing date.
Last Repair Date	Read only	Display SMC last repair date.
MAC ID	Read only	Display SMC MAC ID.
Runtime Statistics	Info only	
Total Runtime	Read only	The returned value specifies the total time in minutes the system is running in the S0 state.
Current Runtime	Read only	The returned value specifies the time in seconds the system is running in the S0 state. This counter is cleared when the system is removed from the external power supply.
Power Cycles	Read only	The returned value specifies the number of times the external power supply has been shut down.
Boot Cycles	Read only	The Bootcounter is increased after a HW- or SW-Reset or after a successful power-up.
Boot Reason	Read only	The boot reason is the event which causes the reboot of the system.

7.2.4 System Date and Time

Feature	Options	Description
System Date	Weekday, MM/DD/YYYY	Requires the alpha-numeric entry of the day of the week, day of the month, calendar month, and all 4 digits of the year, indicating the century and year (Fri XX/XX/20XX).
System Time	HH/MM/SS	Presented as a 24-hour clock setting in hours, minutes, and seconds.
Access Level	Info only	

7.3. Advanced

This menu contains the settings for most of the user interfaces in the system

7.3.1 Serial Console Redirection

Feature	Options	Description
Serial Port Console	Info only	
COM0	Info only	
Console Redirection	**Enabled** Disabled	Console Redirection Enable or Disable.
Console Redirection Settings	Submenu	
COM1	Info only	
Console Redirection	Enabled **Disabled**	Console Redirection Enable or Disable.
Console Redirection Settings	Submenu	
COM2	Info only	
Console Redirection	Enabled **Disabled**	Console Redirection Enable or Disable.

Feature	Options	Description
Console Redirection Settings	Submenu	
COM3	Info only	
Console Redirection	Enabled **Disabled**	Console Redirection Enable or Disable.
Console Redirection Settings	Submenu	
Serial Port for Out-of-Band Management/	Info only	
Windows Emergency Management Services (EMS)	Info only	
Console Redirection EMS	Enabled **Disabled**	Console Redirection Enable or Disable.
Console Redirection Settings	Submenu	

7.3.1.1. Serial Port Console > Console Redirection Settings

Feature	Options	Description
COM0	Info only	
Console Redirection Settings	Info only	
Terminal Type	VT100 VT100+ VT-UTF8 **ANSI**	Emulation: ANSI: Extended ASCII char set. VT100: ASCII char set. VT100+: Extends VT100 to support color, function keys, etc. VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.
Bits per second	9600 19200 38400 57600 **115200**	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Data Bits	7	Data Bits.

Feature	Options	Description
	8	
Parity	**None** Even Odd Mark Space	A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the num of 1's in the data bits is even. Odd: Parity bit is 0 if num of 1's in the data bits is odd. Mark: Parity bit is always 1. Space: Parity bit is always 0. Mark and Space parity does not detect errors.
Stop Bits	**1** 2	Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit.
Flow Control	**None** Hardware RTS/CTS	Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to restart the flow. Hardware flow control uses two wires to send start/stop signals.
VT-UTF8 Combo Key Support	Disabled **Enable**	Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals.
Recorder Mode	**Disabled** Enable	With this mode enabled only text will be sent. This is to capture Terminal data.
Resolution 100x31	**Disabled** Enable	Enables or disables extended terminal resolution
Putty KeyPad	**VT100** LINUX XTERMR6 SCO ESCN VT400	Select FunctionKey and KeyPad on Putty.

7.3.1.2. Serial Port Console > Console Redirection Settings

Feature	Options	Description
Out-of-Band Mgmt Port	**COM0** COM1 COM2 COM3	Microsoft Windows Emergency Management Services (EMS) allows remote management of a Windows Server OS through a serial port.
Terminal Type EMS	VT100 VT100+ **VT-UTF8** ANSI	VT-UTF8 is the preferred terminal type for out-of-band management. The next best choice is VT100+ and then VT100. See above in the Console Redirection Settings page, for more Help with Terminal Type/Emulation.
Bits per second	9600 19200 38400 57600 **115200**	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Flow Control	**None** Hardware RTS/CTS Software Xon/Xoff	Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to restart the flow. Hardware flow control uses two wires to send start/stop signals.
Data Bits EMS	**8**	
Parity EMS	**None**	
Stop Bits EMS	**1**	

7.3.2 PCI Subsystem Settings

Feature	Options	Description
PCI Bus Driver Version	Info only	
PCI Devices Common Settings	Info only	
PCI Latency Timer	**32 PCI Bus Clocks** 64 PCI Bus Clocks 96 PCI Bus Clocks 128 PCI Bus Clocks 160 PCI Bus Clocks 192 PCI Bus Clocks 224 PCI Bus Clocks 248 PCI Bus Clocks	Value to be programmed into PCI Latency Timer Register.
PCI-X Latency Timer	32 PCI Bus Clocks **64 PCI Bus Clocks** 96 PCI Bus Clocks 128 PCI Bus Clocks 160 PCI Bus Clocks 192 PCI Bus Clocks 224 PCI Bus Clocks 248 PCI Bus Clocks	Value to be programmed into PCI Latency Timer Register.
VGA Palette Snoop	**Disabled** Enabled	Enables or Disables VGA Palette Registers Snooping.
PERR# Generation	**Disabled** Enabled	Enables or Disables PCI Device to Generate PERR#.
SERR# Generation	**Disabled** Enabled	Enables or Disables PCI Device to Generate SERR#.
Above 4G Decoding	Disabled **Enabled**	Enables or Disables 64bit capable Devices to be Decoded in Above 4G Address Space (Only if System Supports 64-bit PCI Decoding).
SR-IOV Support	Disabled	If system has SR-IOV capable PCIe Devices, this option Enables or Disables Single Root IO Virtualization

Feature	Options	Description
	Enabled	Support.
BME DMA Mitigation	**Disabled** Enabled	Re-enable Bus Master Attribute disabled during PCI enumeration for PCI Bridges after SMM Locked
PCI Express Settings	submenu	

7.3.2.1. PCI Subsystem Settings > PCI Express Settings

Feature	Options	Description
PCI Express Device Register Settings	Info only	
Relaxed Ordering	Disabled **Enabled**	Enables or Disables PCI Express Device Relaxed Ordering.
Extended Tag	**Disabled** Enabled	If ENABLED, it allows the device to use 8-bit Tag field as a requester.
No Snoop	Disabled **Enabled**	Enables or disables the PCI Express device's No Snoop option.
Maximum Payload	**Auto** 128 Bytes 256 Bytes 512 Bytes 1024 Bytes 2048 Bytes 4096 Bytes	Set Maximum Payload of PCI Express Device or allow System BIOS to select the value.
Maximum Read Request	**Auto** 128 Bytes 256 Bytes 512 Bytes 1024 Bytes 2048 Bytes	Set Maximum Read Request Size of PCI Express Device or allow System BIOS to select the value.

Feature	Options	Description
	4096 Bytes	
ASPM Support	**Disabled** Auto Force L0s	
Extended Synch	**Disabled** Enabled	If ENABLED, it allows generation of Extended Synchronization patterns.
Link Training Retry	Disable 2 3 **5**	Defines number of Retry Attempts software will take to retrain the link if previous training attempt was unsuccessful.
Link Training Timeout (uS)	**1000**	Defines number of Microseconds software will wait before polling 'Link Training' bit in Link Status register. Value ranges from 10 to 10000 uS.
Unpopulated Links	**Keep Link ON** Disable Link	In order to save power, software will disable unpopulated PCI Express links, if this option set to 'Disable Link'.

7.3.2.2. PCI Subsystem Settings > PCI Express Gen 2 Settings

Feature	Options	Description
PCI Express Gen2 Device Register Settings	Info only	
Completion Timeout	**Default** Shorter Longer Disabled	Device Functions that support Completion Timeout programmability, allow system software to modify the Completion Timeout value. 'Default' 50us to 50ms. If 'Shorter' is selected, the software will use shorter timeout ranges supported by hardware. If 'Longer' is selected, the software will use longer timeout ranges.
ARI Forwardin	**Disabled** Enabled	If supported by hardware and set to 'Enabled', the Downstream Port disables its traditional Device Number field being 0 enforcement when turning a Type1 Configuration Request into a Type0 Configuration Request, permitting access to Extended Functions in an ARI Device immediately below the Port. Default value: Disabled

Feature	Options	Description
AtomicOp Requester Enable	**Disabled** Enabled	If supported by hardware and set to 'Enabled', this function initiates AtomicOp Requests only if Bus Master Enable bit is in the Command Register Set.
AtomicOp Egress Blocking	**Disabled** Enabled	If supported by hardware and set to 'Enabled', outbound AtomicOp Requests via Egress Ports will be blocked.
IDO Request Enable	**Disabled** Enabled	If supported by hardware and set to 'Enabled', this permits setting the number of ID-Based Ordering (IDO) bit (Attribute[2]) requests to be initiated.
IDO Completion Enable	**Disabled** Enabled	If supported by hardware and set to 'Enabled', this permits setting the number of ID-Based Ordering (IDO) bit (Attribute[2]) requests to be initiated.
LTR Mechanism Enable	**Disabled** Enabled	If supported by hardware and set to 'Enabled', this enables the Latency Tolerance Reporting (LTR) Mechanism.
End-End TLP Prefix Blocking	**Disabled** Enabled	If supported by hardware and set to 'Enabled', this function will block forwarding of TLPs containing End-End TLP Prefixes.
Target Link Speed	**Auto** Force to 2.5 GT/s Force to 5.0 GT/s Force to 8.0 GT/s Force to 16.0 GT/s Force to 32.0 GT/s	If supported by hardware and set to 'Force to X.X GT/s' for Downstream Ports, this sets an upper limit on Link operational speed by restricting the values advertised by the Upstream component in its training sequences. When 'Auto' is selected HW initialized data will be used.
Clock Power Management	**Disabled** Enabled	If supported by hardware and set to 'Enabled', the device is permitted to use CLKREQ# signal for power management of Link clock in accordance with the protocol defined in appropriate form factor specification.
Compliance SOS	**Disabled** Enabled	If supported by hardware and set to 'Enabled', this will force LTSSM to send SKP Ordered Sets between sequences when sending Compliance Pattern or Modified Compliance Pattern.
Hardware Autonomous Width	Disabled **Enabled**	If supported by hardware and set to 'Disabled', this will disable the hardware's ability to change link width except for width size reduction to correct unstable link operation.
Hardware Autonomous Speed	Disabled **Enabled**	If supported by hardware and set to 'Disabled', this will disable the hardware's ability to change link speed except for speed rate reduction to correct unstable link operation.

7.3.3 Power Management

Feature	Options	Description
Power Management	Info only	
Enable ACPI Auto Configuration	**Disabled** Enabled	Enables or Disables BIOS ACPI Auto Configuration.
LID Function	**Disabled** Enabled	Enable/Disable LID Function
Sleep Function	Disabled **Enabled**	Enable/Disable Sleep Button Function
ECO Mode	**Disabled** Enabled	Reduces the power consumption of the system, but after a shut down, you have to wait at least 5 seconds before you can restart the system.
Power-Up Mode	**Turn On** Remain Off Last State	Turn On: The machine starts automatically when the power supply is turned on. Remain off: To start the machine the power button has to be pressed. Last State: The machine will power up to the last power state
ATTENTION: The Power-Up Mode only has effect, if the module is in ATX-Mode.	Info only	
Power Consumption	Submenu	

7.3.3.1. Power Management > Power Consumption

Feature	Options	Description
Power Consumption	Info only	
Main Current	Read only	Display input current.
Current Input Power	Read only	Display input power.
VRTC	Read only	Display actual voltage of the VRTC.
V5VSB	Read only	Display actual voltage of the V5VSB.
VIN	Read only	Display actual voltage of the VIN.
V3.3S	Read only	Display actual voltage of the V3.3S.
VMEM	Read only	Display actual voltage of the VMEM.
V3V3_A	Read only	Display actual voltage of the V3V3_A.
VCORE	Read only	Display actual voltage of the VCORE.

7.3.4 System Management

Feature	Options
System Management	Info only
SEMA Firmware Version	Info only
SEMA Flags	Submenu
SEMA Features	Info only
Uptime & Power Cycles Counter	Read only
System Restart Event	Read only
4096 Bytes User-Flash	Read only
Runtime Watchdog	Read only

Feature	Options
Temperatures	Read only
Voltage Monitor	Read only
Display Backlight Control	Read only
Power-up Watchdog	Read only
Power Monitor (Current Sense)	Read only
Boot Counter	Read only
Dual-BIOS	Read only
I2C Bus 1	Read only
I2C Bus 2	Read only
CPU Fan	Read only
System Fan 1	Read only
AT/ATX Mode	Read only
ACPI Thermal Trigger	Read only
Power-up to Last State	Read only
Backlight Restore	Read only
Ext - GPIO	Read only
I2C Bus 3	Read only
Other BMC	Read only
Error Log	Read only
Wake-by-BMC	Read only
Soft Fan	Read only
Parameter Memory	Read only

7.3.4.1. System Management > SEMA Flags

Feature	Options
SEMA Flags	Info only
BMC Flags	Read only
BIOS Select	Read only
ATX/AT-Mode	Read only

7.3.5 Thermal Management

Feature	Options	Description
Passive Cooling Trip Point	**Disable** 70 C 80 C 90 C	This value is the temperature threshold of the passive cooling trip point.
Critical Trip Point	**Disable** 80 C 90 C 95 C	This value is the temperature threshold of the critical trip point.
Active Cooling Trip Point	Disable 40 C 50 C 60 C 70 C **Refer to BMC**	This value is the temperature threshold of the active cooling trip point.
Watchdog ACPI Event Shutdown	**Disabled** Enabled	Watchdog ACPI Event Shutdown Enabled/Disabled
Temperatures and Fan Speed	Info only	
CPU Temperature	Info only	

Feature	Options	Description
Current	Read only	
Startup	Read only	
Min	Read only	
Max	Read only	
Board Temperatures	Info only	
Current	Read only	
Startup	Read only	
Min	Read only	
Max	Read only	
CPU Fan Speed	Read only	
Smart Fan	Submenu	

7.3.5.1. Thermal Management > Smart Fan

Feature	Options	Description
Smart Fan	Info only	
CPU Smart FanTemperature Source	**CPU Sensor** Board Sensor	CPU Smart Fan Temperature Source.
CPU Fan Mode	**AUTO (Smart Fan)** Fan Off Fan On	CPU Fan Mode
Trigger Point 1	Info only	
Trigger Temperature	40	Trigger Temperature
PWM Level	30	PWM Level

Feature	Options	Description
Trigger Point 2	Info only	
Trigger Temperature	50	Trigger Temperature
PWM Level	40	PWM Level
Trigger Point 3	Info only	
Trigger Temperature	60	Trigger Temperature
PWM Level	63	PWM Level
Trigger Point 4	Info only	
Trigger Temperature	70	Trigger Temperature
PWM Level	100	PWM Level

7.3.6 Watchdog Timer

Feature	Options	Description
Watchdog Timer	**Info only**	
Power-Up watchdog	**Disabled** Enabled	The Power Up Watchdog resets the system after a certain amount of time after power up. Press F12 during start up to disable the Power Up Watchdog.
ATTENTION: Pressing F12 during start up disables the Power Up Watchdog.	Info only	
RunTime Watchdog	**Disabled** Enabled	The RunTime Watchdog resets the system after a certain period following power-up.

7.3.7 Super IO Configuration

Feature	Options
Super IO Configuration	Info only
ITE5121 Super IO Configuration	submenu
W83627DHGSEC Super IO Configuration	submenu

7.3.7.1. Super IO Configuration> ITE5121 Super IO Configuration

Feature	Options
IT5121E Super IO Configuration	Info only
Super IO Chip	Info only
Serial Port 1 Configuration	submenu
Serial Port 2 Configuration	submenu

7.3.7.2. Super IO Configuration> W83627DHGSEC Super IO Configuration

Feature	Options
W83627DHGSEC Super IO Configuration	Info only
Super IO Chip	Info only
Serial Port 1 Configuration	submenu
Serial Port 2 Configuration	submenu

7.3.7.3. Super IO Configuration >ITE5121 Super IO Configuration > Serial Port 1 Configuration

Feature	Options	Description
Serial Port 1 Configuration	Info only	
Serial Port 1 Configuration	**Enabled** Disabled	Enable or Disable Serial Port (COM).
Device Settings	IO=3F8h; IRQ=4	Fixed configuration of serial port.
Change Settings	**Auto** IO=3F8h; IRQ=4 IO=3F8h; IRQ=3,4,5,6,7,9,10,11,12 IO=2F8h; IRQ=3,4,5,6,7,9,10,11,12 IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12 IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12	Select an optimal setting for Super IO device.
Change Settings	**Normal** High Speed	Select an optimal setting for the Super IO device.

7.3.7.4. Super IO Configuration >ITE5121 Super IO Configuration > Serial Port 2 Configuration

Feature	Options	Description
Serial Port 2 Configuration	Info only	
Serial Port 2 Configuration	**Enabled** Disabled	Enable or Disable Serial Port (COM).
Device Settings	IO=2F8h; IRQ=3	Fixed configuration of serial port.

Feature	Options	Description
Change Settings	**Auto** IO=2F8h; IRQ=3 IO=3F8h; IRQ=3,4,5,6,7,9,10,11,12 IO=2F8h; IRQ=3,4,5,6,7,9,10,11,12 IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12 IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12	Select an optimal setting for Super IO device.

7.3.7.5. Super IO Configuration >W83627DHGSEC Super IO Configuration > Serial Port 1 Configuration

Feature	Options	Description
Serial Port 1 Configuration	Info only	
Serial Port	**Enabled** Disabled	Enable or Disable Serial Port (COM).
Device Settings	IO=240h; IRQ=5	Fixed configuration of serial port.
Change Settings	**Auto** IO=240h; IRQ=10 IO=240h; IRQ=3,4,5,6,7,10,11,12 IO=248h; IRQ=3,4,5,6,7,10,11,12 IO=250h; IRQ=3,4,5,6,7,10,11,12 IO=258h;	Select an optimal setting for the Super IO device.

Feature	Options	Description
	IRQ=3,4,5,6,7,10,11,12 IO=260h; IRQ=3,4,5,6,7,10,11,12 IO=268h; IRQ=3,4,5,6,7,10,11,12	

7.3.7.6. Super IO Configuration >W83627DHGSEC Super IO Configuration > Serial Port 2 Configuration

Feature	Options	Description
Serial Port 2 Configuration	Info only	
Serial Port	**Enabled** Disabled	Enable or Disable Serial Port (COM).
Device Settings	IO=248h; IRQ=7	Fixed configuration of the serial port.
Change Settings	**Auto** IO=248h; IRQ=10 IO=240h; IRQ=3,4,5,6,7,10,11,12 IO=248h; IRQ=3,4,5,6,7,10,11,12 IO=250h; IRQ=3,4,5,6,7,10,11,12 IO=258h; IRQ=3,4,5,6,7,10,11,12 IO=260h; IRQ=3,4,5,6,7,10,11,12 IO=268h; IRQ=3,4,5,6,7,10,11,12	Select an optimal setting for the Super IO device.

Feature	Options	Description
Device Mode	**Standard Serial Port Mode** IrDA Active pulse 1.6 uS IrDA Active pulse 3/16 bit time ASKIR Mode	Change the Serial Port mode.

7.3.8 Miscellaneous

Feature	Options	Description
Miscellaneous	Info only	
Power Supply Unit	Emulate AT Mode **ATX Mode**	ATX: OS will turn off system power when shutdown. NOTE: AT mode will not support S3 & S4 & S5, so it will change Power Loss State to Power On.
I2C Speed Control	**100 Kbps** 400 Kbps	I2C Speed Control
WOL From S5	OFF **ON**	This Config to control power on/off LAN in S5 State by SEMA(EC).
Smart Battery Function	**Disabled** Enabled Auto	Enable/Disable Smart Battery function. Auto: disable Smart Battery function if charger IC not be detected.

7.3.9 Network Stack Configuration

Feature	Options	Description
Network Stack Configuration	Info only	Enable/Disable UEFI Network Stack
Network Stack	**Disabled** Enabled	Enable/Disable UEFI network stack.
Ipv4 PXE Support	**Disabled** Enabled	Enable/Disable IPv4 PXE boot support. If disabled, IPv4 PXE boot support will not be available.
IPv4 HTTP Support	**Disabled** Enabled	Enable/Disable IPv4 PXE boot support. If disabled, IPv4 PXE boot support will not be available.
Ipv6 PXE Support	**Disabled** Enabled	Enable/Disable IPv6 PXE boot support. If disabled, IPv6 PXE boot support will not be available.
IPv6 HTTP Support	**Disabled** Enabled	Enable/Disable IPv6 HTTP boot support. If disabled, IPv6 HTTP boot support will not be available.
PXE boot wait time	**0**	Wait time in seconds to press ESC key to abort the PXE boot. Use either +/- or numeric keys to set the value.
Media detect count	**1**	Number of times the presence of media will be checked. Use either +/- or numeric keys to set the value.

7.3.10 Trusted Computing

Feature	Options	Description
TPM 2.0 Device Found	Info only	
Firmware Version	Info only	
Vendor	Info only	
Security Device Support	**Disabled** Enabled	Security Device Support
Active PCR banks	Info only	

Feature	Options	Description
Available PCR banks	Info only	
SHA-1 PCR Bank	Disabled **Enabled**	Enable or Disable SHA-1 PCR Bank
SHA256 PCR Bank	Disabled **Enabled**	Enable or Disable SHA256 PCR Bank
Pending operation	**None** TPM Clear	Pending operation
Platform Hierarchy	Disabled **Enabled**	Enable or Disable Platform Hierarchy
Storage Hierarchy	Disabled **Enabled**	Enable or Disable Storage Hierarchy
Endorsement Hierarchy	Disabled **Enabled**	Enable or Disable Endorsement Hierarchy
TPM 2.0 UEFI Spec Version	TCG_1_2 **TCG_2**	Select the TCG2 Spec Version Support,\n\r\n\rTCG_1_2: the Compatible mode for Win8/Win10,\n\r\n\rTCG_2: Support new TCG2 protocol and event format for Win10 or later
Physical Presence Spec Version	1.2 **1.3**	Select to Tell O.S. to support PPI Spec Version 1.2 or 1.3. Note some HCK tests might not support 1.3.
TPM 2.0 InterfaceType	Info only	Select the Communication Interface to TPM 20 Device.
Device Select	TPM 1.2 TPM 2.0 **Auto**	TPM 1.2 will restrict support to TPM 1.2 devices, TPM 2.0 will restrict support to TPM 2.0 devices, Auto will support both with the default set to TPM 2.0 devices if not found, TPM 1.2 devices will be enumerated
Disable Block Sid	**Disabled** Enabled	Override to allow SID authentication in TCG Storage device

7.4. Platform Configuration

Feature	Options	Description
PCH-IO Configuration	submenu	
Miscellaneous Configuration	submenu	
Network Configuration	submenu	
Server ME Configuration	submenu	
iRC Firmware Information	submenu	
System Event Log	submenu	
Reserve Memory	submenu	

7.4.1 PCH-IO Configuration

Feature	Options	Description
PCI Express Configuration	submenu	
Fia Mux Configuration	show only	
SATA Configuration	submenu	
USB Configuration	submenu	
Debug Settings	submenu	
Security Configuration	submenu	
Pch Thermal Throttling Control	submenu	
Wake on WLAN and BT Enable	**Disabled** Enabled	Enable/Disable PCI Express Wireless LAN and Bluetooth to wake the system.
Disable DSX ACPRESENT PullDown	**Disabled** Enabled	Disable PCH internal ACPRESENT PullDown when DeepSx or G3 exit.

Feature	Options	Description
Serial IRQ Mode	Quiet **Continuous**	Configure Serial IRQ Mode.
State After G3	S0 State **S5 State**	Specify what state to go to when power is re-applied after a power failure (G3 state).
Port 80h Redirection	LPC Bus **PCI Bus**	Control where the Port 80h cycles are sent.
Enhance Port 80h LPC Decoding	show only	
IOAPIC 24-119 Entries	**Disabled** Enabled	Enables/Disables IOAPIC 24-119 Entries. IRQ24-119 may be used by PCH devices. Disabling those may cause certain device failures.
PCH Cross Throttling	Disabled **Enabled**	Enable/Disable the PCH Cross Throttling feature. Only ULT support this feature.
PCH Energy Reporting	Disabled **Enabled**	Enable Energy Report. MUST set it as ENABLED. This is only for test purposes.
Enable TCO Timer	Disabled **Enabled**	Enable/Disable TCO timer. When disabled, it disables PCH ACPI timer, and stops TCO timer.
Pcie Pll SSC	**Auto** 0.5%	Pcie Pll SSC percentage.AUTO - Keep hw default, no BIOS override. Setting AUTO reveals an option for CSME programming of SSC
SSC override through CSME	Disabled **Enabled**	Turn on / off Spread Spectrum Setting for IsCLK
Lock PCH Sideband Access	Disabled **Enabled**	Lock PCH Sideband access, including SideBand interface lock and SideBand PortID mask for certain endpoints (e.g., PSFx). The option is invalid if POSTBOOT SAI is set.
Flash Protection Range Registers (FPRR)	Disabled **Enabled**	Enable Flash Protection Range Registers
SPD Write Disable	True **Flase**	Enable/Disable setting SPD Write Disable. For security recommendations, SPD write disable bit must be set.
SMBUS defeaturing	**True** Flase	Enable/disable SMBUS defeaturing

Feature	Options	Description
ChipsetInit HECI Message	**Disabled** Enabled	Enable/Disable ChipsetInit HECI Message (disable will prevent the HSIO version check and HSIO init messages from being sent).
Bypass ChipsetInit sync reset	**Disabled** Enabled	Setting this option to skip ChipsetInit sync reset
Enable I/O Margining tool	**Disabled** Enabled	Setting this option to enable I/O Margining tool
LGMR	**Disabled** Enabled	64KB memory block for LGMR (LPC Memory Range Decode)
WDT Enable	Disabled **Enabled**	Enable/Disable WatchDog Timer. Note: This option is ignored on debug BIOS.
HSUART 0 Address mode	HSUART Legacy COM I/O address **HSUART Standard Enumeration**	Choose HSUART address mode. Standard Enumeration (PCIE) requires that HSUART 0 is visible (Function 0)
HSUART 1 Address mode	HSUART Legacy COM I/O address **HSUART Standard Enumeration**	Choose HSUART address mode. Standard Enumeration (PCIE) requires that HSUART 0 is visible (Function 0)
HSUART 2 Address mode	HSUART Legacy COM I/O address **HSUART Standard Enumeration**	Choose HSUART address mode. Standard Enumeration (PCIE) requires that HSUART 0 is visible (Function 0)

7.4.2 Miscellaneous Configuration

Feature	Options	Description
Application Profile Configuration	**Auto** General Computing Memory Bandwidth Matrix Calculation Energy Efficiency Server-Side Java OLTP Virtualization	Application Profile Configuration provides a quick method of BIOS knob tuning accordingly to the application. It's based on benchmark tests and may be not suitable for all workloads. You can still override the options.
KCS Access Control Policy	**Allow All** Restricted Deny All	Decides when IPMI commands shall be sent through the KCS interface. Allow All - Always, Restricted - until BIOS DONE is signaled, Deny All - Never
Max Page Table Size Select	2M **1G**	Select the max page size to use. If 1G size is used, it may cause problems with older OSs.
Reset Platform on Memory Map Change	**Disabled** Enabled	Causes a platform reset if the memory map has changed. Required for S4 resume to function at first boot.
Wake On Lan Support	**Disabled** Enabled	Enable or Disable Wake On Lan Support
Breakpoint Type	**None** After MRC After KTI RC After Resource Allocation After POST After Full Speed Setup Ready for IBIST	Halt at specified points in BIOS
Force Setup	**Disabled** Enabled	Enable/Disable loading setup without pressing F2
PFR Supported	show only	

Feature	Options	Description
BIOS Guard	show only	
Xml Cli Support	**Disabled** Enabled	Enable Disable Xml Cli Support in BIOS
Skip XML Compression	**Disabled** Enabled	If enabled the XML Compression will be skipped
Publish Setup page Pointer	**Disabled** Enabled	Publish Setup page Pointer in BIOS Knobs section of the Xml File
Advanced Debug Function	**Auto** Disabled Enabled	Advanced Debug Function (Dfx Knob)
Active Video	**Auto** Onboard Device PCIE Device	Auto - Onboard VGA by default, if not found then PCI AIC VGA (if present).\n Onboard - Enforces Onboard VGA.\n PCIe - Enforces PCI AIC VGA. (In case of multiple PCIe AIC VGA, platform selection is indeterministic, based on internal platform enumeration of PCIe devices)\n
PS2 Port Swap	**Disabled** Enabled	Enables or Disables the PS2 port swap
NumLock	**Disabled** Enabled	Enables or Disables NumLock
Wake On Lan from S5	**Disabled** Enabled	Enables or Disables Wake on Lan from S5
Boot to Network	**Disabled** Enabled	Enables or Disables Boot to Network. messages from being sent).
ARI Support	Disabled **Enabled**	Enable or disable the ARI support
ARI Forward	**Disabled** Enabled	Enable or disable the ARI Forward
RTC Wake system from S4/S5	**Disabled** Enabled	Enable or disable System wake on alarm event. When enabled, System will wake on the day::hr::min::sec specified

Feature	Options	Description
Firmware Configuration	Ignore Policy Update Production **Test**	Firmware Configuration options.
Warm-Reset Elimination	**Disabled** Enabled	When enabled, BIOS will skip warm-reset on the cold-reset path.\n. However, if BIOS setup option(s) and set-straps are out of sync, BIOS will request for warm-reset.
SSC Enable for Host	**Disabled** Enable SSC with 0.5 spread Enable SSC with 0.25 spread	Enable Spread Spectrum Control for the Host (CPU) PCIe High-Speed Root Ports

7.4.3 Network Configuration

Feature	Options	Description
Legacy Option ROMs support	**Disabled** Enabled	Enable/Disable Legacy PXE Option ROM execution for LANs.
EFI Network	**Disabled** Enabled	Enable/Disable EFI Network support for LANs.

7.4.4 Server ME Configuration

Feature	Options	Description
Oper. Firmware Version	Info only	
Backup Firmware Version	Info only	
Recovery Firmware Version	Info only	
ME Firmware Status #1	Info only	

Feature	Options	Description
ME Firmware Status #2	Info only	
Current State	Info only	
Error Code	Info only	
Recovery Cause	Info only	
Altitude	**8000**	The altitude of the platform location above the sea level, expressed in meters. The hex number is decoded as 2's complement signed integer.\n. Provide the 8000h value if the altitude is unknown.
MCTP Bus Owner	**0**	MCTP bus owner location on PCIe: [15:8] bus, [7:3] device, [2:0] function. If all zeros sending bus owner is disabled.
Server ME firmware features list	Info only	

7.4.5 iRC Firmware Information

Feature	Options
Active Firmware Tag	Info only
Active Firmware Version	Info only
Active Firmware Type	Info only
Backup Firmware Tag	Info only
Backup firmware version	Info only
Backup firmware type	Info only

7.4.6 System Event Log

Feature	Options	Description
System Errors	Disabled **Enabled** Auto	System Error Enable/Disable setup options.
RAS Log Level	None **MIN (BASIC_FLOW)** MID (BASIC_FLOW, FUNC_FLOW) MAX (BASIC_FLOW, FUNC_FLOW, REG)	RAS Log setup options.
System Memory Poison	Disabled **Enabled**	Enable/Disable System Memory Poison.
Viral Status	Info only	
Clear Viral Status	**Disabled** Enabled	Enable/Disable Clear Viral Status.
Cloak Devhide registers from being accessible from OS	**Disabled** Enabled	Enable/Disable OS to access Devhide registers.
System Cloaking	**Disabled** Enabled	When enabled, Corrected errors are masked from OS/SW visibility. This option is valid only when EMCA is enabled
FatalErrDebugHalt	**Disabled** Enabled	DEBUG loop for McBank Fatal error case ONLY. Warning: Enable this knob only in conjunction with ITP as the thread will halt in Fatal error flow.
Mca Bank Warm Boot Clear Errors	Disabled **Enabled**	Enable/Disable Mca Bank Warm Boot Clear Errors.
CrashLog Feature	Disabled **Enabled**	The feature helps collecting crash data from PMC SSRAM
CrashLog On All Reset	**Disabled** Enabled	Option to invoke CrashLog collection on all reset.

Feature	Options	Description
Shutdown Suppression	**Disabled** Enabled	Shutdown Suppression and Log MCA IERR.
eMCA Settings	submenu	
Whea Settings	submenu	
Error Injection Settings	submenu	
Memory Error Enabling	submenu	
IIO Error Enabling	submenu	
PCIe Error Enabling	submenu	
Error Control Setting	submenu	

7.4.6.1. eMCA Settings

Feature	Options	Description
EMCA Logging Support	Disabled **Enabled**	Enable/Disable EMCA Logging.
LMCE Support	Disabled **Enabled**	Enable/Disable Local MCE firmware support.
Ignore OS EMCA Opt-in	**Disabled** Enabled	Enable/Disable Ignore OS EMCA Opt-in and log.
EMCA CMCI-SMI Morphing	Disabled **EMCA gen 2 CSMI**	Enable/Disable EMCA CSMI.
EMCA CMCI-SMI Threshold	**0**	Set the threshold of correctable error for signaling CMCI-CSMI.
CSMI Dynamic Disable	Disabled **Enabled**	[Enable] - BIOS disables CSMI when error threshold reached.\n[Disabled] - CSMI always on.
EMCA MCE-SMI Enable	Disabled	Enable/Disable EMCA Uncorrected SMI for gen2.

Feature	Options	Description
	EMCA gen 2 - MSMI	
Corrected Error eLog	Disabled **Enabled**	Enable/Disable Corrected Error eLog.
Memory Error eLog	Disabled **Enabled**	Enable/Disable Memory Error eLog.
Processor Error eLog	Disabled **Enabled**	Enable/Disable Processor Error eLog.
Ubox Error Mask	**Disabled** Enabled	Mask SMI generation for Ubox Error.

7.4.6.2. Whea Settings

Feature	Options	Description
WHEA Support	Disabled **Enabled**	Enable or disable the WHEA support.
Whea Log Memory Error	Disabled **Enabled**	Enable/Disable Whea Log Memory Error.
Whea Log Processor Error	Disabled **Enabled**	Enable/Disable Whea Log Processor Error.
Whea Log PCI Error	Disabled **Enabled**	Enable/Disable Whea Log PCI Error.

7.4.6.3. Error Injection Settings

Feature	Options	Description
WHEA Error Injection Support	**Disabled** Enabled	Enable/Disable WHEA Error Injection Support.

7.4.6.4. Memory Error Enabling

Feature	Options	Description
Memory Error	Disabled **Enabled**	Enable/Disable Memory Error.
Memory Corrected Error	Disabled **Enabled**	Enable/Disable Memory Corrected Error
Spare Interrupt	Disabled **SMI** Error Pin CMCI	Spare Interrupt Selection

7.4.6.5. IIO Error Enabling

Feature	Options	Description
IIO/PCH Global Error Support	Disabled **Enabled**	Enable/Disable IIO/PCH Error Support.
Os Native AER Support	**Disabled** Enabled	Select FFM or OS native for AER error handling. If OS native is selected, BIOS also initializes FFM first until handshake, which depends on OS capability.
IIO MCA Support	Info only	
Clear PCC for IIO Non-Fatal Error	**Disabled** Enabled	Enable/Disable PCC equal 0 for IIO severity 1 error.

Feature	Options	Description
IIO Error Pin0 Enable	**Disabled** Enabled	Enable/Disable IIO Error Pin0.
IIO OOB Mode	Disabled **Enabled**	Enable/Disable System Event Generation when Error Pin is enabled.
IIO Error Registers Clear	Disabled **Enabled**	Enable/Disable Clear IIO Error Registers.
IIO eDPC Support	**Disabled** Enabled	Enable/Disable IIO eDPC Support.
IIO Coherent Interface Error	Disabled **Enabled**	Enable/Disable IIO Coherent Interface Error.
"IIO IRP0 protocol parity error	Disabled **Enabled**	Enable or disable Coherent Interface protocol IIO parity error reporting.
IIO IRP0 protocol qt overflow underflow error	Disabled **Enabled**	Enable or disable IIO Coherent Interface protocol queue table overflow or underflow error reporting.
IIO IRP0 protocol rcvd unexprsp	Disabled **Enabled**	Enable or disable IIO Coherent Interface protocol layer received unexpected response or completion error reporting.
IIO IRP0 csr acc 32b unaligned	Disabled **Enabled**	Enable or disable IIO Coherent Interface CSR Access Crossing 32-bit Boundary error reporting.
IIO IRP0 wrcache uncecccs0 error	Disabled **Enabled**	Enable or disable IIO Coherent Interface Write Cache Un-correctable ECC error reporting.
IIO IRP0 wrcache uncecccs1 error	Disabled **Enabled**	Enable or disable IIO Coherent Interface Write Cache Un-correctable ECC error reporting.
IIO IRP0 protocol rcvd poison error	Disabled **Enabled**	Enable or disable IIO Coherent Interface Protocol Layer Received Poisoned Packet error reporting.
IIO IRP0 wrcache correcccs0 error	Disabled **Enabled**	Enable or disable IIO Coherent Interface Write Cache Correctable ECC error reporting.
IIO IRP0 wrcache correcccs1 erro	Disabled	Enable or disable IIO Coherent Interface Write Cache Correctable ECC error reporting.

Feature	Options	Description
	Enabled	
IIO Misc. Error	Disabled **Enabled**	Enable/Disable IIO Misc. Error.
IIO Vtd Error	Disabled **Enabled**	Enable/Disable IIO Vtd Error.
IIO Dma Error	Disabled **Enabled**	Enable/Disable IIO Dma Error.
IIO Dmi Error	Disabled **Enabled**	Enable/Disable IIO Dmi Error.
PCIE Error	Disabled **Enabled**	Enable/Disable PCIE Error.
IIO PCIE Additional Corrected Error	Disabled **Enabled**	Enable/Disable IIO PCIE Additional Corrected Error.
IIO PCIE Additional Uncorrected Error	Disabled **Enabled**	Enable/Disable IIO PCIE Additional Uncorrected Error.
IIO PCIE Additional Received Completion With UR	**Disabled** Enabled	Enable/Disable IIO PCIE Additional Received Completion With UR.
IIO PCIE AER Spec Compliant	**Disabled** Enabled	Enable/Disable IIO PCIE AER Spec Compliant.
ITC/OTC CA/MA Errors	**Disabled** Enabled	Enable/Disable Completer Abort and Master Abort (Unsupported Request) on ITC and OTC.
PSF UR Error	Disabled **Enabled**	Enable/Disable Unsupported Request Error on PSF.
PMSB Router Parity Error	Disabled **Enabled**	Enable/Disable PMSB Router Parity Error.

7.4.6.6. PCIe Error Enabling

Feature	Options	Description
Corrected Error	Disabled **Enabled**	Enable & escalate Correctable Errors to error pins.
Uncorrected Error	Disabled **Enabled**	Enable & escalate Uncorrectable/Recoverable to error pins.
Fatal Error Enable	Disabled **Enabled**	Enable & escalate fatal errors to error pins.
PCIE Corrected Error Threshold Counter	**Disabled** Enabled	Enable/Disable PCIE Corrected Error Counter
PCIe Corrected Error Limit Check	**Disabled** Enabled	Enable/Disable the feature to disable reporting PCIe corrected errors for a device if they exceed a given limit.
PCIe Corrected Error Limit	Info only	
PCIE AER Corrected Errors	Disabled **Enabled**	Enable/Disable PCIE AER Corrected Errors.
PCIE AER Advisory Nonfatal Error	Disabled **Enabled**	Enable/Disable PCIE AER Advisory Nonfatal Error.
PCIE AER Fatal Error	Disabled **Enabled**	Enable/Disable PCIE AER Fatal Error.
PCIE AER NonFatal Error	Disabled **Enabled**	Enable/Disable PCIE AER NonFatal Error.
PCIE AER Fatal Error	Disabled **Enabled**	Enable/Disable PCIE AER Fatal Error.
PCIE AER Advisory Nonfatal Error	Disabled **Enabled**	Enable/Disable PCIE AER Advisory Nonfatal Error.
PCIE Unsupported Request Error	**Disabled** Enabled	Enable/Disable PCIE Unsupported Request Error.

Feature	Options	Description
PCIE Surprise Link Down Error	**Disabled** Enabled	Enable/Disable PCIE Surprise Link Down Error.
Assert NMI on SERR	Disabled **Enabled**	On SERR, generate an NMI and log an error.\n. Note: [Enabled] must be selected for the Assert NMI on PERR setup option to be visible.
Assert NMI on PERR	Disabled **Enabled**	On PERR, generate an NMI and log an error.\n. Note: This option is only active if the Assert NMI on SERR option has [Enabled] selected.
Expected BER	**34359738367**	Set the expected Bit Error Rate for all speeds.
Time Window (Gen1/2)	**65535**	Set the error burst protection time window for Gen1 and Gen2 speeds. A burst of errors within the window is counted as one.
Time Window (Gen3/4)	**2**	Set the error burst protection time window for Gen3 and Gen4 speeds. A burst of errors within the window is counted as one.
Error Threshold (Gen1/2)	**0**	Set the error threshold for Gen1 and Gen2 speeds. An event is triggered when the error count exceeds the threshold.
Error Threshold (Gen3/4)	**16**	Set the error threshold for Gen3 and Gen4 speeds. An event is triggered when the error count exceeds the threshold.
Gen3/4 Re-Equalization	Disabled **Enabled**	Enable or disable Gen3 and Gen4 re-equalization. This applies only when operating at Gen2 or Gen4 speeds. When an event is triggered, equalization is re-run.
Gen2 Link Degradation	Disabled **Enabled**	Enable or disable Gen2 link degradation. This applies only when operating at Gen2 speeds. When an event is triggered, 5GT/s and higher modes are disabled.
Gen3 Link Degradation	Disabled **Enabled**	Enable or disable Gen3 link degradation. This applies only when operating at Gen3 speeds. When an event is triggered, 8GT/s and higher modes are disabled.
Gen4 Link Degradation	Disabled **Enabled**	Enable or disable Gen4 link degradation. This applies only when operating at Gen4 speeds. When an event is triggered, 16GT/s and higher modes are disabled.

7.4.6.7. Error Control Setting

Feature	Options	Description
Latch First Corrected Error in KTI	Disabled **Enabled**	Enable or disable latch first corrected error in KTI.
Patrol Scrub Error Reporting	**UCNA**	Enable/Disable Memory Corrected Error

7.4.7 Reserve Memory

Feature	Options	Description
Reserve Memory Range	**Disabled** Enabled	Sets aside an empty memory page that is hidden from the OS\n Memory address should be available otherwise, reservation will fail.

7.5. Socket Configuration

Feature	Options
Processor Configuration	submenu
Common RefCode Configuration	submenu
Uncore Configuration	submenu
Memory Configuration	submenu
IIO Configuration	submenu
Advanced Power Management Configuration	submenu

7.5.1 Processor Configuration

Feature	Options	Description
Per-Socket Configuration	Info only	
Processor BSP Revision	Info only	
Processor Socket	Info only	
Processor ID	Info only	
Processor Frequency	Info only	
Processor Max Ratio	Info only	
Processor Min Ratio	Info only	
Microcode Revision	Info only	
L1 Cache RAM(Per Core)	Info only	
L2 Cache RAM(Per Core)	Info only	
L3 Cache RAM(Per Package)	Info only	
Processor 0 Version	Info only	
Hyper-Threading [ALL]	Info only	
IED Trace memory	**Disabled** 4M 8M 16M 32M 64M 128M 256M 512M 1G	Option to allocate memory for PSMI trace.

Skip Flex Ratio Override	**Disabled** Enabled	Skip Flex Ratio overrides to use power-on default Flex Ratio values. In multi-socket systems, this will allow mixed flex ratio limits.
Check CPU BIST Result	Disabled **Enabled**	Disable failed BIST core when enabled, otherwise, ignore the BIST result
3StrikeTimer	Disabled **Enabled**	The 3 strike counter can be turned off by writing into the MISC_FEATURE_CONTROL_DISABLE_THREE_STRIKE_CNT(MSR 0x01a4).
Fast String	Disabled **Enabled**	When enabled, enable fast strings for REP MOVS/STOS.
Machine Check	Disabled **Enabled**	Enable or Disable the Machine Check.
Max CPUID Value Limit	**Disabled** Enabled	This should be enabled in order to boot legacy OSes that cannot support CPUs with extended CPUID functions.
Hardware Prefetcher	Disabled **Enabled**	= MLC Streamer Prefetcher (MSR 1A4h Bit[0]).
Adjacent Cache Prefetch	Disabled **Enabled**	= MLC Spatial Prefetcher (MSR 1A4h Bit[1]).
DCU Streamer Prefetcher	Disabled **Enabled**	DCU streamer prefetcher is an L1 data cache prefetcher (MSR 1A4h [2]).
DCU IP Prefetcher	Disabled **Enabled**	DCU IP prefetcher is an L1 data cache prefetcher (MSR 1A4h [3]).
LLC Prefetch	**Disabled** Enabled	Enable/Disable LLC Prefetch on all threads.
DCU Mode	**Normal** Mirror-Mode	Normal: The whole DCU is used for caching; Mirror-Mode: DCU organized as 2x16KB mirrored copies.

Bsp Selection	Socket 0 Socket 1 Socket 2 Socket 3 Socket 4 Socket 5 Socket 6 Socket 7 **Auto**	Choose the method to select BSP.
Extended APIC	**Disabled** Enabled	Enable/disable extended APIC support\n\nNote:\nThis will enable VT-d automatically if x2APIC is enabled.
APIC Physical Mode	**Disabled** Enabled	Enable/Disable the APIC physical destination mode.
PECI	Disabled **Enabled**	PECI in trust bit enable.
Legacy Agent	Disabled **Enabled**	Legacy PECI agent in trust bit enable.
SMBus Agent	**Disabled** Enabled	SMBus PECI agent in trust bit enable.
IE Agent	Disabled **Enabled**	IE PECI agent in trust bit enable.
Generic Agent	**Disabled** Enabled	Generic PECI agent in trust bit enable.
eSPI Agent	**Disabled** Enabled	ESPI PECI agent in trust bit enable.
DBP-F	**Disabled** Enabled	The DBP-F can be turned off by writing into the (MSR 792h [5:6] for CLX, CPX, and MSR 6Dh [2:3] for ICX).
IIO LLC Ways [19:0](Hex)	**0**	MSR INGRESS_SPARE bitmask[10:0]
Remote Ways [22:12](Hex)	**0**	MSR INGRESS_SPARE bitmask[26:16], Value 0 means no override

SMM Blocked and Delayed	**Disabled** Enabled	Enable/Disable SMM Blocked and Delayed
eSMM Save State	**Disabled** Enabled	Enable or Disable the eSMM Save State Feature.
Smbus Error Recovery	Disabled **Enabled**	Enable or Disable Smbus Error Recovery.
Enable Intel(R) TXT	**Disabled** Enabled	Enables Intel(R) TXT.
VMX	Disabled **Enabled**	Enables the Vanderpool Technology, which takes effect after reboot.
Enable SMX	**Disabled** Enabled	Enables Safer Mode Extensions.
Lock Chipset	Disabled **Enabled**	Lock or Unlock the chipset.
MSR Lock Control	Disabled **Enabled**	Enable - MSR 3Ah and CSR 80h will be locked. Power Good reset is needed to remove lock bits.
PKG CST CONFIG CONTROL MSR Lock	Disabled **Enabled**	Enable - MSR 3Ah and CSR 80h will be locked. Power Good reset is needed to remove lock bits.
PKG CST CONFIG CONTROL MSR Lock	Disabled **Enabled**	Enable - MSR E2h will be locked. Power Good reset is needed to remove lock bits.
PPIN Control	Lock/Disabled **Unlock/Enabled**	Unlock and Enable/Disable PPIN Control.
AES-NI	Disabled **Enabled**	Enable/disable AES-NI support
TSC Reset	**Disabled** Enabled	Enable or Disable TSC reset during warm reboot.
#AC Exception On Split Lock	**Disabled** Enabled	Enable or Disable #AC (Alignment Check) Exception On Split Lock.

Total Memory Encryption (TME)	**Disabled** Enabled	Enable/Disable Total Memory Encryption (TME)
Limit CPU PA to 46 bits	Disabled **Enabled**	Limit CPU physical address to 46 bits to support older Hyper-v. If enabled, automatically disables TME-MT.
PSMI Configuration	submenu	PSMI Configuration
RDT CAT Opportunistic Tuning	**Default 0x7FF** Tuned 0x600 Tuned 0x003 Tuned 0x700	Cache Allocation Technology mask tuning options. NOTE: If IOT is enabled on any socket this option will override to 0x003

7.5.1.1. PSMI Configuration

Feature	Options	Description
Global PSMI Enable	Disabled **Enabled**	Global PSMI Enable.
Socket 0 Configuration	submenu	
PSMI Enable	**Disabled** Enabled	PSMI Enable

7.5.2 Common RefCode Configuration

Feature	Options	Description
MMCFG Base	1G 1.5G 1.75G 2G 2.25G 3G **Auto**	Select MMCFG Base.
MMCFG Size	64M 128M 256M 512M 1G 2G **Auto**	Select MMCFG Size
MMIO High Base	56T 40T 32T 24T 16T 4T **2T** 1T 512G 3854T	Select MMIO High Base

MMIO High Granularity Size	1G 4G 16G **64G** 256G 1024G	Selects the allocation size used to assign mmioh resources.\nTotal mmioh space can be up to 32xgranularity.\nPer stack mmioh resource assignments are multiples of the granularity where 1 unit per stack is the default allocation.
Numa	Disabled **Enabled**	Enable or Disable Non-Uniform Memory Access (NUMA)
Virtual Numa	**Disabled** Enabled	Divide physical NUMA nodes into evenly sized virtual NUMA nodes in the ACPI table. This may improve Windows performance on CPUs with more than 64 logical processors.
UMA-Based Clustering	**Disable (All2All)** Hemisphere (2-clusters)	UMA Based Clustering options include Disable (ALL2ALL), Hemisphere (2 clusters), and Quadrant (4 clusters, not supported on ICX). These options are only valid when SNC is disabled. If SNC is enabled, UMA-Based Clustering is automatically disabled by BIOS.
Publish SRAT	Disabled **Enabled**	Publish the SRAT ACPI table to the OS.
SRAT Memory Hot Plug	**Disabled** Enabled	Fix for OS that does not support memory hot plug.\nEx: SuSE SLES10 SP2. \n \nEnable by default. \nDisable will clear all hot plug bits and remove the hot plug entries in the SRAT table.
SRAT CPU Hot Plug	**Disabled** Enabled	Set Processor Flag to Enabled for all processor entries in SRAT.

7.5.3 Uncore Configuration

Feature	Options	Description
Uncore General Configuration	submenu	Displays and provides option to change the Uncore General Settings
Uncore Per Socket Configuration	submenu	Uncore Per Socket Configuration.

7.5.3.1. Uncore General Configuration

Feature	Options	Description
Uncore Status	Info only	
SplitLock	**Disabled** Enabled	Enable - Enable the split lock. Disable - Disable the split lock.
XPT Prefetch	Disabled Enabled **Auto**	XPT Prefetch.
Snoop All Cores Configuration	Disabled Enabled **Auto**	Select the level of snoop throttle setting for CHA.
Legacy VGA Socket	**0**	Stack that claims the legacy VGA range; valid values are 0-3; 0 is default.
PCIe Remote P2P Relaxed Ordering	**Disabled** Enabled	Relax P2P write ordering in hardware if software enforces ordering or doesn't care. The default is DISABLED, so the hardware will enforce P2P write ordering.
Uncore Debug Print Level	Fatal Warning Summary Detail **All**	Uncore Debug Print Level Enable-Disable.
Stale AtoS	Disabled Enabled **Auto**	Stale A to S Dir optimization.
LLC dead line alloc	Disabled **Enabled** Auto	Enable - opportunistically fill dead lines in LLC. Disable - never fill dead lines in LLC

7.5.3.2. Uncore Per Socket Configuration

Feature	Options	Description
CPU 0	submenu	CPU 0 Configuration\nSilk Screen Equivalent->CPU 1.
Bus Resources Allocation Ratio	**1**	Bus resources allocation ratio, range 0 to 8

7.5.4 Memory Configuration

Feature	Options	Description
Enforce POR	**POR** Disable	Enable - Enforces Plan Of Record restrictions for DDR4 frequency and voltage programming. Disable - Disables this feature and the user can run at higher frequencies, specified in the DDR Frequency Limit field (limited by processor support). Auto - Sets it to the MRC default setting (current default is Enabled).
Enforce Population POR	Disable Enforcement **Enforce Supported Populations** Enforce Validated Populations	Enable Memory Population POR Enforcement. Selecting Enforce Validated Populations will only allow populations that have been validated.
PPR Type	PPR Disabled Hard PPR **Soft PPR**	Selects Post Package Repair Type - Hard / Soft / Disabled. Auto - Sets it to the MRC default setting; current default is Soft PPR.
PPR Error Injection test	**Disabled** Enabled	Enable / Disable support for c-script err inj test.

Memory Frequency	**Auto** 1200 1333 1400 1600 1800 1866 2000 2133 2200 2400 2600 2666 2800 2933 3000 3200 3400-OvrClk 3466-OvrClk 3600-OvrClk 3733-OvrClk 3800-OvrClk 4000-OvrClk 4200-OvrClk 4266-OvrClk 4400-OvrClk 4800-OvrClk	Maximum Memory Frequency Selections in Mhz. If Enforce POR is disabled, the user will be able to run at higher frequencies than the memory support (limited by processor support). Do not select Reserved.
IMC BCLK	**Info only**	
Refresh Watermarks	**Auto** High WM Low WM	Auto selects Low WM (Hi/Panic = 1/2) for 16Gb-based DIMMs and High WM (Hi/Panic = 8/9) for other DIMM configs. Low WM can mitigate power delivery issues with 128GB and larger DIMMs. Low WM can also mitigate failures due to row hammer traffic patterns. High WM can provide better performance when power delivery and row hammer are not a concern.

pTRR	**Disabled** Enabled	Enable / Disable pTRR support.
MRC Promote Warnings	**Disabled** Enabled	Determines if MRC warnings are promoted to the system level.
Promote Warnings	Disabled **Enabled**	Determines if warnings are promoted to the system level.
Halt on mem Training Error	Disabled **Enabled**	Halt on mem Training Error Disable/Enable
Multi-Threaded MRC	**Disabled** Enabled	Enable - Executes the Memory Reference Code multi-threaded. Disable - Disables this feature. Auto - Sets it to MRC default setting; current default is Enable.
SPD CRC Check	**Auto** Disabled Enabled	Enable to turn on checking the SPD CRC.
Enhanced Log Parsing	**Disabled** Enabled	Enables additional output in the debug log for easier machine parsing
LRDIMM Module Delay	Disabled **Auto**	When Disabled, MRC will not use SPD bytes 90-95 for LRDIMM Module Delay. When Auto, MRC will boundary check the values and use default values, if SPD is 0 or out of range
Allow Untested Memory for DXE Drivers	Disabled **Enabled**	Enable - Sets the TESTED flag for all memory in PEI, making it available for DXE Drivers' usage.
SmartTestKey	**0**	Number of SmartTest Key
MemTest	Disabled **Enabled**	Enable - Enables memory test during normal boot. Disable - Disables this feature.
MemTest Loops	**1**	Number of memory test loops during normal boot, set to 0 to run memtest infinitely
Adv MemTest Options	**0**	This option is a bit mask[19:0]: All 0 = disabled: bit-0=XMATS8, bit-1=XMATS16, bit-2=XMATS32, bit-3=XMATS64, bit-4=WCMATS8, bit-5=WCMCH8, bit-6=GNDB64, bit-7=MARCHCM64, bits[8:10]=Reserved, bit-11=TWR, bit-12=DATARET, bit-13=MATS8TC1, bit-14=MATS8TC2, bit-15=MATS8TC3, bit-16=SK-HYNIX, bit-17=SAMSUNG, bit-18=MICRON, bit-19=SCRAM_X2
Number of Ranks to Test	**0**	Select how many Ranks will be tested by AdvMemTest. A maximum of 8 Ranks are allowed. A default value of 0 will test all present Ranks in the system.

Adv MemTest PPR	Disabled **Enabled**	This option enable/disable ppr flow for MemTest
Adv MemTest Retry After Repair	Disabled **Enabled**	Enables/disables Retry of the current Adv MemTest step after a PPR repair is done.
Adv MemTest Reset Failure Tracking List	**Disabled** Enabled	Enable/disable Reset of the Row Failure Tracking List after each Adv MemTest option. Useful for testing the performance of multiple options.
Adv MemTest Conditions	Disable **Auto** Manual	Auto = set test conditions based on test type; Manual = specify global test conditions; Disable = Do not apply test conditions.
Training Result Offset	**Disabled** Enabled	Enable - Enables training results to be offset. Disable - Disables this feature; enabled by default
Memory Type	RDIMMs only UDIMMs only **UDIMMs and RDIMMs**	Selects the Memory type supported by this platform.
Attempt Fast Boot	**Disabled** Enabled	Enable - Portions of memory reference code will be skipped when possible to increase boot speed on warm boots. Disable - Disables this feature. Auto - Sets it to the MRC default setting; the current default is Disable.
Attempt Fast Cold Boot	Disabled **Enabled**	Enable - Portions of memory reference code will be skipped when possible to increase boot speed on cold boots. Disable - Disables this feature. Auto - Sets it to the MRC default setting; the current default is Disable.
MemTest On Cold Fast Boot	**Disabled** Enabled	Enable - Enables memory test during cold fast boot. Disable - Disables this feature. Auto - Sets it to the MRC default setting; the current default is Disable.
DDRT DIMM BCOM Margining Support	**Disabled** Enabled	Enables DDRT DIMM BCOM margining support for RMT and BSSA.
BDAT	Disabled **Enabled**	Enable Disables publishing BDAT ACPI Table
Data Scrambling for DDR4/5	Disabled **Enabled**	Enable - Enables data scrambling for DDR4 and DDR5. Disable - Disables this feature. Auto - Sets it to the MRC default setting; the current default is Enable.
Allow Memory Training Correctable Error	**Disabled** Enabled	Enable - Allows correctable errors during memory training. Disable - Disables this feature. Auto - Sets it to the MRC default setting; the current default is Disable.

Allow Memory Test Correctable Error	Disabled **Enabled**	Enable - Logs error and allows correctable errors during memory test (DIMM Rank not removed). Disable - Logs error and removes DIMM Rank. Auto - Sets it to the MRC default setting; the current default is Enable.
WR CRC feature Control	**Disabled** Enabled	Enable - Enables Write CRC. Disable - Disables this feature.
DIMM Isolation Enable	Disabled **Enabled**	Enable - Enables DIMM Isolation for Command/Address Parity and Write CRC. Disable - Disables this feature; the current default is Enable.
Write Preamble TCLK	1TCLK 2TCLK **Auto**	Override WritePreamble to 1TCLK or 2TCLK. Auto will set WritePreamble timing to 1TCLK. PMem configurations do not support 2TCLK.
Read Preamble TCLK	1TCLK 2TCLK **Auto**	Override ReadPreamble to 1TCLK or 2TCLK. Auto will set ReadPreamble timing to 2TCLK for speeds 2933 and above. DDR4 speeds below 2400 and PMem configurations do not support 2TCLK.
Rank Switch Configuration	Disable TA Floor **Rcven Ave** Reserved	TA Floor enforces t_rrdr, t_rrdd minimum of 3; Rcven Ave attempts to match Rcven logic delay across ranks
Scrambling Seed Low	**41003**	Low 32 bits of the scrambling seed.
Scrambling Seed High	**54165**	High 32 bits of the scrambling seed.
Enable ADR	**Disabled** Enabled	Enables the detecting and enabling of ADR\nThis is not available if eADR is enabled since eADR requires ADR to be enabled.
Custom Refresh Enable	**Disabled** Enabled	Enable/disable a custom memory refresh rate.
2x Refresh Enable	**Auto** Disable Enable	Enable/Disable 2x Refresh.
DLL Reset Test	**0**	Set this to the number of loops to execute the DDL reset test. The test will execute RMT for the provided number of loops without DLL resets and then it will execute RMT for the same number of loops with DLL resets.

Opp read during WMM	Disabled **Enabled**	Enable - Enables issuing read commands opportunistically during Write Major Mode. Disable - Disables this feature. Auto - Sets it to the MRC default setting; the current default is Enable.
Normal Operation Duration	**400**	Set normal operation duration interval (0 - 65535)
SMB Clock Frequency	100 Khz **400 Khz** 700 Khz 1 Mhz	Sets DDR4 SMBus Clock Frequencies For SPD Access. The current default is 700Khz. Note: If Intel Optane Persistent Memory (PMem) is present, SMBus Clock Frequency is restricted to 400Khz regardless of this setting.
SPD-SMBUS Access	**Lock** Unlock	Allow Cpu Spd Smbus access to be Locked\UnLocked before booting to OS
DDR Cycling	**Disabled** Enabled	When enabled, MRC will train the memory and then power cycle over and over to stress MRC
Mem Flows	**FFFFFFFF**	Enable(1)/Disable(0) memory training steps in MRC flow; X_OVER-BIT0; SENSE_AMP-BIT1; E_CMDCLK-BIT2; REC_EN-BIT3; RD_DQS-BIT4; WR_LVL-BIT5; WR_FLYBY-BIT6; WR_DQ-BIT7; CMDCLK-BIT8; RD_ADV-BIT9; WR_ADV-BIT10; RD_VREF-BIT11; WR_VREF-BIT12; RT_OPT-BIT13; RX_TX_DESKEW-BIT14; TX_EQ-BIT15; IMODE-BIT16; EARLY_RID-BIT17; DQ_SWIZ-BIT18; LRBUF_RD-BIT19; LRBUF_WR-BIT20; RANK_MARGIN-BIT21; EARLY_WR_VREF-BIT22; EARLY_RD_VREF-BIT23; LR_RD_VREF-BIT24; MEM_INIT-BIT25; DQ_SWIZZLE_EN-BIT26; NORMAL_MODE-BIT27; CMD_VREF-BIT28; LR_WR_VREF-BIT29; MEMTEST-BIT30; E_CTLCLK-BIT31.
Mem FlowsExt	**FFFFFFFF**	Enable(1)/Disable(0) memory training steps in MRC flow; RX_CTLE_EN-BIT0; PXC_EN-BIT1; CMD_NORM_EN-BIT2; LRDIMM_BKSIDE_DQ-BIT3; DRAM_RX_EQ-BIT4; BCOM-BIT5; CHECK_POR-BIT6; MMRC_INIT-BIT7; THROTTLING_EARLY-BIT8; THROTTLING-BIT9; POST_TRAINING-BIT10; E_CONFIG-BIT11; L_CONFIG-BIT12; BIOS_SSA_RMT_EN-BIT13; MCODT_EN-BIT14; MCRON_EN-BIT15; DIMMRON_EN-BIT16; QCA_EN-BIT17; X16_DQSWIZ-BIT18; TCO_COMP_EN-BIT19; TX_SLEW_RATE_EN-BIT20; INIT_MEMMAP-BIT21; CMD_TX_EQ_EN-BIT22; RCOMP_STAT_LEG-BIT23; DDJC_EN-BIT24; RX_DFE_EN-BIT25; DCS-BIT26; QCS-BIT27; DCA-BIT28; HW_XOVER_EN-BIT29; CMI_SMEE_CFG_EN-BIT30; QxCA_CLK_EN-BIT31.
Mem FlowsExt2	**FFFFFFFF**	Enable(1)/Disable(0) memory training steps in MRC flow; TX_DQDQS_PRE_DFE-BIT0; TX_DQDQS_POST_DFE-BIT1; DCA_DUTY-BIT2; RCD_DCA_DFE-BIT3; RX_DQDQS_PRE_DFE_BIT4; RX_DQDQS_POST_DFE_BIT5; TX_PERIODIC_RETRAIN-BIT6; CA_SLEW_RATE-BIT7; DCA_TCO-BIT8; E_REQ_CLK-BIT9; TURNAROUND_TRAIN-BIT10; RX_DFE-BIT11; TX_DFE-BIT12; DQ_SLEW_RATE-BIT13; DB_DFE-BIT14.
Mem FlowsExt3	**FFFFFFFF**	Enable(1)/Disable(0) memory training steps in MRC flow
BLOCK GNT2CMD1CYC	PO Safe Value **POR**	Enable\Disable BLOCK GNT2CMD1CYC.

Cmd Setup % Offset	**50**	Cmd setup / hold percent offset for late cmd traning result. The possible values are from 0 to 100.
Periodic Rcomp	**Auto** Disable Enable	Anto(2)/Enable(1)/Disable(0) Memory Periodic Rcomp cycles.
Periodic Rcomp Interval	10.24 us 20.48 us 40.96 us 81.92 us 163.84 us 327.68 us 655.36 us 1310.72 us 2621.44 us 5242.88 us 10.48576 ms 20.97152 ms 41.94304 ms 83.88608 ms 167.77216 ms 335.54432 ms **671.08864 ms**	Memory Periodic Rcomp interval. The possible values for the registeredCOMP_INTERVAL is from 0 to 15. The time is indicated by power(2,COMP_INTERVAL)*10.24 usec.
Memory Topology	submenu	Displays memory topology with Dimm population information.
Page Policy	submenu	Set memory page policy parameters.
Memory Training	submenu	DDR4 training options.
Memory Boot Health Check	submenu	Check the restored memory margin offsets are within Warning\Critical Limits.
Memory Timings Override	submenu	Selects the XMP profile to use.
Memory Map	submenu	Set memory mapping settings.
Memory RAS Configuration	submenu	Displays and provides options to change the Memory RAS Settings.
BSSA Configuration Menu	submenu	Configuration options for the BSSA Tool.

CMI Init Configuration	submenu	Helps configure cmi init

7.5.4.1. Memory Topology

Feature	Options
Socket0.Chx.Dimmx:	Info only

7.5.4.2. Page Policy

Feature	Options	Description
Page Policy	Closed **Adaptive**	Select Page Policy.

7.5.4.3. Memory Training

Feature	Options	Description
Command Normalization	Disable **Enable**	Enable/Disable Command Normalization.
LRDIMM Backside Vref	Disable **Enable**	Enable\Disable LRDIMM Backside Vref Training.
Command Vref Training	Disable **Enable**	Enable\Disable Command Vref
MC RON Training	Disable **Enable**	Enable\Disable MC RON Training.
DRAM RON Training	**Disable** Enable	Enable\Disable DRAM RON Training.

Rx ODT Training	Disable **Enable**	Enable\Disable Rx ODT Training
Rx CTLE Training	Disable **Enable**	Enable\Disable Rx CTLE Training.
LRDIMM Write Vref	Disable **Enable**	Enable\Disable LRDIMM Write Vref Training.
LRDIMM Read Vref	Disable **Enable**	Enable\Disable LRDIMM Read Vref Training.
LRDIMM TX DQ Centering	Disable **Enable**	Enable\Disable LRDIMM TX DQ Centering.
LRDIMM RX DQ Centering	Disable **Enable**	Enable\Disable LRDIMM RX DQ Centering.
Tx Eq Training	Disable **Enable**	Enable/Disable Tx Eq Training.
CMD Tx Eq Training	**Disable** Enable	Enable/Disable CMD Tx Eq Training.
Rx Dfe Training	**Disable** Enable	Enable/Disable Rx DFE Training. AUTO will enable if DDR Freq >= 2400. Enable or Disable will control Rx DFE regardless of frequency.
TX Rise Fall Slew Rate Training	Disable Enable **Auto**	Enable/Disable TX Rise Fall Slew Rate Training. AUTO will enable if DDR Freq >= 2933. Enable or Disable will control TXRFSR regardless of frequency.
iMode Training	Disable **Enable**	Enable/Disable iMode Training.
Tco Comp Training	**Disable** Enable	Enable/Disable Tco Comp Training.
RoundTrip Latency Training	Disable **Enable**	Enable/Disable RoundTrip Latency Training.

Duty Cycle Training	Disable **Enable**	Enable/Disable Duty Cycle Training.
Read Vref Centering	Disable **Enable**	Read Vref Centering Disable/Enable.
Eye Diagrams	**Disable** Enable	Enables Rx and Tx Dq eye diagrams for each rank.
Turnaround Time Optimization	Disable **Enable**	Enables optimal turnaround times.
One Rank Timing Mode	Disable **Enable**	LRDIMM One Rank Timing Mode turnaround time optimization.
PDA	Disable **Enable**	Enables Per DRAM Addressing.
Write Vref Centering	Disable **Enable**	Write Vref Centering Disable/Enable.
PXC Training	Disable **Enable**	Enable/Disable PXC Training.

7.5.4.4. Memory Boot Health Check

Feature	Options	Description
Memory Boot Health Check	**Auto** Manual Disable	Check the restored memory margin offsets are within Warning\Critical Limits.

7.5.4.5. Memory Timings Override

Feature	Options	Description
XMP Profile	**Disable** Manual	Selects the XMP profile to use.

7.5.4.6. Memory Map

Info only

7.5.4.7. Memory RAS Configuration

Feature	Options	Description
Enable Pcode WA for SAI PG	**Disable** Enable	Enable Pcode Work Around for SAI Policy group for A Step.
Mirror Mode	**Disable** Full Mirror Mode	Full Mirror Mode will set the entire 1LM memory in the system to be mirrored, consequently reducing the memory capacity by half. Partial Mirror Mode will enable the required size of memory to be mirrored. If rank sparing is enabled partial mirroring will not take effect. Enabling any type of Mirror Mode will disable XPT Prefetch.
Memory Correctable Error Flood Policy	Disable Once **Frequency**	
Correctable Error Threshold	**7FFF**	Correctable Error Threshold (0x01 - 0x7fff) used for sparing, and leaky bucket.
Trigger SW Error Threshold	**Disable** Enable	Enable or Disable Sparing trigger SW Error Match Threshold
Leaky bucket time window based interface	**Disable** Enable	Enable/Disable leaky bucket time window based interface.
Leaky bucket low bit	**28**	Leaky bucket low bit (0x1 - 0x29).
Leaky bucket high bit	**29**	Leaky bucket high bit (0x1 - 0x29).

Partial Cache Line Sparing PCLS	Disable **Enable**	Enable/Disable PCLS Sparing.
ADDDC Sparing	**Disable** Enable	Enable/Disable ADDDC Sparing.
Column Correction Disable	**Disable** Enable	Disable - Turns ON Column Correction feature. Enable - Turns OFF Column Correction feature.
Patrol Scrub	Disable Enable **Enable at End of POST**	Enable/Disable Patrol Scrub.
Patrol Scrub Interval	**24**	Selects the number of hours (1-24) required to complete full scrub. A value of zero means auto!.

7.5.4.8. BSSA Configuration Menu

Feature	Options	Description
BSSA Rank Margin Tool	Disable **Enable**	Enables the BSSA Rank Margin Tool.
Rmt on Advanced Memtest	**Disable** Enable	Execute RMT after advanced Memory Training, as per memory policy.
BSSA RMT on Fast Cold Boot	**Disable** Enable	Enable/Disable the BSSA Rank Margin Tool on a Fast Cold Boot.
Per Bit Margining	Disable **Enable**	Enable Per Bit Margining.
Display Tables	Disable **Enable**	Enable displaying results as tables.
Display Plots	Disable **Enable**	Enable the display of per-bit results as plots.
Loop Count	**16**	Exponential loop count for single rank test.

Backside Margining	**Disable** Enable	Enable margin test on the register or buffer backside.
Early Read ID Margining	**Disable** Enable	Enable PMem Early Read ID test.
Step Size Override	**Disable** Enable	Enable overriding the default step sizes.
RMT Debug Messages	**Disable** Enable	Enables the BSSA RMT debug messages.
RMT Minimum Margin Check	Disable **Enable**	Enable RMT minimum margin check.

7.5.4.9. CMI Init Configuration

Feature	Options	Description
CMI Init Option	**Auto** Register default Value	Select Auto/Register default Value for spreadsheet value programming/normal register default value.

7.5.5 IIO Configuration

Feature	Options	Description
Socket0 Configuration	submenu	
IOAT Configuration	submenu	All IOAT configuration options.
IntelÂ® VT for Directed I/O (VT-d)	submenu	Press <Enter> to bring up the IntelÂ® Virtualization for Directed I/O (VT-d) Configuration menu.
IntelÂ® VMD technology	submenu	Press <Enter> to bring up the IntelÂ® VMD for Volume Management Device Configuration menu.
IntelÂ® AIC Retimer/AIC SSD Technology (non-VMD)	submenu	Press <Enter> to bring up the IntelÂ® AIC Retimer/AIC SSD Configuration menu.
IIO Global Performance Tuning	submenu	All IIO performance tuning configuration options.

PCIe Train by BIOS	No **Yes**	Assume IIO is strapped for Wait-for-BIOS because straps are unreliable in A-0 Silicon.
NTB Link Train by BIOS	No Yes **Auto**	This knob enables or disables the BIOS to train the NTB link.
Delay before link training	**No delay** 100ms 300ms 500ms 1s 2s	Custom delay before PCIe link training on IIO ports.
PCIe Hot Plug	**No** Yes	Enable/Disable PCIe Hot Plug globally.
Mask PCIe RP warm reset MCA	Disable **Enable**	Enable/Disable Mask CPU Complex PCIe Root Port warm reset MCA.
PCIe ACPI Hot Plug	**No** Yes Per-Port	Enable/Disable PCIe ACPI Hot Plug globally, or allow per-port control. When Disabled, MSI is generated on the HP event. When Enabled, _HPGPE message is generated.
PCIe Low Latency Retimers	**No** Yes	Enable/Disable PCIe low latency retimers.
Skip PCIe retimers detection	**No** Yes	Skip PCIe retimers detection to speed up the boot. Retimers are present only in specific HW configurations.
CbDma MultiCast Enable	No **Yes**	Enable CbDma MultiCast (for validation use).
MultiCast Enable	**No** Yes	Enable MultiCast (for validation use).
NoSnoop Read Config	**Disable** Enable	NoSnoop Read Configuration.

NoSnoop Write Config	Disable **Enable**	NoSnoop Write Configuration.
Max Read Comp Comb Size	**Minimum** Maximum	Minimum or Maximum size.
Problematic port	**Disable** NP-NP problematic P-P problematic	Selects whether problematic port lock flows need to be enabled in the system. The selection allows for P-P or NP-NP lock flows or neither.
DMI Allocating Write Flows	Non-Allocating **Allocating**	Selects DMI Vc0/VCp writes selection as either allocating or non-allocating. Auto enables POR setting
PCIe Allocating Write Flows	Non-Allocating **Allocating**	Selects Vc0/VCp writes selection for all CPU PCIe ports as either allocating or non-allocating. Auto enables POR setting.
Skip Halt On DMI Degradation	**No** Yes	Enable this option to avoid the system being halted on DMI width/link degradation.
Hide PCU Func 6	**Disable** Enable	Hide Power Control Unit Device 30 Function 6.
EN1K	**No** Yes	Enables 1K granularity for I/O space to decode in each of the virtual P2P bridges corresponding to root ports, and DMI ports.
Dual CV IO Flow	No **Yes**	Allow ucode enable Dual CV feature in the Cbo.
PCIE Coherent Read Partial	**PCIRdCur Setting** PRd Setting	Configures Coherent Reads for Available Settings
PCIE Coherent Read Full	**PCIRdCur Setting** PRd Setting	Configures Coherent Reads for Available Settings
PCI-E Completion Timeout	Per-Port **Global**	Configure PCIe Completion Timeout in Device Control2 register.

PCI-E Completion Timeout	50us to 50ms 50us to 100us 1ms to 10ms 16ms to 55ms 65ms to 210ms **260ms to 900ms** 1s to 3.5s Disable	Configure PCIe Completion Timeout in Device Control2 register.
PCI-E ASPM Support (Global)	Disable **Per-Port**	This option can disable ASPM support in all PCIe root ports.
Snoop Response Hold Off	**9**	Sets Snoop Response Hold Off value, 256 cycles as Default.
PCIe LTR Support	Disable **Auto**	This option can disable Latency Tolerance Reporting support in all PCIe root ports. 'Auto' keeps hardware default.
PCIe Extended Tag Support	Disable **Auto**	This option can disable 8-bit Tag support in all PCIe root ports. 'Auto' keeps hardware default.
PCIe 10-bit Tag Support	Disable **Auto**	This option can disable PCIe 10-bit Tag Requester support in all PCIe root ports. 'Auto' keeps hardware default.
PCIe Atomic Op Support	Disable **Auto**	This option can disable the Atomic Operation Routing support in all PCIe root ports and block Atomic Operation Requester in the PCI hierarchy. 'Auto' keeps hardware default.
PCIe Max Read Request Size	Keep Default 128B 256B 512B 1024B 2048B **4096B**	This option can set the requested Max Read Request Size in the PCI hierarchy. 'Default' keeps hardware default.
PCIe PTM Support	Disable **Auto**	This option can disable Precision Time Management support in the PCI hierarchy. 'Auto' keeps hardware default.
PCIe Relaxed Ordering	No **Yes**	Enable Relaxed Ordering in PCIe devices where it is supported. Note that in some devices it can be not supported, hardwired to zero.

PCIe PHY test mode	**No** Yes	PCIe PHY test mode Enable/Disable

7.5.5.1. Socket0 Configuration

Feature	Options	Description
IOU0 (IIO PCIe Port 1)	**Auto** X4X4X4X4 X4X4X8 X8X4X4 X8X8 X16	Selects PCIe port Bifurcation for selected slot(s)".
Sck0 RP Correctable Err	**No** Yes	Applies to root ports only. Enable interrupt on correctable errors.
Sck0 RP NonFatal Uncorrectable Err	**No** Yes	Applies to root ports only. Enable interrupt on a non-fatal error.
Sck0 RP Fatal Uncorrectable Err	**No** Yes	Applies to root ports only. Enable MSI/INTx interrupt on fatal errors.
TraceHub Configuration Menu		TraceHub Configuration Settings.
North Trace Hub Enable Mode	**Disable** Target Debugger Host Debugger	Select 'Host Debugger' if Trace Hub is used with the host debugger tool or 'Target Debugger' if Trace Hub is used by target debugger software.
R-Link	submenu	Settings related to PCI Express Ports (0/1A/1B/1C/1D/2A/2B/2C/2D/3A/3B/3C/3D/4A/4B/4C/4D/5A/5B/5C/5D)
Link Speed	**Auto** Gen 1 (2.5 GT/s) Gen 2 (5 GT/s) Gen 3 (8 GT/s)	Choose Link Speed for this PCIe port.
PCI-E Port DeEmphasis	**-6.0 dB**	De-Emphasis control (LNKCON2[6]) for this PCIe port.

Feature	Options	Description
	-3.5 dB	
PCI-E Port Link Status	Info only	
PCI-E Port Link Max	Info only	
PCI-E Port Link Speed	Info only	
PCI-E Port Clocking	**Common** Distinct	Configure port clocking via LNKCON[6]. This refers to this component and the downstream components.
PCI-E Port Clock Gating	Disable **Enable**	Enable/Disable Clock Gating for this PCIe port.
Data Link Feature Exchange	Disable **Enable**	Enable/Disable data link feature negotiation in the Data Link Feature Capabilities (DLFCAP) register.
DMI Port MPSS	128B 256B **Auto**	Configure Max Payload Size Supported in the DMI Device Capabilities register. 'Auto' keeps hardware default. If 'Auto' is not used make sure MPSS in PCH root ports is updated to the same or smaller value.
PCI-E Port D-state	D0 D3Hot	Set to D0 for normal operation, D3Hot to be in a low-power state.
PCI-E Completion Timeout	50us to 50ms 16ms to 55ms 65ms to 210ms **260ms to 900ms** 1s to 3.5s Disable	Configure PCIe Completion Timeout in the Device Control2 register.
PCI-E ASPM Support	Disable **Auto**	This option can disable ASPM support in a PCIe root port. 'Auto' keeps hardware default.
PCI-E Port L1 Exit Latency	<1uS 1uS - 2uS 2uS - 4uS 4uS - 8uS 8uS - 16uS	The length of time this port requires to complete the transition from L1 to L0.

Feature	Options	Description
	16uS - 32uS **32uS - 64uS** >64uS	
MSI	**Disable** Enable	BUS0 DEVx FUN0 OFF 0x5A bit 0, Where X is 0-3.
PCI-E Extended Sync	**No** Yes	Enable / disable the Extended Sync Mode (D:x F:0 O:7Ch B:7) where x is 0-9.
Compliance Mode	**No** Yes	Enable/Disable Compliance Mode for this PCIe port.
EOI	Disable **Enable**	Dev 0,2,3 MISCCTRLSTS (Reg 0x188)Bit 26.
Unsupported Request	**Disable** Enable	Controls the reporting of unsupported requests that IIO itself detects on requests it receives from a PCI Express/DMI port.
Alternate TxEq	**Disable** Enable	Enable or Disable TxEq.
Alt ATTEN Table	**Disable** Enable	Enable/Disable Alternate Attenuator Table.
SRIS	**Disable** Enable	Enable or Disable SRIS.
ECRC Generation	**Disable** Enable	Enable or Disable ECRC Generation (Error Capabilities and Control Register).
ECRC Check	**Disable** Enable	Enable or Disable ECRC Check (Error Capabilities and Control Register).
SERRE	**Disable** Enable	Enable or Disable SERRE (SERR Reporting Enable).
MCTP	No **Yes**	Enable/Disable MCTP.

7.5.5.2. IOAT Configuration

Feature	Options	Description
Sck0 IOAT Config	submenu	
IOAT Function 0 Items	Show only	
DMA	No **Yes**	Select Dma Enable/Disable for each CB device.
No Snoop	**No** Yes	No Snoop Enable/Disable for each CB device.
IOAT Function 1 Items	Show only	
DMA	No **Yes**	Select Dma Enable/Disable for each CB device.
No Snoop	**No** Yes	No Snoop Enable/Disable for each CB device.
IOAT Function 2 Items	Show only	
DMA	No **Yes**	Select Dma Enable/Disable for each CB device.
No Snoop	**No** Yes	No Snoop Enable/Disable for each CB device.
IOAT Function 3 Items	Show only	
DMA	No **Yes**	Select Dma Enable/Disable for each CB device.
No Snoop	**No** Yes	No Snoop Enable/Disable for each CB device.
IOAT Function 4 Items	Show only	
DMA	No **Yes**	Select Dma Enable/Disable for each CB device.

Feature	Options	Description
No Snoop	**No** Yes	No Snoop Enable/Disable for each CB device.
IOAT Function 5 Items	Show only	
DMA	No **Yes**	Select Dma Enable/Disable for each CB device.
No Snoop	**No** Yes	No Snoop Enable/Disable for each CB device.
IOAT Function 6 Items	Show only	
DMA	No **Yes**	Select Dma Enable/Disable for each CB device.
No Snoop	**No** Yes	No Snoop Enable/Disable for each CB device.
IOAT Function 7 Items	Show only	
DMA	No **Yes**	Select Dma Enable/Disable for each CB device.
No Snoop	**No** Yes	No Snoop Enable/Disable for each CB device.
Disable TPH	**No** Yes	TLP Processing Hint disable.
Prioritize TPH	Enable **Disable**	Prioritize TPH.
Relaxed Ordering	**No** Yes	Relaxed Ordering Enable/Disable.

7.5.5.3. Intel® VT for Directed I/O (VT-d)

Feature	Options	Description
Intel® VT for Directed I/O	**Enable** Disable	Enable/Disable IntelÂ® Virtualization Technology for Directed I/O (VT-d) by reporting the I/O device assignment to VMM through DMAR ACPI Tables.
DMA Control Opt-In Flag	Enable **Disable**	Enable/Disable DMA_CTRL_PLATFORM_OPT_IN_FLAG in the DMAR table in ACPI. Not compatible with Direct Device Assignment (DDA).
Interrupt Remapping	**Auto** Enable Disable	Enable/Disable VT-d Interrupt Remapping Support.
X2APIC Opt Out	Enable **Disable**	Enable/Disable X2APIC_OPT_OUT bit.
Pre-boot DMA Protection	Enable **Disable**	Enable DMA Protection in the Pre-boot environment (If the DMAR table is installed in DXE and If VTD_INFO_PPI is installed in PEI.)
PCIe ACSCTL	Enable **Disable**	Enable/Disable overwrite of PCI Access Control Services Control register in PCI root ports.

7.5.5.4. Intel® VMD technology

Feature	Options	Description
Intel® VMD for Volume Management Device on Socket 0	submenu	
Enable/Disable VMD	Enable **Disable**	Enable/Disable VMD in this Stack.

7.5.5.5. Intel® AIC Retimer/AIC SSD Technology (non-VMD)

Feature	Options	Description
Intel® AIC Retimer/AIC SSD on Socket 0	submenu	
Intel® AIC Retimer/AIC SSD HW at Stack1	Enable **Disable**	Announce Intel® AIC Retimer/AIC SSD HW at Stack1(Port2A-2D, 3A-3D). Override IOUx bifurcation if required.

7.5.5.6. IIO Global Performance Tuning

Feature	Options	Description
Performance Tuning Mode	Safe Mode **Performance Enable Mode**	Select IIO performance tuning mode, where Safe mode contains the default HW state and Performance Enable Mode has the recommended performance values.

7.5.6 Advanced Power Management Configuration

Feature	Options	Description
Pcode Dispatcher Watchdog Timer	Disable Enable **Auto**	Enable/disable Pcode Dispatcher Watchdog Timer.
CPU P State Control	submenu	P State Control Configuration Sub Menu, include Turbo, XE and etc.
Hardware PM State Control	submenu	Hardware P-State setting.
Frequency Prioritization	submenu	Frequency Prioritization Control.
Overclocking	submenu	Provide manual XE Ratio Limit setting.
CPU C State Control	submenu	CPU C State setting.
Package C State Control	submenu	Package C State setting.
CPU Thermal Management	submenu	CPU Thermal Related setting.

Feature	Options	Description
CPU - Advanced PM Tuning	submenu	Setting Energy Per Bias, Pwr_Ctl, PP0 Current SWLTD, SAPM etc.
Package Current Config	submenu	Program PRI_PLANE_CURT_CFG_CTRL_MSR 0x601 Sub Men
SOCKET RAPL Config	submenu	SOCKET RAPL Configuration Sub Menu - TURBO_POWER_LIMIT CSR & MSR.
PMax Detector Configuration	submenu	PMax Detector Control Sub Menu
ACPI Sx State Control	submenu	ACPI Sx State Control individually
Memory Power & Thermal Configuration	submenu	Displays and provides option to change the Memory Settings.

7.5.6.1. CPU P State Control

Feature	Options	Description
AVX Licence Pre-Grant Override	**Disable** Enable	Enables AVX ICCP pre-grant level override.
SpeedStep (Pstates)	Disable **Enable**	Enable/Disable EIST (P-States).
Config TDP Lock	Disable **Enable**	Config TDP CONTROL Lock Bit.
AVX P1	**Normal** Level 1 Level 2	AVX P1 level selection.
EIST PSD Function	**HW_ALL** SW_ALL	Choose HW_ALL/SW_ALL in _PSD return.
Boot performance mode	**Max Performance** Max Efficient Set by Intel Node Manager	Select the performance state that the BIOS will set before OS hand off.

Feature	Options	Description
Energy Efficient Turbo	Disable **Enable**	Energy Efficient Turbo Disable, MSR 0x1FC [19].
Turbo Mode	Disable **Enable**	Enable/Disable processor Turbo Mode (requires EMTTM enabled too).
CPU Flex Ratio Override	**Disable** Enable	Enable/Disable CPU Flex Ratio Programming.
CPU Core Flex Ratio	Info only	
GPSS timer	0 us 50 us **500 us**	P-state change hysteresis time window.
Perf P-Limit	submenu	Program PERF_P_LIMIT 1:30:2:0xe4 Sub Menu.
Perf P-Limit Differential	1	Parameter used to tune how far below local socket frequency remote socket frequency is allowed to be. Also impacts the rate at which frequency drops when the feature disengages.
Perf P-Limit Clip	1F	The maximum value the floor is allowed to be set to for perf P-limit.
Perf P-Limit Threshold	F	Uncore frequency threshold above which this socket will trigger the feature and start trying to raise the frequency of other sockets.
Perf P Limit	Disable **Enable**	Enable/Disable Performance P-Limit

7.5.6.2. Hardware PM State Control

Feature	Options	Description
Hardware P-States	Disable **Native Mode** Out of Band Mode Native Mode with No Legacy Suppor	Disable: Hardware chooses a P-state based on OS Request (Legacy P-States)\nNative Mode:Hardware chooses a P-state based on OS guidance\nOut of Band Mode:Hardware autonomously chooses a P-state (no OS guidance).
HardwarePM Interrupt	**Disable** Enable	Enable/Disable Hardware PM Interrupt.
EPP Enable	Disable **Enable**	When disabled, HW masks EPP in CPUID[6].10 and uses EPB for EPP.
APS rocketing	**Disable** Enable	Enable/Disable the rocketing mechanism in the HWP p-state selection pcode algorithm. Rocketing enables the core ratio to jump to max turbo instantaneously as opposed to a smooth ramp up.
Scalability	**Disable** Enable	Enable/Disable Core Performance to Frequency Scalability Based Optimizations in the CPU.
Native ASPM	**Auto** Enable Disable	Enabled - OS Controlled ASPM, Disabled - ASPM Off, AUTO - BIOS Controlled ASPM.

7.5.6.3. Frequency Prioritization

Feature	Options	Description
RAPL Prioritization	Disable **Enable**	This knob controls whether RAPL balancer is enabled. When enabled it activates per core power budgeting.

7.5.6.4. Overclocking

Feature	Options	Description
Extreme Edition	Disable **Enable**	Enable/Disable Extreme Edition support.
TurboRatioLimit0	0	User defined Ratio for TurboRatioLimits Msr(0x1AD).
TurboRatioCores0	FF	User defined core# for TurboRatioLimits Msr(0x1AE).
TurboRatioLimit1	4	User defined Ratio for TurboRatioLimits Msr(0x1AD).
TurboRatioCores1	FF	User defined core# for TurboRatioLimits Msr(0x1AE).
TurboRatioLimit2	0	User defined Ratio for TurboRatioLimits Msr(0x1AD).
TurboRatioCores2	FF	User defined core# for TurboRatioLimits Msr(0x1AE).
TurboRatioLimit3	0	User defined Ratio for TurboRatioLimits Msr(0x1AD).
TurboRatioCores3	FF	User defined core# for TurboRatioLimits Msr(0x1AE).
TurboRatioLimit4	0	User defined Ratio for TurboRatioLimits Msr(0x1AD).
TurboRatioCores4	FF	User defined core# for TurboRatioLimits Msr(0x1AE).
TurboRatioLimit5	0	User defined Ratio for TurboRatioLimits Msr(0x1AD).
TurboRatioCores5	FF	User defined core# for TurboRatioLimits Msr(0x1AE).
TurboRatioLimit6	0	User defined Ratio for TurboRatioLimits Msr(0x1AD).
TurboRatioCores6	FF	User defined core# for TurboRatioLimits Msr(0x1AE).
TurboRatioLimit7	0	User defined Ratio for TurboRatioLimits Msr(0x1AD).
TurboRatioCores7	FF	User defined core# for TurboRatioLimits Msr(0x1AE).

7.5.6.5. CPU C State Control

Feature	Options	Description
Enable Monitor MWAIT	Disable **Enable**	Allows Monitor and MWAIT instructions.
CPU C1 auto demotion	Disable **Enable**	Allows CPU to automatically demote to C1. Takes effect after reboot.
CPU C1 auto undemotion	Disable **Enable**	Allows CPU to automatically undemote from C1. Takes effect after reboot.
CPU C6 report	Disable Enable **Auto**	Enable/Disable CPU C6(ACPI C3) report to OS.
Enhanced Halt State (C1E)	Disable **Enable**	Core C1E auto promotion Control. Takes effect after reboot.
OS ACPI Cx	**ACPI C2** ACPI C3	Report CC3/CC6 to OS ACPI C2 or ACPI C3

7.5.6.6. Package C State Control

Feature	Options	Description
Package C State	C0/C1 state C2 state C6(non Retention) state **Auto**	Package C State limit.
Register Access Low Latency Mode	**Disable** Enable	Enable lower latency mode for register accesses. Note: Enabling this mode will prevent PkgC6 as register access fabric is prevented from going idle.
C2C3TT	**0**	Default = 0, means [AUTO]. C2 to C3 Transition Timer, PPDN_INIT = 1:10:1:74 Bit[11:0].
Dynamic L1	Disable **Enable**	PCU_MISC_CONFIG Bit[21] = dynamic L1 enable.

Feature	Options	Description
PKG C-state Lat. Neg.	**Disable** Enable	MSR 1FCh Bit[30] = PCH_NEG_DISABLE.
LTR IIO Input	Take IIO LTR input. **Ignore IIO LTR input.**	MSR 1FCh Bit[29] = LTR_IIO_DISABLE. Disable = Ignore IIO LTR input.
Latency Tolerance Requirement (LTR)	submenu	Program PCIE_ILTR_OVRD 1:30:1:0xFC Sub Menu
PCIe LTR Override Control	**Disable** Enable	Allows manual overrides for PCIE_ILTR_OVRD.
Enable PKGC_SA_PS_CRITERIA	Disable Enable **Auto**	Program WRITE_PKGC_SA_PS_CRITERIA Sub Menu.
PkgC SA PS Criteria Power Management Control	submenu	Program WRITE_PKGC_SA_PS_CRITERIA Sub Menu.
CPU0 PKGC_SA_PS_CRITERIA	submenu	Socket Specific PKGC_SA_PS_CRITERIA.
CPU0 Logical_ip_type	**KTI** Rlink MCDDR IIO	WRITE_PKGC_SA_PS_CRITERIA Command [19:12]\nLogical_ip_type\n0h: KTI; 1h: Rlink\n10h-17h: MCDDR0, 1...\n18h-1Fh: HBM0, 1...\n20h-27h: IIO0, 1...\n33h: MDFS.
PKGC_CRITERIA KTI	**Disable** Enable	Enable: B2P WRITE_PKGC_SA_PS_CRITERIA accepts input value.
MDLL Off	Disable Enable **Auto**	Enable to shut down MDLL during SR.
PKGc Interrupt Response Time	submenu	Programmable Package C-state interrupt response time setup control.
C_STATE_LATENCY_CONTROL_0	**Disable** Enable	Programmable Package C-state interrupt response time setup control
C_STATE_LATENCY_CONTROL_1	**Disable** Enable	Programmable Package C-state interrupt response time setup control

Feature	Options	Description
C_STATE_LATENCY_CONTROL_2	**Disable** Enable	Programmable Package C-state interrupt response time setup control

7.5.6.7. CPU Thermal Management

Feature	Options	Description
CPU T State Control	submenu	CPU T State setting.
Software Controlled T-States	**Disable** Enable	Enable/Disable Software Controlled T-States
PROCHOT Modes	Output-only Disable Both Input and Output **Input-only**	When a processor thermal sensor trips (either core), the PROCHOT# will be driven.\nIf bi-direction is enabled, external agents can drive PROCHOT# to throttle the processor.
Therm-Monitor-Status Filter	**Disable** Enable	Enable Filter based therm_monitor_status(IA32_THERM_STATUS[0]) reporting.
PROCHOT RATIO	**0**	Controls the CPU response to an inbound platform assertion of xxPROCHOT# by capping to the programmed ratio. Default value 0 will allow ME to control this value. If ME does not set a ratio, default 0 equates to Pn. A non-zero value will override the ME setting. The min allowed ratio is defined by PLATFORM_INFO[MIN_OPERATING_RATIO].

7.5.6.8. CPU - Advanced PM Tuning

Feature	Options	Description
Uncore Freq Scaling	Disable **Enable**	If disable, user can input Uncore Frequency.
Uncore Freq RAPL	Disable **Enable**	Enable: BYPASS_CLM_RAPL_LIMIT = 0\n\nDisable: BYPASS_CLM_RAPL_LIMIT = 1.

Feature	Options	Description
Energy Perf BIAS	submenu	Energy Perf BIAS Sub Menu.
Power Performance Tuning	**OS Controls EPB** BIOS Controls EPB PECI Controls EPB	Options decides who Controls EPB.\nIn OS mode: IA32_ENERGY_PERF_BIAS is used\nIn BIOS mode: ENERGY_PERF_BIAS_CONFIG is used\nIn PECI mode: PCS53 is used.
PECI PCS EPB	**OS controls EPB** PECI controls EPB using PCS	Controls whether PECI has control over EPB.
Dynamic Loadline Switch	Disable **Enable**	Dynamic Loadline Switch control. MSR 0x1FC[Bit24].
Workload Configuration	**Balanced** I/O sensitive	This allows optimization for the workload characterization. The three options for selection.
Averaging Time Window	**1A**	This is used to control the effective window of the average for C0 an P0 time.
P0 TotalTimeThreshold Low	**28**	The HW switching mechanism DISABLES the performance setting (0) when the total P0 time is less than this threshold.
P0 TotalTimeThreshold High	**3F**	The HW switching mechanism ENABLES the performance setting (0) when the total P0 time is greater than this threshold.
SAPM Control	Disable **Enable**	MSR 1FCh Bit[22] = PWR_PERF_TUNING_DISABLE_SAPM_CTRL.
EET Mode	**Coarse Grained Mode** Fine Grained Mode	Coarse Grained Mode decides whether to grant user request turbo or P1. Fine Grained Mode decides how much turbo to be granted. More helpful with Scalability Enabled.

7.5.6.9. Package Current Configuration

Feature	Options	Description
Current Limit Override	**Disable** Enable	0 - Default, do nothing; 1 - Manual, override Current limitation in 1/8 A increments.
Lock Indication	Disable **Enable**	Lock for CURRENT_LIMIT settings\nMove this into the Config Above.

7.5.6.10. SOCKET RAPL Configuration

Feature	Options	Description
FAST_RAPL_NSTRIKE_PL2_DUTY_CYCLE	**64**	FAST_RAPL_NSTRIKE_PL2_DUTY_CYCLE value between 25 (10%) - 64 (25%).
Package RAPL Limit MSR Lock	**Disable** Enable	Enable/Disable locking of Package RAPL Limit MSR and a reset will be required to unlock the register.
Package RAPL Limit CSR Lock	Disable **Enable**	Enable/Disable locking of Package RAPL Limit CSR and a reset will be required to unlock the register.
PL1 Limit	Disable **Enable**	Enable/Disable PL1. If this option is disabled, BIOS will program the default values for PL1 Power Limit and PL1 Time Window.
PL1 Power Limit	0	PL1 Power Limit in Watts. The value may vary from 0 to Fused Value. If the value is 0, the fused value will be programmed. A value greater than the fused TDP value will not be programmed.
PL1 Time Window	1	PL1 value in seconds. The value may vary from 0 to 448. Indicates the time window over which the TDP value should be maintained. If the value is 0, the fused value will be programmed.
PL2 Limit	Disable **Enable**	Enable/Disable PL2. If this option is disabled, BIOS will program the default values for PL2 Power Limit and PL2 Time Window.
PL2 Power Limit	0	PL2 Power Limit in Watts. The value may vary from 0 to Fused Value. If the value is 0, BIOS programs 125% * TDP.
PL2 Time Window	1	PL2 value in seconds. The value may vary from 0 to 448. Indicates the time window over which the TDP value should be maintained. If the value is 0, the fused value will be programmed.

7.5.6.11. PMax Detector Configuration

Feature	Options	Description
Detector	Disable **Enable**	Enable/Disable the PMAX detector feature.\n\nWARNING: Disabling this feature can cause system instability.
BIOS Auto Adjustment	**Disable** Enable	Enable BIOS Auto Adjustment.
PMAX Config Sign	**Positive** Negative	Negative: The detector will trip on higher power consumption.\nPositive: Detector will trip on lower power consumption.
PMAX Config Positive Offset	**0**	Input decimal correction factor to the program. Valid input values are 0 to 63. It will be positive or negative depending on PMAX Config Sign value.
Trigger Setup	**0**	Possible selection options [0], [1], [2]\n[0] = Interaction disabled (default)\n[1] = Enable external trigger mode\n[2] = Enable internal trigger observability.

7.5.6.12. ACPI Sx State Control

Feature	Options	Description
ACPI S3	Disable **Enable**	Control ACPI S3 State.
ACPI S4	Disable **Enable**	Control ACPI S4 State

7.5.6.13. Memory Power & Thermal Configuration

Feature	Options	Description
DRAM RAPL Configuration	submenu	DRAM RAPL Control Sub Menu.
DRAM RAPL Power Limit Lock CSR	Disable **Enable**	This Option allows unlock/lock DRAM_PLANE_POWER_LIMIT.pp_pwr_lim_lock.\n\nEnable - Lock\nDisable – Unlock.

Feature	Options	Description
Override BW_LIMIT_TF	0	Allows custom tuning of BW_LIMIT_TF when DRAM RAPL is enabled.
DRAM RAPL	Disable **Enable**	Enable\Disable DRAM Rapl.
DRAM RAPL Extended Range	Disable **Enable**	Select DRAM RAPL Extended Range.
CMS ENABLE DRAM PM	Disable **Enable**	CMS ENABLE DRAM PM.
Memory Thermal	submenu	Set memory thermal settings.
Throttling Mode	Disable OLTT **CLTT** CLTT with PECI	Configure Thermal Throttling Mode.
OFF PKG MEM TO THERMTRIP	**Disable** Enable	If set to 0, the processor will ignore offpkg Memtrip to thermtrip tree. If set to 1 processor will include offpkg Memtrip to thermtrip tree.
OFF PKG MEM TO MEMTRIP	**Disable** Enable	If set to 0, the processor will ignore offpkg memtrip to memtrip tree. If set to 1 processor will include offpkg memtrip to memtrip tree.
Select Temperature Refresh Value	**Auto** Manual	Option to manually enter Temperature refresh value. Select Manual to enter a value; Auto by default.
MEMHOT Throttling Mode	Disable **Enable**	Configure MEMHOT Input and Output Mode: Mem Hot Sense Therm Throt or Mem Hot Output Therm Throt.
MemHot Input Pin	Disable **Enable**	Configure Memhot input.
MemHot Output Pin	Disable **Enable**	Configure Memhot output.
MEMHOT Output Throttling Mode Options	Disable **Enable only temphi** Enable only temphi &	Configure MEMHOT Output Mode options: Enable/Disable the Throt Output high, mid and low bit fields.

Feature	Options	Description
	mid Enable only temphi, mid and low	
Memory Power Savings Advanced Options	submenu	Advanced Settings for CKE and related Memory Power Savings Features.
CKE Throttling	**Auto** Manual	Configures CKE Throttling.
SREF Feature	**Auto** Manual	Select manual or auto programming Self Refresh feature.
PKGC SREF EN	Disable **Enable**	Enables or disables PKGC Self Refresh.

7.6. Security

Feature	Options	Description
Administrator Password	Enter password	Set Administrator Password
User Password	Enter password	Set User Password
HDD Security Configuration	Info only	
Secure Boot	submenu	

7.6.1 Secure Boot Menu

Feature	Options	Description
Secure Mode	Info only	

Feature	Options	Description
Secure Mode	Info only	
Secure Boot	**Disabled** Enabled	Secure Boot feature is Active if Secure Boot is Enabled, Platform Key (PK) is enrolled and the System is in User mode, The mode change requires a platform reset
Secure Boot Mode	**Standard** Custom	Secure Boot mode options: Standard or Custom. In Custom mode, Secure Boot Policy variables can be configured by a physically present user without full
Restore Factory Keys	Info only	Force System to User Mode. Install factory default Secure Boot key databases
Reset To Setup Mode	Info only	
Key Management		Enables expert users to modify Secure Boot Policy variables without full authentication

7.7. Boot

7.7.1 Boot Configuration

Feature	Options	Description
Boot Configuration	Info only	
Setup Prompt Timeout	**3**	Number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite waiting.
Bootup NumLock State	**On** Off	Select the keyboard NumLock state
Quiet Boot	Disabled **Enabled**	Enables or disables Quiet Boot option
Fast Boot	Disabled **Enabled**	Enables or disables boot with initialization of a minimal set of devices required to launch the active boot option. Has no effect on BBS boot options.
SATA Support	Last Boot SATA Devices Only	If set to 'Last Boot SATA Devices' Only, only the last boot SATA device will be available in the POST. If set to "all SATA Devices," all SATA devices will be available during both the OS boot and POST.

Feature	Options	Description
	All SATA Devices	
NVME Support	Disabled **Enabled**	If Disabled, NVMe device will be skipped.
VGA Support	Auto **EFI Driver**	If Auto, only install Legacy OpRom with Legacy OS and logo will NOT be shown during post. Efi driver will still be installed with EFI OS.
USB Support	Disabled Full Initial **Partial Initial**	If Disabled, all USB devices will NOT be available until after the OS boot. If Partial Initial, USB Mass Storage and specific USB port/device will NOT be available before OS boot. If Enabled, all USB devices will be available in OS and Post.
PS2 Devices Support	Disabled **Enabled**	If Disabled, PS2 devices will be skipped.
NetWork Stack Driver Support	**Disabled** Enabled	If Disabled, NetWork Stack Driver will be skipped.
Redirection Support	Disabled **Enabled**	If disable, Redirection function will be disabled.

7.8. Save & Exit

7.8.1 Save Options

Feature	Options	Description
Save Option	Info only	
Save Changes and Exit		Exit system setup after saving the changes.
Discard Changes and Exit		Exit system setup without saving any changes.
Save Changes and Reset		Reset the system after saving the changes.
Discard Changes and Reset		Reset system setup without saving any changes.
Save Changed		Save changes done so far to any of the setup options.
Discard Changes		Discard Changes done so far to any of the setup options.

7.8.2 Default Options

Feature	Options	Description
Default Options	Info only	
Restore Defaults		Restore/Load Default values for all the setup options.
Save as User Defaults		Save the changes done so far as User Defaults.
Restore User Defaults		Restore the User Defaults to all the setup options.
Boot Override	Info only	

8. BIOS Checkpoints, Beep Codes

This document section lists checkpoints and beep codes generated by AMI Aptio BIOS. The checkpoints defined are inherent to the AMIBIOS generic core and do not include any chipset or board-specific checkpoint definitions.

Checkpoints and Beep Codes Definition

A checkpoint is either a byte or word value output to I/O port 80h. The BIOS outputs checkpoints throughout the boot block and Power-On Self-Test (POST) to indicate the task the system is currently executing. Checkpoints are very useful for debugging problems that occur during the preboot process.

Beep codes are used by the BIOS to indicate a serious or fatal error. They are used when an error occurs before the system video has been initialized and generated by the system board speaker.

Aptio Boot Flow

While performing the functions of the traditional BIOS, Aptio 5.x core follows the firmware model described by the Intel Platform Innovation Framework for EFI ("the Framework"). The Framework refers to the following "boot phases", which may apply to various status codes & checkpoint descriptions:

- Security (SEC) – initial low-level initialization
- Pre-EFI Initialization (PEI) – memory initialization[1]
- Driver Execution Environment (DXE) – main hardware initialization[2]
- Boot Device Selection (BDS) – system setup, pre-OS user interface & selecting a bootable device (CD/DVD, HDD, USB, Network, Shell, …)

Viewing BIOS Checkpoints

Viewing all checkpoints generated by the BIOS requires a checkpoint card, also referred to as an OST Card or POST Diagnostic Card. These are PCI add-in cards that show the value of I/O port 80h on a LED display.

Some computers display checkpoints in the bottom right corner of the screen during POST. This display method is limited- since it only displays checkpoints that occur after the video card has been activated.

Keep in mind that not all computers using AMI Aptio BIOS enable this feature. In most cases, a checkpoint card is the best tool for viewing AMI Aptio BIOS checkpoints.

[1]Analogous to "boot block" functionality of legacy BIOS
[2]Analogous to "POST" functionality in legacy BIOS

8.1. Status Code Ranges

Status Code Range	Description
0x01 – 0x0F	SEC execution
0x10 – 0x2F	PEI CAR execution
0x30 – 0x4F	PEI execution after memory detection
0x50 – 0x5F	PEI errors
0x60 – 0xCF	DXE execution
0xD0 – 0xDF	DXE errors
0xE0 – 0xE8	S3 Resume (PEI)
0xE9 – 0xEF	S3 Resume errors (PEI)
0xF0 – 0xF8	Recovery (PEI)
0xF9 – 0xFF	Recovery errors (PEI)

8.2. Standard Status Codes

8.2.1 SEC Phase

Status Code	Description
0x00	Not used

Status Code	Description
Progress Codes	
0x01	Power on. Reset type detection (soft/hard).
0x02	AP initialization before microcode loading
0x03	North Bridge initialization before microcode loading
0x04	South Bridge initialization before microcode loading
0x05	OEM initialization before microcode loading
0x06	Microcode loading
0x07	AP initialization after microcode loading
0x08	North Bridge initialization after microcode loading
0x09	South Bridge initialization after microcode loading
0x0A	OEM initialization after microcode loading
0x0B	Cache initialization

SEC Error Codes	
0x0C – 0x0D	Reserved for future AMI SEC error codes
0x0E	Microcode not found
0x0F	Microcode not loaded

8.2.2 SEC Beep Codes

None

8.2.3 PEI Phase

Status Code	Description
Progress Codes	
0x10	PEI Core is started
0x11	Pre-memory CPU initialization is started
0x12 – 0x14	Reserved for CPU
0x15	Pre-memory North Bridge initialization is started
0x16 – 0x18	Reserved for North Bridge
0x19	Pre-memory South Bridge initialization is started
0x1A – 0x1C	Reserved for South Bridge
0x1D – 0x2A	OEM pre-memory initialization codes
0x2B	Memory initialization. Serial Presence Detect (SPD) data reading
0x2C	Memory initialization. Memory presence detection
0x2D	Memory initialization. Programming memory timing information
0x2E	Memory initialization. Configuring memory
0x2F	Memory initialization (other).
0x30	Reserved for ASL (see ASL Status Codes section below)
0x31	Memory Installed
0x32	CPU post-memory initialization is started
0x33	CPU post-memory initialization. Cache initialization
0x34	CPU post-memory initialization. Application Processor(s) (AP) initialization
0x35	CPU post-memory initialization. Boot Strap Processor (BSP) selection

Status Code	Description
0x36	CPU post-memory initialization. System Management Mode (SMM) initialization
0x37	Post-Memory North Bridge initialization is started
0x38 – 0x3A	Reserved for North Bridge initialization
0x3B	Post-Memory South Bridge initialization is started
0x3C -0x3E	Reserved for South Bridge
0x3F-0x4E	OEM post memory initialization codes
0x4F	DXE IPL is started
PEI Error Codes	
0x50	Memory initialization error. Invalid memory type or incompatible memory speed
0x51	Memory initialization error. SPD reading has failed
0x52	Memory initialization error. Invalid memory size or memory modules do not match.
0x53	Memory initialization error. No usable memory detected
0x54	Unspecified memory initialization error.
0x55	Memory not installed
0x56	Invalid CPU type or Speed
0x57	CPU mismatch
0x58	CPU self-test failed or possible CPU cache error
0x59	CPU micro-code is not found or micro-code update is failed
0x5A	Internal CPU error
0x5B	reset PPI is not available
0x5C-0x5F	Reserved for future AMI error codes

Status Code	Description
S3 Resume Progress Codes	
0xE0	S3 Resume is stared (S3 Resume PPI is called by the DXE IPL)
0xE1	S3 Boot Script execution
0xE2	Video repost
0xE3	OS S3 wake vector call
0xE4-0xE7	Reserved for future AMI progress codes

Status Code	Description
S3 Resume Error Codes	
0xE8	S3 Resume Failed
0xE9	S3 Resume PPI not Found
0xEA	S3 Resume Boot Script Error
0xEB	S3 OS Wake Error
0xEC-0xEF	Reserved for future AMI error codes
Recovery Progress Codes	
0xF0	Recovery condition triggered by firmware (Auto recovery)
0xF1	Recovery condition triggered by user (Forced recovery)
0xF2	Recovery process started
0xF3	Recovery firmware image is found
0xF4	Recovery firmware image is loaded
0xF5-0xF7	Reserved for future AMI progress codes
Recovery Error Codes	
0xF8	Recovery PPI is not available
0xF9	Recovery capsule is not found
0xFA	Invalid recovery capsule
0xFB – 0xFF	Reserved for future AMI error codes

8.2.4 PEI Beep Codes

# of Beeps	Description
1	Memory not Installed
1	Memory was installed twice (InstallPeiMemory routine in PEI Core called twice)
2	Recovery started
3	DXEIPL was not found
3	DXE Core Firmware Volume was not found
4	Recovery failed
4	S3 Resume failed
7	Reset PPI is not available

8.2.5 DXE Status Codes

Status Code	Description
0x60	DXE Core is started
0x61	NVRAM initialization
0x62	Installation of the South Bridge Runtime Services
0x63	CPU DXE initialization is started
0x64 – 0x67	Reserved for CPU DXE initialization (CPU module specific)
0x68	PCI host bridge initialization
0x69	North Bridge DXE initialization is started
0x6A	North Bridge DXE SMM initialization is started
0x6B – 0x6F	Reserved for North Bridge DXE initialization (North Bridge module specific)

Status Code	Description
0x70	South Bridge DXE initialization is started
0x71	South Bridge DXE SMM initialization is started
0x72	South Bridge devices initialization
0x73 – 0x77	Reserved for South Bridge DXE Initialization (South Bridge module specific)
0x78	ACPI module initialization
0x79	CSM initialization
0x7A – 0x7F	Reserved for future AMI DXE codes
0x80 – 0x8F	OEM DXE initialization codes
0x90	Boot Device Selection (BDS) phase is started
0x91	Driver connecting is started
0x92	PCI Bus initialization is started
0x93	PCI Bus Hot Plug Controller Initialization
0x94	PCI Bus Enumeration
0x95	PCI Bus Request Resources
0x96	PCI Bus Assign Resources
0x97	Console Output devices connect
0x98	Console input devices connect
0x99	Super IO Initialization
0x9A	USB initialization is started
0x9B	USB Reset
0x9C	USB Detect
0x9D	USB Enable
0x9E – 0x9F	Reserved for future AMI codes

Status Code	Description
0xA0	IDE initialization is started
0xA1	IDE Reset
0xA2	IDE Detect
0xA3	IDE Enable
0xA4	SCSI initialization is started
0xA5	SCSI Reset
0xA6	SCSI Detect
0xA7	SCSI Enable
0xA8	Setup Verifying Password
0xA9	Start of Setup
0xAA	Reserved for ASL (see ASL Status Codes section below)
0xAB	Setup Input Wait
0xAC	Reserved for ASL (see ASL Status Codes section below)
0xAD	Ready To Boot event
0xAE	Legacy Boot event
0xAF	Exit Boot Services event
0xB0	Runtime Set Virtual Address MAP Begin
0xB1	Runtime Set Virtual Address MAP End
0xB2	Legacy Option ROM Initialization
0xB3	System Reset
0xB4	USB hot plug
0xB5	PCI bus hot plug
0xB6	Clean-up of NVRAM

Status Code	Description
0xB7	Configuration Reset (reset of NVRAM settings)
0xB8 – 0xBF	Reserved for future AMI codes
0xC0 – 0xCF	OEM BDS initialization codes
DXE Error Codes	
0xD0	CPU initialization error
0xD1	North Bridge initialization error
0xD2	South Bridge initialization error
0xD3	Some of the Architectural Protocols are not available
0xD4	PCI resource allocation error. Out of Resources
0xD5	No Space for Legacy Option ROM
0xD6	No Console Output Devices are found
0xD7	No Console Input Devices are found
0xD8	Invalid password
0xD9	Error loading Boot Option (LoadImage returned error)
0xDA	Boot Option is failed (StartImage returned error)
0xDB	Flash update is failed
0xDC	Reset protocol is not available

8.2.6 DXE Beep Codes

# of Beeps	Description
1	Invalid password
4	Some of the Architectural Protocols are not available
5	No Console Output Devices are found
5	No Console Input Devices are found
6	Flash update is failed
7	Reset protocol is not available
8	Platform PCI resource requirements cannot be met (out of resource)

8.2.7 ACPI/ASL Checkpoint

Status Code	Description
0x01	System is entering S1 sleep state
0x02	System is entering S2 sleep state
0x03	System is entering S3 sleep state
0x04	System is entering S4 sleep state
0x05	System is entering S5 sleep state
0x10	System is waking up from the S1 sleep state
0x20	System is waking up from the S2 sleep state
0x30	System is waking up from the S3 sleep state
0x40	System is waking up from the S4 sleep state
0xAC	System has transitioned into ACPI mode. Interrupt controller is in PIC mode.
0xAA	System has transitioned into ACPI mode. Interrupt controller is in APIC mode.

8.3. OEM-Reserved Checkpoint Ranges

Status Code	Description
0x05	OEM SEC initialization before microcode loading
0x0A	OEM SEC initialization after microcode loading
0x1D – 0x2A	OEM pre-memory initialization codes
0x3F – 0x4E	OEM PEI post memory initialization codes
0x80 – 0x8F	OEM DXE initialization codes
0xC0 – 0xCF	OEM BDS initialization codes

9. Software Support

9.1. Windows Server 2019, Windows 10 IoT Enterprise LTSC

Windows Server 2022 is scheduled to be supported in Q4.

9.2. Yocto Linux

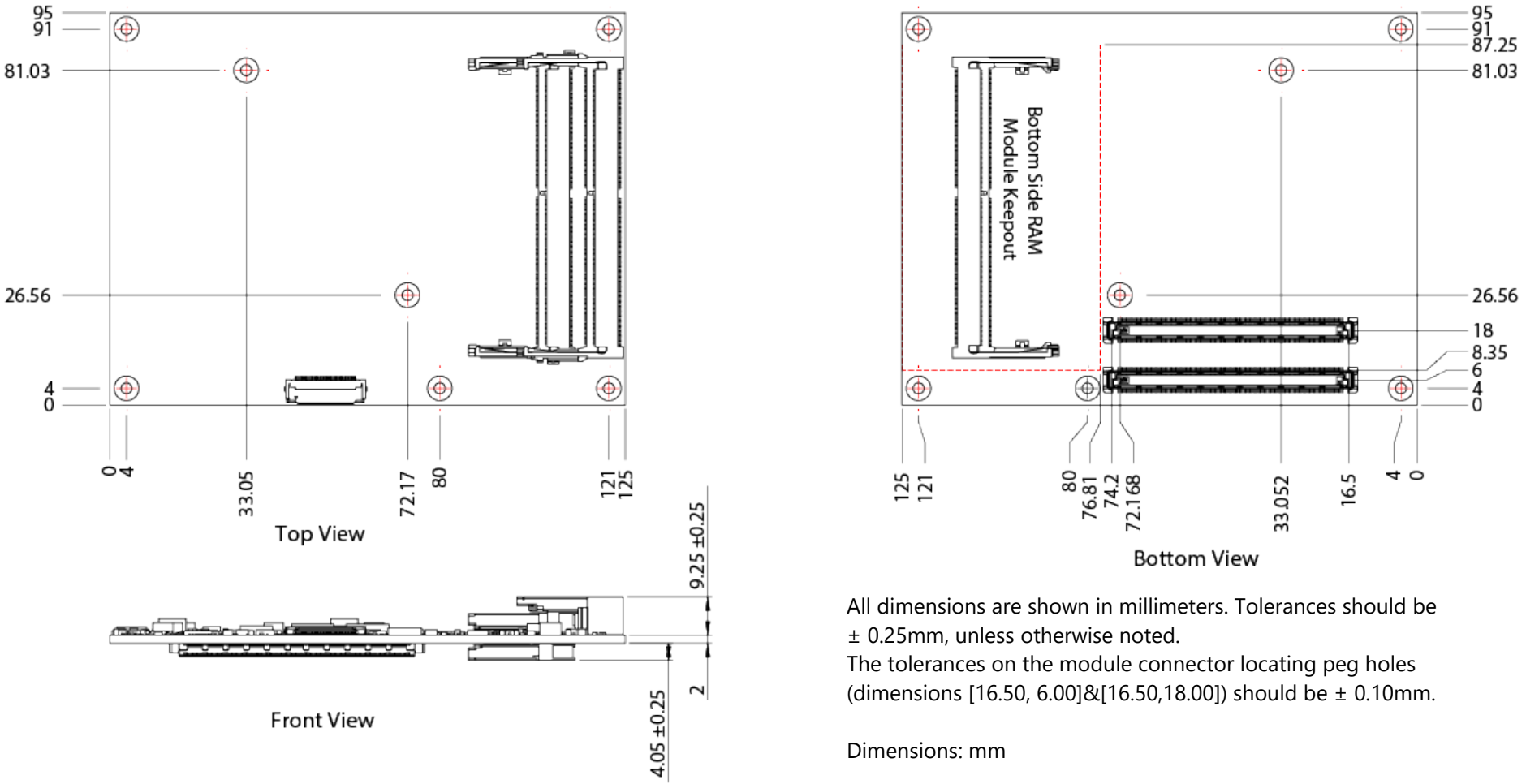
Yocto is scheduled to be supported in Q3

9.3. VxWorks

VxWorks is scheduled to be supported in Q3

10. Mechanical and Thermal

10.1. Module Dimensions



All dimensions are shown in millimeters. Tolerances should be ± 0.25mm, unless otherwise noted.
The tolerances on the module connector locating peg holes (dimensions [16.50, 6.00]&[16.50,18.00]) should be ± 0.10mm.

Dimensions: mm

Figure 5 – Module mechanical dimensions

10.2. Thermal Solutions

10.2.1 Heatspreader: HTS

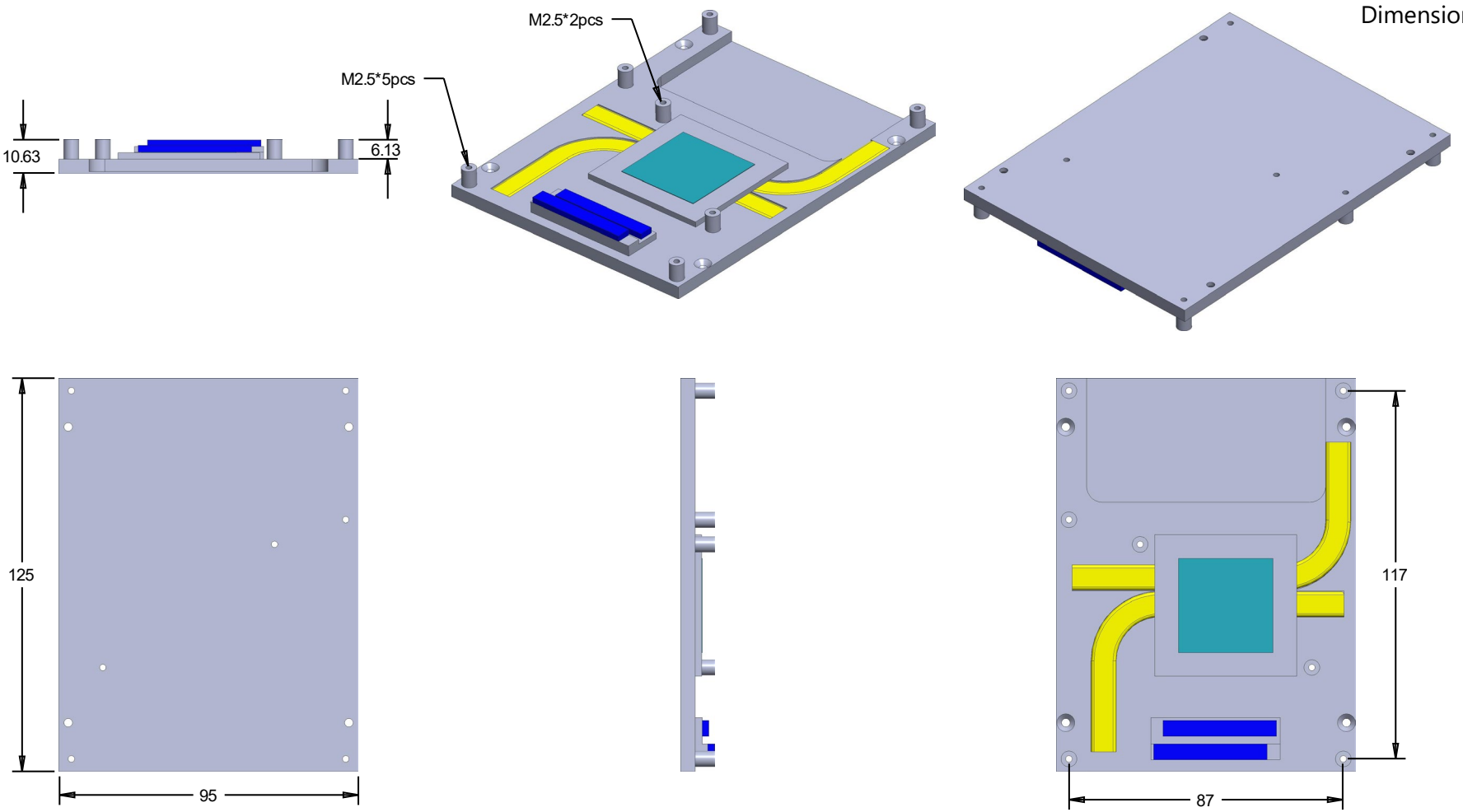


Figure 6 – Heatspreader HTS

10.2.2 Heatsink with Fan: THSF

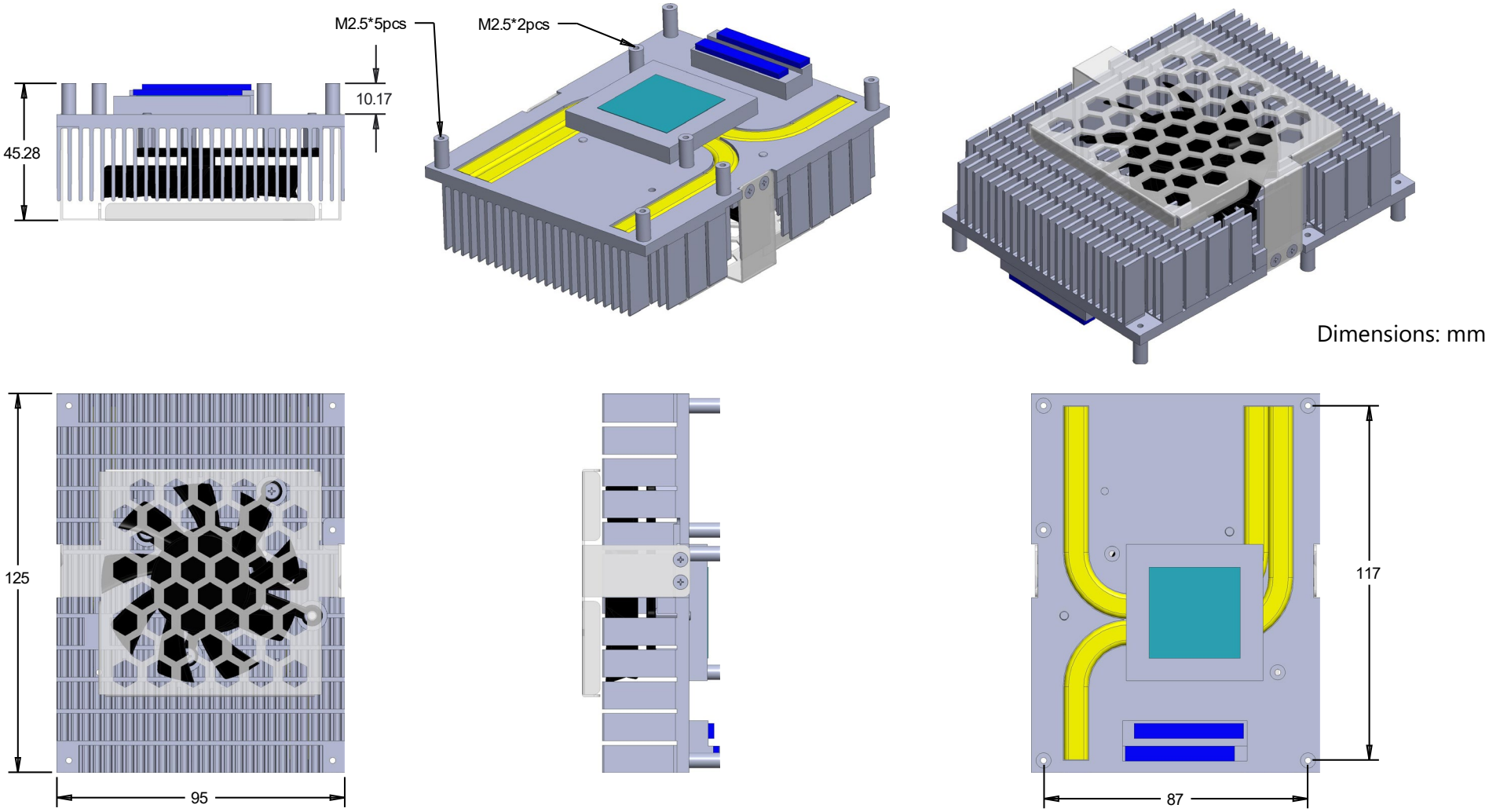


Figure 7 – Heatsink with Fan: THSF