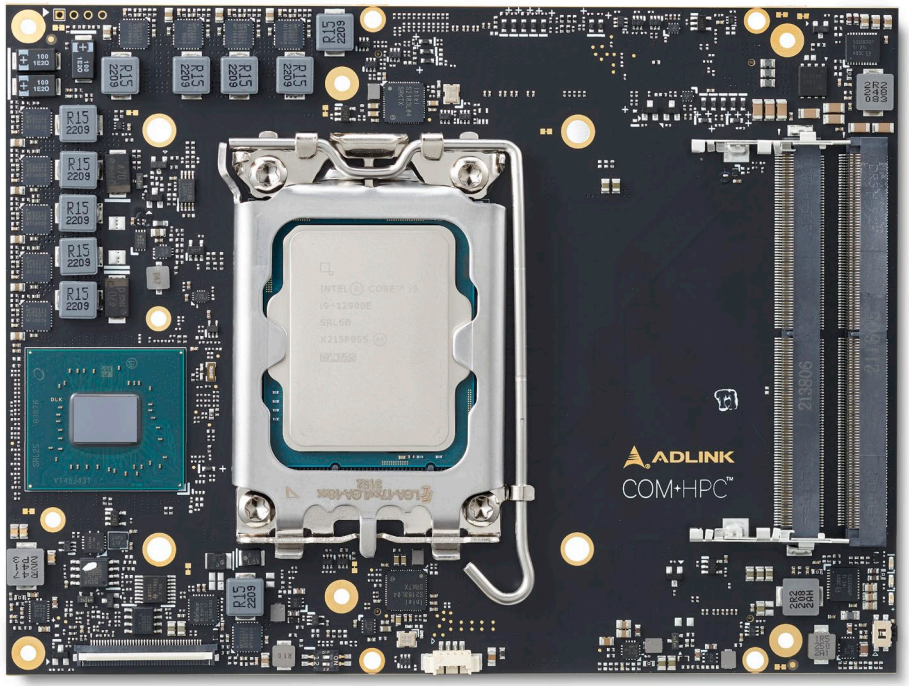
COM-HPC-cRLS

User's Guide

intel



COM-HPC™

Revision: Rev. 0.2
Date: 2024-01-11
Part Number: 50M-73301-1000

ADLINK
LEADING EDGE COMPUTING

Revision History

Revision	Description	Date	Author
0.1	Preliminary release	2023-12-26	CC
0.2	BIOS info added	2024-01-11	CC

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 COM-HPC-cRLS is a Client Type COM-HPC Size C module based on 13th Gen Intel® Core™ processors (formerly "Raptor Lake-S"). The processor offers up to 24 cores (8P-cores + 16 E-cores) at 5.2/4.2GHz boost frequency, and puts an emphasis on industrial-class reliability and longevity.

With Intel's hybrid architecture, the module fulfills the need of high-performance computing while maintaining low power portfolio, making it ideal for use cases including industrial automation and control, medical ultra sound, image processing and analysis, high-speed video encoding and streaming, predictive traffic analysis, multi-camera-based AI, and more.

Adding on, COM-HPC-cRLS features AVX2 VNNI (Vector Neural Network Instructions) that deliver accelerated AI inferencing performance and provides up to four DIMM sockets, supporting up to 128GB (4x 32GB) of DDR5 SORDIMM memory at a frequency of up to 4000 MT/s (dependent on memory configuration).

Selected SKUs feature industrial-class reliability with extended temperature range operability. Combined with ultra-low latency-focused Intel® Time Coordinated Computing (Intel® TCC) technology and an onboard 2.5Gigabit Ethernet port with optional Time Sensitive Network (TSN) support, COM-HPC-cRLS is well suited for mission critical, hard real-time, and rugged solutions.

Inputs/outputs provided include 1x PCIe Gen5 x16 lane, 1x PCIe Gen4 x4 lane (from CPU), also 3x PCIe Gen4 x4, 1x PCIe Gen3 x4, and 2x gen3 x1 lanes (from PCH), can be used for NVMe SSD, 2x PCIe lanes for onboard NASE-T controller (i226), 4x USB 3.0/2.0 ports, 2x SATA 6Gb/s ports, and 12x GPIO pins. TPM chip is equipped for security-related usage.

Support for SMBus and 2x I^2C is also available, and 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

13th Gen Core™ Processor (formerly "Raptor Lake-S")

Processor	Base Frequency	Turbo Frequency	Cache	Core/Thread	TDP
• i9-13900E	2.0/1.5GHz	5.2GHz/4.2GHz	36MB	24C(8P+16E)/32T	65W
• i7-13700E	1.9/1.3GHz	5.1GHz/3.9GHz	30MB	16C(8P+8E)/24T	65W
• i5-13500E,	2.4/1.5GHz	4.6GHz/3.3GHz	24MB	14C(6P+8E)/20T	65W
• i3-13100E,	3.3GHz	4.4GHz	12MB	4C(4P)/8T	65W

Note: 35W and 125W TDP SKUs are supported by project basis. Please consult our ADLINK local representative.

Memory

Up to 128GB (4x 32GB) DDR5 SODIMM in 4x DIMM sockets (ECC or non-ECC)

Up to 4000 MT/s in 4x sockets (2x on top, 2x at bottom), configured as:

- 2 DIMMs per channel 1R – 4000MT/s
- 2 DIMMs per channel 2R – 3600MT/s

Embedded BIOS

AMI UEFI with CMOS backup in 32MB SPI BIOS (dual BIOS by build option)

2.2 Expansion Buses

1x PCI Express x16 Gen5: Lanes 16-31 (configurable to 1 x16, 2 x8)

1x PCI Express x4 Gen4: Lanes 8-11 (configurable to 1 x4, 2 x2)

6x PCI Express x1 Gen3: Lanes 0-5 (configurable to 6 x1)

More lanes with R680E/ 670E (all x4, x2, x1):

1x PCI Express x4 Gen4: Lanes 12-15 (configurable to 1 x4, 2 x2, 4 x1)

1x PCI Express x4 Gen4: Lanes 32-35 (configurable to 1 x4, 2 x2, 4 x1)

1x PCI Express x4 Gen4: Lanes 36-39 (configurable to 1 x4, 2 x2, 4 x1)

Note: Gen5, Gen4 support dependent on carrier design.

4 PCI Express Reference Clock: (TBC)

2.3 Ethernet NBASE-T

2x NBASE-T ports

Onboard Intel® i226 series (IT version, TBC) Ethernet Controller

2.5Gbps, 1Gbps, and 100/10Mbps connections, 1000BASE-T mode support

IT version supports TSN on Linux OS, with NBASET0_SDP available when TSN support is enabled (TBC)

2.4 Multi I/O and Storage

USB

4x USB3.2/2.0/1.1 (USB 0, 1, 2, 3)

4x USB2.0/1.1 (USB 4, 5, 6, 7)

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

SATA

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

UART

2x UART on module

Console Redirection COM1 or COM2 selectable by BIOS

COM Port	Description	IRQ	Address	Console Redirection Support
COM0	Supported by module (UART 0), via embedded controller	4	0x3F8	Yes
COM1	Supported by module (UART 1), via embedded controller	5	0x2F8	Yes

GPIO

12x GPIO (GPI with interrupt, TBC)

2.5 Trusted Platform Module (TPM)

Chipset: Infineon solution

Type: TPM 2.0 (SPI bus based)

2.6 SEMA Board Controller

Supports Voltage/current monitoring, Power sequence debug support, Logistics and forensic information, General purpose I2C, Failsafe BIOS (dual BIOS, build, optional support), Watchdog timer, and Fan control

2.7 Debug

40-pin flat cable connector for DB40-HPC debug module

Supports BIOS POST code LED, SEMA Board Controller access, Module Management Controller access, SPI BIOS flashing, Internal power rail test points, and Debug LEDs

2.8 Power

Power Modes: AT, ATX (TBC)

Standard Voltage Input: AT: 12V±5%

Power Management: ACPI 5.0 compliant

Power States: S0, S5 (TBC)

2.9 Mechanical and Environmental

Form Factor and Specification

PICMG COM-HPC Revision 1.1, Client Type, Size C 160 x 120 mm

Operating Temperature

Standard	0°C to 60°C (Standard Voltage Input)	Storage: -20°C to 80°C

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

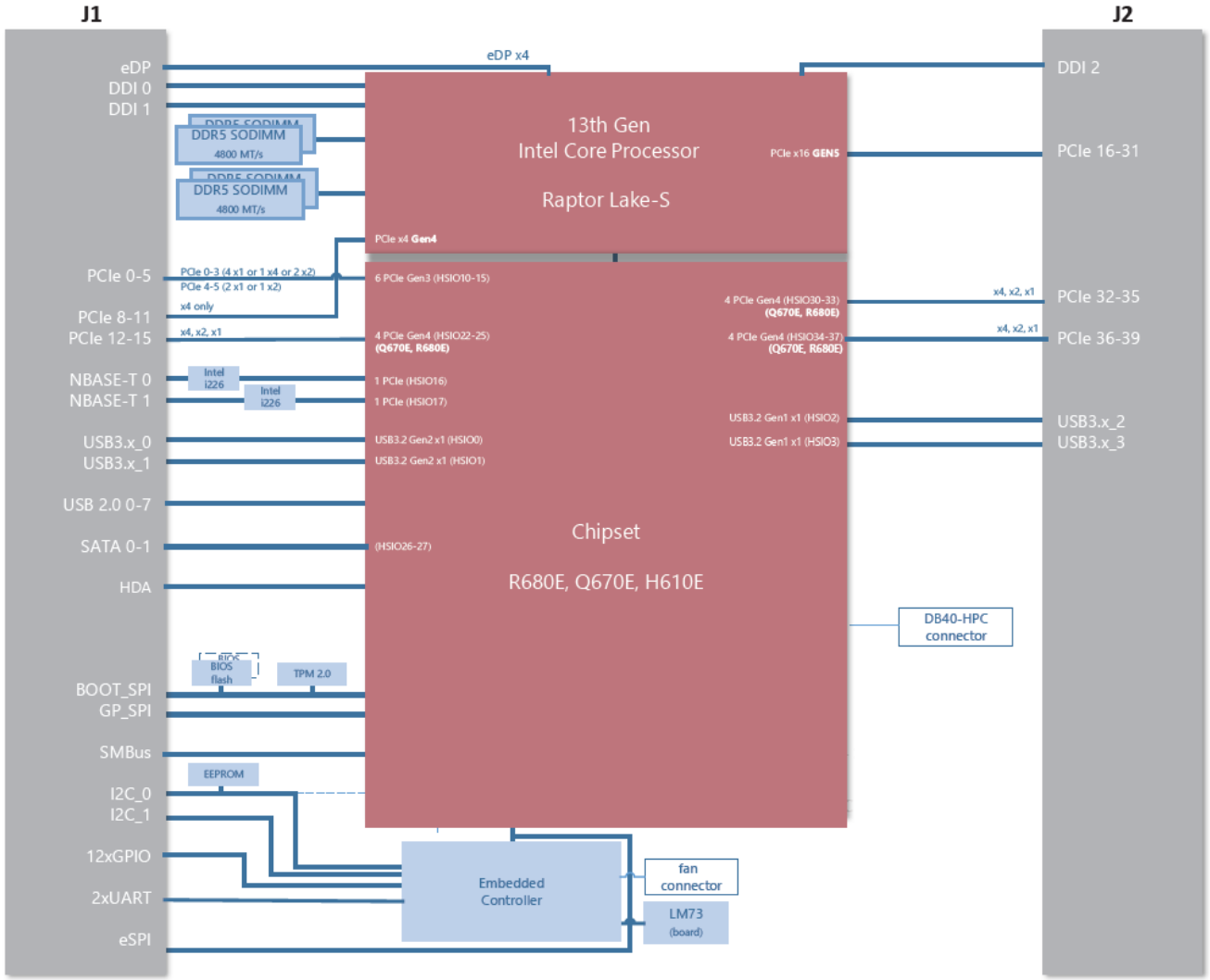


Figure 1 – Module function diagram

4. Pinout and Signal Descriptions

4.1 Pin Summary

The table below is a comprehensive list of all signal pins supported on the dual 400-pin COM-HPC connectors as defined for Client Type in the PICMG COM-HPC R1.1 specification. Signals described in the specification but not supported on the COM-HPC-cRLS are marked by ~~STRIKETHROUGH.~~

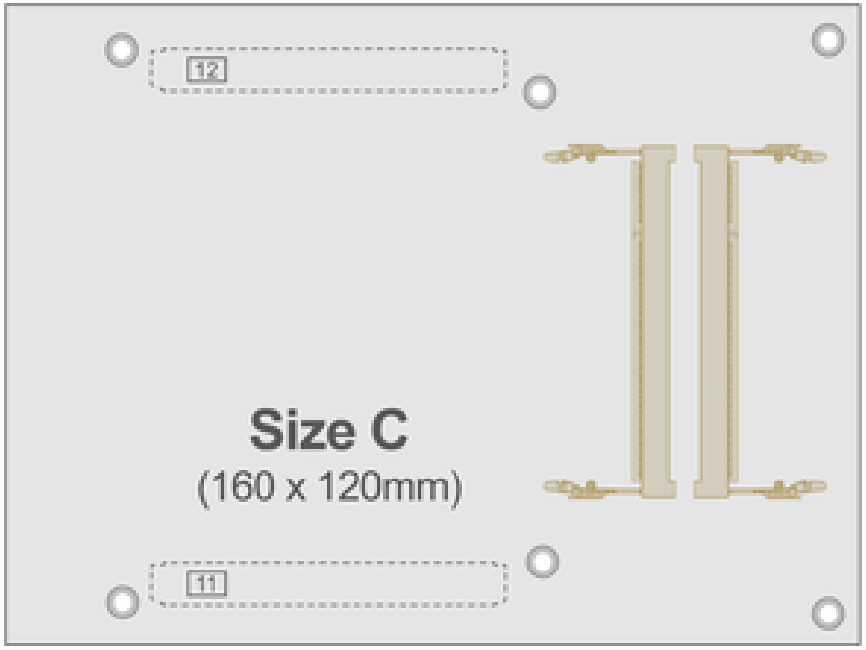


Figure 2 - Module rear side row and pin numbering

Row A			Row B			Row C			Row D	
A1	VCC		B1	VCC		C1	VCC		D1	VCC
A2	VCC		B2	PWRBTN#		C2	RSTBTN#		D2	VCC
A3	VCC		B3	VCC		C3	VCC		D3	VCC
A4	VCC		B4	THERMTRIP#		C4	CARRIER_HOT#		D4	VCC
A5	VCC		B5	VCC		C5	VCC		D5	VCC
A6	VCC		B6	TAMPER#		C6	VIN_PWR_OK		D6	VCC
A7	VCC		B7	VCC		C7	VCC		D7	VCC
A8	VCC		B8	SUS_S3#		C8	SUS_S4_S5#		D8	VCC
A9	VCC		B9	VCC		C9	VCC		D9	VCC
A10	GND		B10	WD_STROBE#		C10	GND		D10	WAKE0#
A11	BATLOW#		B11	WD_OUT		C11	FAN_PWMOUT		D11	WAKE1#
A12	PLTRST#		B12	GND		C12	FAN_TACHIN		D12	GND
A13	GND		B13	USB5-		C13	GND		D13	USB1-
A14	USB7-		B14	USB5+		C14	USB3-		D14	USB1+
A15	USB7+		B15	GND		C15	USB3+		D15	GND
A16	GND		B16	USB4-		C16	GND		D16	USB0-
A17	USB6-		B17	USB4+		C17	USB2-		D17	USB0+
A18	USB6+		B18	GND		C18	USB2+		D18	GND
A19	GND		B19	I2S_LRCLK/SNDW_CLK3/HDA_SYNC		C19	GND		D19	DDI0_SDA_AUX-
A20	DDI_SDA_AUX-		B20	I2S_DOUT/SNDW_DAT3/HDA_SDO		C20	SNDW_DMIC_CLK1		D20	DDI0_SCL_AUX+
A21	DDI_SCL_AUX+		B21	I2S_MCLK/HDA_RST#		C21	SNDW_DMIC_DAT1		D21	GND
A22	GND		B22	I2S_DIN/SNDW_DAT2/HDA_SDI		C22	GND		D22	DDI0_PAIR0-
A23	DDI_PAIR0-		B23	I2S_CLK/SNDW_CLK2/HDA_BCLK		C23	SNDW_DMIC_CLK0		D23	DDI0_PAIR0+
A24	DDI_PAIR0+		B24	VCC_5V_SBY		C24	SNDW_DMIC_DAT0		D24	GND
A25	GND		B25	USB67_OC#		C25	GND		D25	DDI0_PAIR1-
A26	DDI_PAIR1-		B26	USB45_OC#		C26	DDI0_DDC_AUX_SEL		D26	DDI0_PAIR1+
A27	DDI_PAIR1+		B27	USB23_OC#		C27	DDI1_DDC_AUX_SEL		D27	GND
A28	GND		B28	USB01_OC#		C28	DDI0_HPD		D28	DDI0_PAIR2-
A29	DDI_PAIR2-		B29	SML1_CLK		C29	DDI1_HPD		D29	DDI0_PAIR2+
A30	DDI_PAIR2+		B30	SML1_DAT		C30	eDP_HPD		D30	GND
A31	GND		B31	PMCALERT#		C31	eDP_VDD_EN		D31	DDI0_PAIR3-
A32	DDI_PAIR3-		B32	SML0_CLK		C32	eDP_BKLT_EN		D32	DDI0_PAIR3+
A33	DDI_PAIR3+		B33	SML0_DAT		C33	eDP_BKLTCTL		D33	GND
A34	GND		B34	USB_PD_ALERT#		C34	GND		D34	AC_PRESENT
A35	eDP_AUX-		B35	USB_PD_I2C_CLK		C35	USB1_AUX-		D35	RSVD
A36	eDP_AUX+		B36	USB_PD_I2C_DAT		C36	USB1_AUX+		D36	GND

Row A			Row B			Row C			Row D	
A37	GND		B37	USB_RT_ENA		C37	GND		D37	USB1_SSTX0-
A38	eDP_TX0-		B38	USB1_LSRX		C38	USB1_SSRX0-		D38	USB1_SSTX0+
A39	eDP_TX0+		B39	USB1_LSTX		C39	USB1_SSRX0+		D39	GND
A40	GND		B40	USB0_LSRX		C40	GND		D40	USB1_SSTX1-
A41	eDP_TX1-		B41	USB0_LSTX		C41	USB1_SSRX1-		D41	USB1_SSTX1+
A42	eDP_TX1+		B42	GND		C42	USB1_SSRX1+		D42	GND
A43	GND		B43	USB0_AUX-		C43	GND		D43	USB0_SSTX0-
A44	eDP_TX2-		B44	USB0_AUX+		C44	USB0_SSRX0-		D44	USB0_SSTX0+
A45	eDP_TX2+		B45	LID#		C45	USB0_SSRX0+		D45	GND
A46	GND		B46	SLEEP#		C46	GND		D46	USB0_SSTX1-
A47	eDP_TX3-		B47	VCC_BOOT_SPI		C47	USB0_SSRX1-		D47	USB0_SSTX1+
A48	eDP_TX3+		B48	BOOT_SPI_CS#		C48	USB0_SSRX1+		D48	GND
A49	GND		B49	BSEL0		C49	GND		D49	SATA0_RX- *
A50	eSPI_IO0		B50	BSEL1		C50	BOOT_SPI_IO0		D50	SATA0_RX+ *
A51	eSPI_IO1		B51	BSEL2		C51	BOOT_SPI_IO1		D51	GND
A52	eSPI_IO2		B52	eSPI_ALERT0#		C52	BOOT_SPI_IO2		D52	SATA0_TX- *
A53	eSPI_IO3		B53	eSPI_ALERT1#		C53	BOOT_SPI_IO3		D53	SATA0_TX+ *
A54	eSPI_CLK		B54	eSPI_CS0#		C54	BOOT_SPI_CLK		D54	GND
A55	GND		B55	eSPI_CS1#		C55	GND		D55	SATA1_RX- *
A56	PCIe_CLKREQ0_LO#		B56	eSPI_RST#		C56	PCIe_REFCLK0_HI-		D56	SATA1_RX+*
A57	PCIe_CLKREQ0_HI#		B57	GND		C57	PCIe_REFCLK0_HI+		D57	GND
A58	GND		B58	PCIe_BMC_RX-		C58	GND		D58	SATA1_TX- *
A59	PCIe_BMC_TX-		B59	PCIe_BMC_RX+		C59	PCIe_REFCLK0_LO-		D59	SATA1_TX+*
A60	PCIe_BMC_TX+		B60	GND		C60	PCIe_REFCLK0_LO+		D60	GND
A61	GND		B61	PCIe08_RX-		C61	GND		D61	PCIe00_TX-
A62	PCIe08_TX-		B62	PCIe08_RX+		C62	PCIe00_RX-		D62	PCIe00_TX+
A63	PCIe08_TX+		B63	GND		C63	PCIe00_RX+		D63	GND
A64	GND		B64	PCIe09_RX-		C64	GND		D64	PCIe01_TX-
A65	PCIe09_TX-		B65	PCIe09_RX+		C65	PCIe01_RX-		D65	PCIe01_TX+
A66	PCIe09_TX+		B66	GND		C66	PCIe01_RX+		D66	GND
A67	GND		B67	PCIe10_RX-		C67	GND		D67	PCIe02_TX-
A68	PCIe10_TX-		B68	PCIe10_RX+		C68	PCIe02_RX-		D68	PCIe02_TX+
A69	PCIe10_TX+		B69	GND		C69	PCIe02_RX+		D69	GND
A70	GND		B70	PCIe11_RX-		C70	GND		D70	PCIe03_TX-
A71	PCIe11_TX-		B71	PCIe11_RX+		C71	PCIe03_RX-		D71	PCIe03_TX+
A72	PCIe11_TX+		B72	GND		C72	PCIe03_RX+		D72	GND

Row A			Row B			Row C			Row D	
A73	GND		B73	PCIe12_RX-		C73	GND		D73	PCIe04_TX-
A74	PCIe12_TX-		B74	PCIe12_RX+		C74	PCIe04_RX-		D74	PCIe04_TX+
A75	PCIe12_TX+		B75	GND		C75	PCIe04_RX+		D75	GND
A76	GND		B76	PCIe13_RX-		C76	GND		D76	PCIe05_TX-
A77	PCIe13_TX-		B77	PCIe13_RX+		C77	PCIe05_RX-		D77	PCIe05_TX+
A78	PCIe13_TX+		B78	GND		C78	PCIe05_RX+		D78	GND
A79	GND		B79	PCIe14_RX-		C79	GND		D79	~~PCIe06_TX-~~
A80	PCIe14_TX-		B80	PCIe14_RX+		C80	~~PCIe06_RX-~~		D80	~~PCIe06_TX+~~
A81	PCIe14_TX+		B81	GND		C81	~~PCIe06_RX+~~		D81	GND
A82	GND		B82	PCIe15_RX-		C82	GND		D82	~~PCIe07_TX-~~
A83	PCIe15_TX-		B83	PCIe15_RX+		C83	~~PCIe07_RX-~~		D83	~~PCIe07_TX+~~
A84	PCIe15_TX+		B84	GND		C84	~~PCIe07_RX+~~		D84	GND
A85	GND		B85	TEST#		C85	GND		D85	NBASET0_MDI0-
A86	VCC_RTC		B86	RSMRST_OUT#		C86	SMB_CLK		D86	NBASET0_MDI0+
A87	SUS_CLK		B87	UART1_TX		C87	SMB_DAT		D87	GND
A88	GPIO_00		B88	UART1_RX		C88	SMB_ALERT#		D88	NBASET0_MDI1-
A89	GPIO_01		B89	UART1_RTS#		C89	UART0_TX		D89	NBASET0_MDI1+
A90	GPIO_02		B90	UART1_CTS#		C90	UART0_RX		D90	GND
A91	GPIO_03		B91	~~IPMB_CLK~~		C91	UART0_RTS#		D91	NBASET0_MDI2-
A92	GPIO_04		B92	~~IPMB_DAT~~		C92	UART0_CTS#		D92	NBASET0_MDI2+
A93	GPIO_05		B93	~~GPSPI_MOSI~~		C93	I2C0_CLK		D93	GND
A94	GPIO_06		B94	~~GPSPI_MISO~~		C94	I2C0_DAT		D94	NBASET0_MDI3-
A95	GPIO_07		B95	~~GPSPI_CS0#~~		C95	I2C0_ALERT#		D95	NBASET0_MDI3+
A96	GPIO_08		B96	~~GPSPI_CS1#~~		C96	I2C1_CLK		D96	GND
A97	GPIO_09		B97	~~GPSPI_CS2#~~		C97	I2C1_DAT		D97	NBASET0_LINK_MAX#
A98	GPIO_10		B98	~~GPSPI_CS3#~~		C98	NBASET0_SDP *		D98	NBASET0_LINK_MID#
A99	GPIO_11		B99	~~GPSPI_CLK~~		C99	NBASET0_CTREF		D99	NBASET0_LINK_ACT#
A100	TYPE0		B100	~~GPSPI_ALERT#~~		C100	TYPE1		D100	TYPE2

Row E			Row F			Row G			Row H	
E1	RAPID_SHUTDOWN		F1	FUSA_STATUS0		G1	VCC_5V_SBY		H1	GND
E2	GND		F2	FUSA_STATUS1		G2	GND		H2	USB2_SSTX0-
E3	RSVD		F3	FUSA_ALERT#		G3	USB2_SSRX0-		H3	USB2_SSTX0+
E4	RSVD		F4	FUSA_SPI_CS#		G4	USB2_SSRX0+		H4	GND
E5	GND		F5	FUSA_SPI_CLK		G5	GND		H5	USB2-SSTX1-
E6	RSVD		F6	FUSA_SPI_MISO		G6	USB2_SSRX1-		H6	USB2-SSTX1+
E7	RSVD		F7	FUSA_SPI_MOSI		G7	USB2_SSRX1+		H7	GND
E8	GND		F8	FUSA_SPI_ALERT		G8	GND		H8	USB3_SSTX0-
E9	RSVD		F9	FUSA_VOLTAGE_ERR#		G9	USB3_SSRX0-		H9	USB3_SSTX0+
E10	RSVD		F10	PROCHOT#		G10	USB3_SSRX0+		H10	GND
E11	GND		F11	CATERR#		G11	GND		H11	USB3-SSTX1-
E12	RSVD		F12	RSVD		G12	USB3_SSRX1-		H12	USB3-SSTX1+
E13	RSVD		F13	RSVD		G13	USB3_SSRX1+		H13	GND
E14	GND		F14	RSVD		G14	GND		H14	USB2_AUX-
E15	RSVD		F15	RSVD		G15	USB3_LSRX		H15	USB2_AUX+
E16	RSVD		F16	RSVD		G16	USB3_LSTX		H16	GND
E17	GND		F17	RSVD		G17	USB3_LSRX		H17	USB3_AUX-
E18	RSVD		F18	RSVD		G18	USB3_LSTX		H18	USB3_AUX+
E19	RSVD		F19	GND		G19	PEG_LANE_REV#		H19	GND
E20	GND		F20	PCIe32_RX-		G20	GND		H20	PCIe40_TX-
E21	PCIe32_TX-		F21	PCIe32_RX+		G21	PCIe40_RX-		H21	PCIe40_TX+
E22	PCIe32_TX+		F22	GND		G22	PCIe40_RX+		H22	GND
E23	GND		F23	PCIe33_RX-		G23	GND		H23	PCIe41_TX-
E24	PCIe33_TX-		F24	PCIe33_RX+		G24	PCIe41_RX-		H24	PCIe41_TX+
E25	PCIe33_TX+		F25	GND		G25	PCIe41_RX+		H25	GND
E26	GND		F26	PCIe34_RX-		G26	GND		H26	PCIe42_TX-
E27	PCIe34_TX-		F27	PCIe34_RX+		G27	PCIe42_RX-		H27	PCIe42_TX+
E28	PCIe34_TX+		F28	GND		G28	PCIe42_RX+		H28	GND
E29	GND		F29	PCIe35_RX-		G29	GND		H29	PCIe43_TX-
E30	PCIe35_TX-		F30	PCIe35_RX+		G30	PCIe43_RX-		H30	PCIe43_TX+
E31	PCIe35_TX+		F31	GND		G31	PCIe43_RX+		H31	GND
E32	GND		F32	PCIe36_RX-		G32	GND		H32	PCIe44_TX-
E33	PCIe36_TX-		F33	PCIe36_RX+		G33	PCIe44_RX-		H33	PCIe44_TX+
E34	PCIe36_TX+		F34	GND		G34	PCIe44_RX+		H34	GND
E35	GND		F35	PCIe37_RX-		G35	GND		H35	PCIe45_TX-
E36	PCIe37_TX-		F36	PCIe37_RX+		G36	PCIe45_RX-		H36	PCIe45_TX+

Row E			Row F			Row G			Row H	
E37	PCIe37_TX+		F37	GND		G37	PCIe45_RX+		H37	GND
E38	GND		F38	PCIe38_RX-		G38	GND		H38	PCIe46_TX-
E39	PCIe38_TX-		F39	PCIe38_RX+		G39	PCIe46_RX-		H39	PCIe46_TX+
E40	PCIe38_TX+		F40	GND		G40	PCIe46_RX+		H40	GND
E41	GND		F41	PCIe39_RX-		G41	GND		H41	PCIe47_TX-
E42	PCIe39_TX-		F42	PCIe39_RX+		G42	PCIe47_RX-		H42	PCIe47_TX+
E43	PCIe39_TX+		F43	GND		G43	PCIe47_RX+		H43	GND
E44	GND		F44	PCIe16_RX-		G44	GND		H44	PCIe24_TX-
E45	PCIe16_TX-		F45	PCIe16_RX+		G45	PCIe24_RX-		H45	PCIe24_TX+
E46	PCIe16_TX+		F46	GND		G46	PCIe24_RX+		H46	GND
E47	GND		F47	PCIe17_RX-		G47	GND		H47	PCIe25_TX-
E48	PCIe17_TX-		F48	PCIe17_RX+		G48	PCIe25_RX-		H48	PCIe25_TX+
E49	PCIe17_TX+		F49	GND		G49	PCIe25_RX+		H49	GND
E50	GND		F50	PCIe18_RX-		G50	GND		H50	PCIe26_TX-
E51	PCIe18_TX-		F51	PCIe18_RX+		G51	PCIe26_RX-		H51	PCIe26_TX+
E52	PCIe18_TX+		F52	GND		G52	PCIe26_RX+		H52	GND
E53	GND		F53	PCIe19_RX-		G53	GND		H53	PCIe27_TX-
E54	PCIe19_TX-		F54	PCIe19_RX+		G54	PCIe27_RX-		H54	PCIe27_TX+
E55	PCIe19_TX+		F55	GND		G55	PCIe27_RX+		H55	GND
E56	GND		F56	PCIe20_RX-		G56	GND		H56	PCIe28_TX-
E57	PCIe20_TX-		F57	PCIe20_RX+		G57	PCIe28_RX-		H57	PCIe28_TX+
E58	PCIe20_TX+		F58	GND		G58	PCIe28_RX+		H58	GND
E59	GND		F59	PCIe21_RX-		G59	GND		H59	PCIe29_TX-
E60	PCIe21_TX-		F60	PCIe21_RX+		G60	PCIe29_RX-		H60	PCIe29_TX+
E61	PCIe21_TX+		F61	GND		G61	PCIe29_RX+		H61	GND
E62	GND		F62	PCIe22_RX-		G62	GND		H62	PCIe30_TX-
E63	PCIe22_TX-		F63	PCIe22_RX+		G63	PCIe30_RX-		H63	PCIe30_TX+
E64	PCIe22_TX+		F64	GND		G64	PCIe30_RX+		H64	GND
E65	GND		F65	PCIe23_RX-		G65	GND		H65	PCIe31_TX-
E66	PCIe23_TX-		F66	PCIe23_RX+		G66	PCIe31_RX-		H66	PCIe31_TX+
E67	PCIe23_TX+		F67	GND		G67	PCIe31_RX+		H67	GND
E68	GND		F68	RSVD		G68	GND		H68	RSVD
E69	RSVD		F69	RSVD		G69	RSVD		H69	RSVD
E70	RSVD		F70	GND		G70	RSVD		H70	GND
E71	RSVD		F71	NBASET1_MDI0-		G71	GND		H71	CSI1_RX0-
E72	RSVD		F72	NBASET1_MDI0+		G72	CSI0_RX0-		H72	CSI1_RX0+

Row E			Row F			Row G			Row H	
E73	RSVD		F73	GND		G73	CSI0_RX0+		H73	GND
E74	RSVD		F74	NBASET1_MDI1-		G74	GND		H74	CSI1_RX1-
E75	RSVD		F75	NBASET1_MDI1+		G75	CSI0_RX1-		H75	CSI1_RX1+
E76	RSVD		F76	GND		G76	CSI0_RX1+		H76	GND
E77	RSVD		F77	NBASET1_MDI2-		G77	GND		H77	CSI1_RX2-
E78	NBASET1_CTREF		F78	NBASET1_MDI2+		G78	CSI0_RX2-		H78	CSI1_RX2+
E79	NBASET1_SDP		F79	GND		G79	CSI0_RX2+		H79	GND
E80	NBASET1_LINK_MID#		F80	NBASET1_MDI3-		G80	GND		H80	CSI1_RX3-
E81	NBASET1_LINK_ACT#		F81	NBASET1_MDI3+		G81	CSI0_RX3-		H81	CSI1_RX3+
E82	NBASET1_LINK_MAX#		F82	GND		G82	CSI0_RX3+		H82	GND
E83	GND		F83	RSVD		G83	GND		H83	CSI1_CLK-
E84	RSVD		F84	RSVD		G84	CSI0_CLK-		H84	CSI1_CLK+
E85	RSVD		F85	GND		G85	CSI0_CLK+		H85	GND
E86	GND		F86	ETH0_TX-		G86	GND		H86	CSI1_I2C_CLK
E87	ETH0_RX-		F87	ETH0_TX+		G87	CSI0_I2C_CLK		H87	CSI1_I2C_DAT
E88	ETH0_RX+		F88	GND		G88	CSI0_I2C_DAT		H88	CSI1_MCLK
E89	GND		F89	ETH1_TX-		G89	CSI0_MCLK		H89	CSI1_RST#
E90	ETH1_RX-		F90	ETH1_TX+		G90	CSI0_RST#		H90	CSI1_ENA
E91	ETH1_RX+		F91	GND		G91	CSI0_ENA		H91	GND
E92	GND		F92	PCIe_REFCLK2-		G92	GND		H92	PCIe_REFCLKIN0-
E93	PCIe_REFCLK1-		F93	PCIe_REFCLK2+		G93	RSVD		H93	PCIe_REFCLKIN0+
E94	PCIe_REFCLK1+		F94	GND		G94	RSVD		H94	GND
E95	GND		F95	RSVD		G95	GND		H95	PCIe_REFCLKIN1-
E96	PCIe_CLKREQ1#		F96	ETH0-1_PRSNT#		G96	ETH0-1_I2C_CLK		H96	PCIe_REFCLKIN1+
E97	PCIe_CLKREQ2#		F97	ETH0-1_PHY_RST#		G97	ETH0-1_I2C_DAT		H97	GND
E98	PCIe_CLKREQ_OUT0#		F98	ETH0_SDP		G98	ETH0-1_PHY_INT#		H98	ETH0-1_MDIO_CLK
E99	PCIe_CLKREQ_OUT1#		F99	ETH1_SDP		G99	ETH0-1_INT#		H99	ETH0-1_MDIO_DAT
E100	PCIe_PERST_IN0#		F100	PCIe_PERST_IN1#		G100	PCIe_WAKE_OUT0#		H100	PCIe_WAKE_OUT1#

Note: NBASET0_SDP is dependent on LAN controller SKU.

4.2 Signal Terminology Descriptions

Meaning of the terms used in 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

5. Additional Features

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

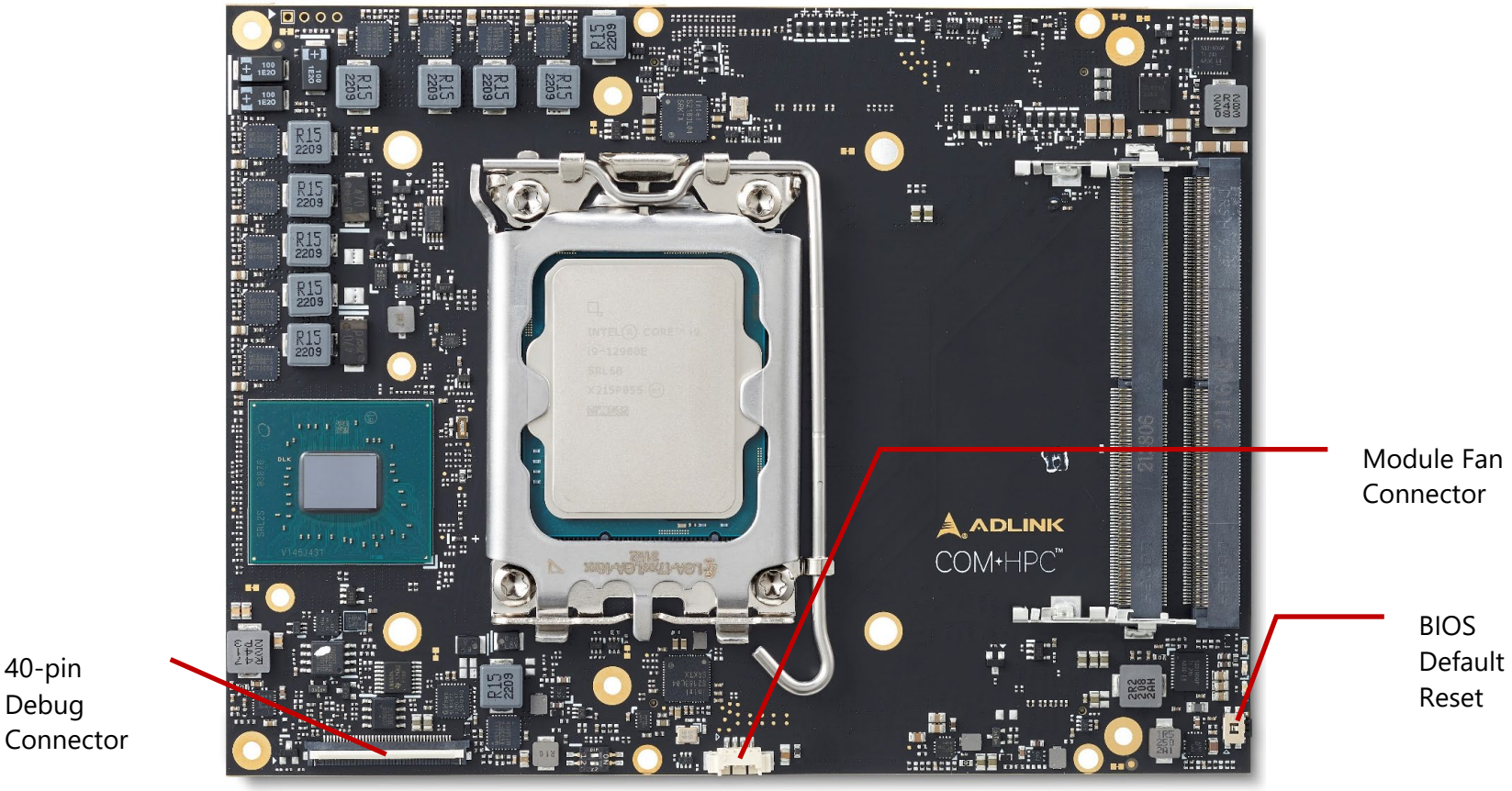


Figure 3 – Module feature locations (front)

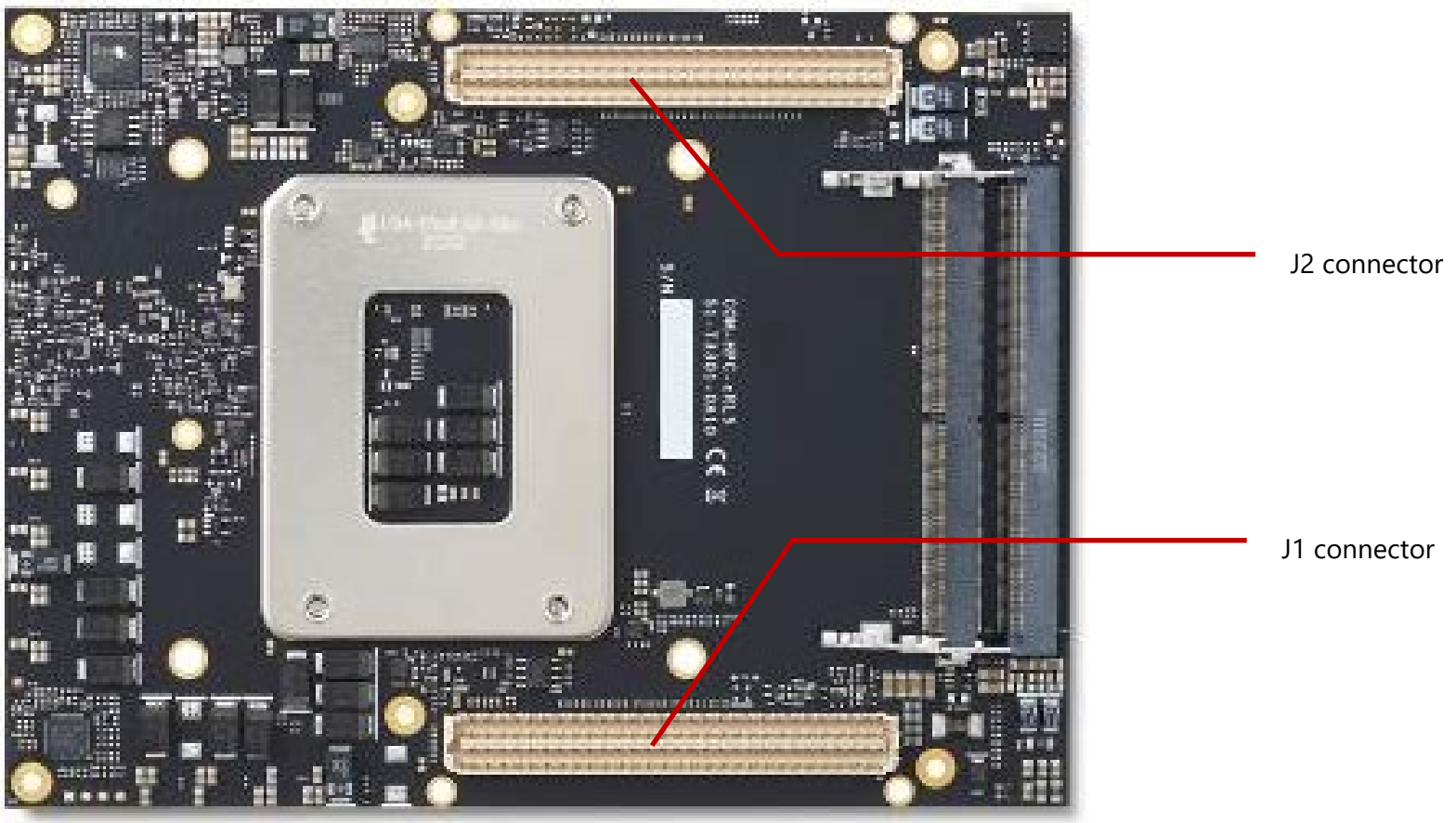
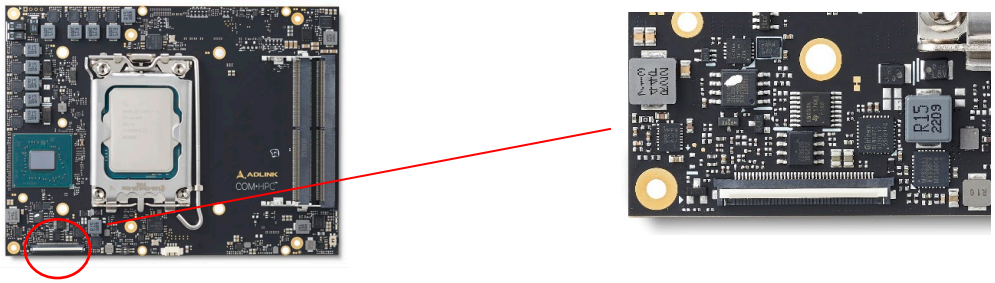


Figure 4 – Module feature locations (back)

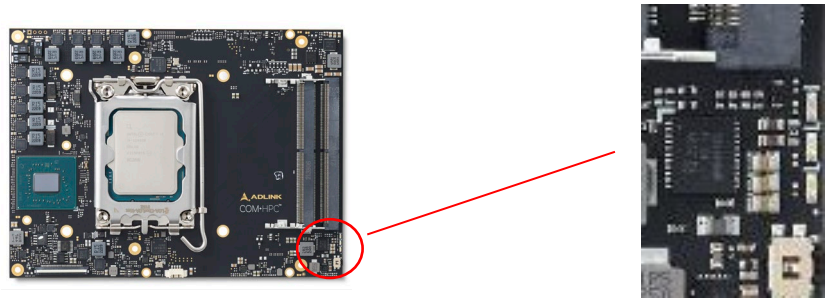
5.1 Debug Connector (40-pin connector)



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 for measurement of internal power rails
- SPI BIOS programming interface
- I2C bus for BIOS POST code readout
- Module EC and MMC programming interface

5.2 Status LEDs



Status LEDs are mounted on the module as illustrated above.

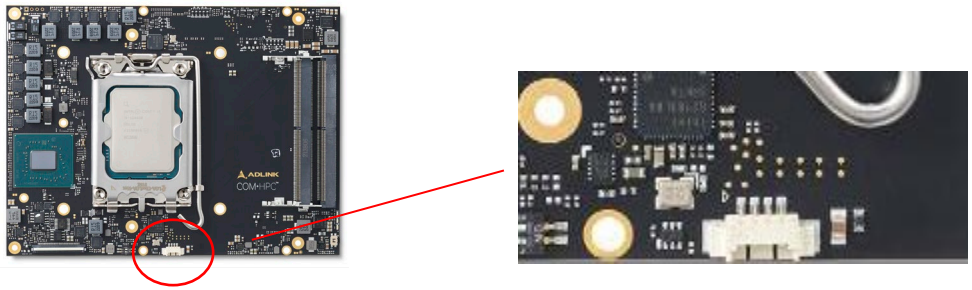
LED behavior are described in the table below.

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 B-to-B 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 by power button WD LED = LED OFF Rebooted by reset button 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
3	NO_SLP_S5
4	NO_SLP_S4
5	NO_SLP_S3
6	BIOS_FAIL
7	RESET_FAIL
9	NO_CB_PWROK
10	CRITICAL_TEMP
11	POWER_FAIL
12	VOLTAGE_FAIL
13	RSMRST_FAIL
14	NO_VDDQ_PG
16	NO_VCORE_PG
17	NO_SYS_GD
19	NO_V3P3A
21	NO_PWRSRC_GD
24	NO_PCH_PG

5.4 Fan Connector

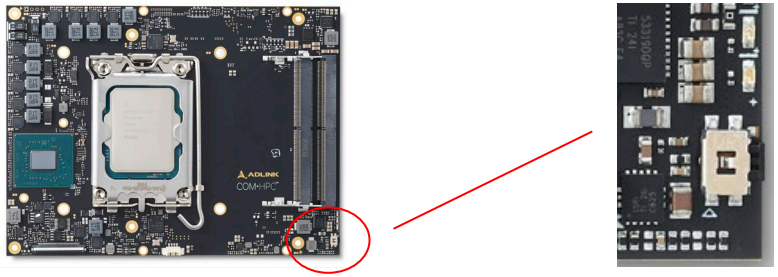


Connector Type: JVE 24W1125A-04M00

Name	Description
1	FAN_PWMOUT
2	FAN_TACHIN
3	GND
4	12V*

The supply voltage and maximum current of the fan connector is dependent on the module's input voltage (VCC_12V pins).

5.5 BIOS Default Reset



To perform a hardware reset to revert BIOS settings back to default, follow the steps below.

1. Shut down the system.
2. Press and hold the BIOS Setup Default Reset Button and boot up the system. Release the button when the BIOS prompt screen appears.
3. Once BIOS settings are reset to default, you will be asked to reboot the system.

5.6 BIOS Boot Select

The module has two BIOS chips (BOM option), allowing you to configure its BIOS operation to "PICMG" and/or "dual-BIOS"Failsafe" modes using the 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, TBC)	-	On
Set BIOS to Failsafe BIOS mode	-	Off

6. System Resources

6.1 System Memory Map

Address Range (hex)	Description
7FFFF00000-7FFFFFFFFF	High Definition Audio Controller
7FFFEFC000-7FFFEFFFFF	High Definition Audio Controller
7FFFEFB000-7FFFEFBFFF	Intel® GNA Scoring Accelerator module
7FFFEFA000-7FFFEFAFFF	Intel® Serial IO I2C Host Controller – 7AAB
7FFFEF9000-7FFFEF9FFF	Intel® Serial IO I2C Host Controller – 7ACC
7FFFEF8000-7FFFEF8FFF	Intel® Serial IO I2C Host Controller – 7ACD
7FFFEF7000-7FFFEF7FFF	Intel® Serial IO I2C Host Controller – 7ACE
7FFFEF6000-7FFFEF6FFF	Intel® Serial IO I2C Host Controller – 7ACF
7FFFEF5000-7FFFEF5FFF	Intel® Management Engine Interface
7FFFEF4000-7FFFEF4FFF	Intel® Serial IO I2C Host Controller – 7AFC
7FFFEF3000-7FFFEF3FFF	Intel® Serial IO I2C Host Controller – 7AFD
7FFFEF2000-7FFFEF2FFF	Intel® Serial IO UART Host Controller – 7AA8
7FFFEC0000-7FFFEDFFFF	Intel® Innovation Platform Framework Processor Participant
4000000000-400FFFFFFF	Intel® UHD Graphics 770
FED20000-FED7FFFF FED45000-FED8FFFF FED90000-FED93FFF FEDA0000-FEDA0FFF FEDA1000-FEDA1FFF FEDC0000-FEDC7FFF	Motherboard resource

Address Range (hex)	Description
FEE00000-FEEFFFFF	
FED00000-FED003FF	High precision event timer
FE010000-FE010FFF	Intel® SPI (flash) Controller - 7AA4
E0690000-E069FFFF E06A0000-E06AFFFF E06B0000-E06BFFFF E06D0000-E06DFFFF E06E0000-E06EFFFF	Intel® Serial IO GPIO Host Controller – INT1056
C0000000-CFFFFFFF	Motherboard resources
80400000-BFFFFFFF	PCI Express Root Complex
000F0000-000FFFFF	PCI Express Root Complex
000EC000-000EFFFF	PCI Express Root Complex
000E8000-000EBFFF	PCI Express Root Complex
000E4000-000E7FFF	PCI Express Root Complex
000E0000-000E3FFF	PCI Express Root Complex
000A0000-000BFFFF	PCI Express Root Complex

6.2 I/O Map

Hex Range	Device
00h - CF7h	PCI Express Root Complex
20h - 2Dh	Programmable interrupt controller
2Eh - 2Fh	Motherboard resources
30h - 3Dh	Programmable interrupt controller
40h - 43h	System Timer
4Eh – 4Fh	Motherboard resources
50h - 53h	System Timer
61h, 63h, 65h	Motherboard resources
62h and 66h	ACPI-Compliant Embedded Controller
67h, 70h , 80h and 92h	Motherboard resources
A0h, A4h, A8h, ACh - ADh, B0h -B1h, B4h - B5h, B8h - B9h and BCh – BDh	Programmable interrupt controller
B2h - B3h	Motherboard resources
200h - 201h	SEMA Embedded Controller
2E8h – 2EFh	Serial port 4 (COM4)
2F8h - 2FFh	Serial port 2 (COM2)
3E8h – 3EFh	Serial port 3 (COM3)
3F8h - 3FFh	Serial port 1 (COM1)
4D0h - 4D1h	Programmable interrupt controller
680h - 69Fh	Motherboard resources
A00h - A1Fh, A20h – A2Fh, A30h - A3Fh, A40h - A4Fh, A50h - A5Fh and A60h - A6Fh	Motherboard resources

Hex Range	Device
CF8h – 0CFBh	PCI configuration address register (32bit I/O only)
0CF9h	Reset Controller register (8 bit I/O)
0CFCh – 0CFFh	PCI configuration data register
D00h - FFFFh	PCI Express Root Complex
164Eh - 164Fh, 1854h – 1857h and 2000h – 20FEh	Motherboard resources
3000h- 307Fh	Microsoft Basic Display Adapter
3080h- 3083h and 3090h - 3097h	Standard SATA AHCI Controller
EFA0h - EFBFh	Intel® SMBus
FFF8h - FFFFh	Intel® Active Management Technology

6.3 Interrupt Request (IRQ) Lines

APIC Mode

IRQ#	Typical Interrupt Resource
0	System timer
3	Serial Port 2
4	Serial Port 1
5	Serial Port 3
7	Serial Port 4
14	Intel® Serial IO GPIO Host Controller – INT1056
16	Intel® Serial IO UART Host Controller
17	High Definition Audio Controller
19	Intel® Active Management Technology – SOL

IRQ#	Typical Interrupt Resource
27	Intel® Serial IO I2C Host Controller – 7ACC
29	Intel® Serial IO I2C Host Controller – 7ACE
31	Intel® Serial IO I2C Host Controller – 7AFC
32	Intel® Serial IO I2C Host Controller – 7AFD
37	Intel® Serial IO I2C Host Controller – 7AAB
40	Intel® Serial IO I2C Host Controller – 7ACD
43	Intel® Serial IO I2C Host Controller – 7ACF

6.4 PCI Configuration Space Map

Bus Number	Device Number	Function Number	Routing	Description
00h	00h	00h	Internal	Intel Host Bridge
00h	02h	00h	Internal	Intel VGA Controller(Pci Express)
00h	04h	00h	Internal	Intel Data acquisition/signal process
00h	08h	00h	Internal	Intel System Peripherals
00h	0Ah	00h	Internal	Intel Data acquisition/signal process
00h	14h	00h	Internal	Intel USB3.0 XHCI
00h	14h	02h	Internal	Intel RAM
00h	15h	00h	Internal	Intel Serial Bus controller
00h	15h	01h	Internal	Intel Serial Bus controller
00h	15h	02h	Internal	Intel Serial Bus controller
00h	15h	03h	Internal	Intel Serial Bus controller

Bus Number	Device Number	Function Number	Routing	Description
00h	16h	00h	Internal	Intel Communication device
00h	16h	03h	Internal	Intel 16550 serial controller
00h	17h	00h	Internal	Intel AHCI 1.0 Controller
00h	19h	00h	Internal	Intel Serial Bus controller
00h	19h	01h	Internal	Intel Serial Bus controller
00h	1Ch	00h	Internal	Intel PCI-to-PCI bridge(PCI Express)
00h	1Ch	07h	Internal	Intel PCI-to-PCI bridge(PCI Express)
00h	1Eh	00h	Internal	Intel Communication device
00h	1Fh	00h	Internal	Intel Serial Bus controller
00h	1Fh	00h	Internal	Intel ISA bridge
00h	1Fh	03h	Internal	Intel Audio device
00h	1Fh	04h	Internal	Intel SMBUS
00h	1Fh	05h	Internal	Intel Serial Bus controller
01h	00h	00h	Internal	Intel Ethernet controller(PCI Express)
02h	00h	00h	Internal	Intel Ethernet controller(PCI Express)

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	INTB:17	INTA:16	INTA:16			INTA:16
Int1	INTC:18			INTB:17		
Int2	INTD:19				INTC:18	
Int3	INTA:16					

INT Line	XHCI Controller	Intel I225_1	Intel I225_2
Int0	INTA:16		
Int1			
Int2		INTC:18	
Int3			INTD:19

INT Line	PCIE Port1	PCIE Port 2	PCIE Port 3	PCIE Port 4	PCIE Port 5	
Int0	INTB:17	INTB:17	INTC:18	INTD:19	INTA:16	N/A
Int1	INTC:18	INTC:18	INTD:19	INTA:16	INTB:17	N/A
Int2	INTD:19	INTD:19	INTA:16	INTB:17	INTC:18	N/A
Int3	INTA:16	INTA:16	INTB:17	INTC:18	INTD:19	N/A

6.6 SMBus Address Table

Device	Address
DDR5 Channel A(SO-DIMM1)	A0h
DDR5 Channel B(SO-DIMM2)	A2h
DDR5 Channel C(SO-DIMM3)	A4h
DDR5 Channel D(SO-DIMM4)	A6h

6.7 I2C Address Table

Device	Address
Thermal Sensor	90h
Thermal Sensor	92h
EEPROM	A0h
Crypto Authentication	60h

7. BIOS Configurations

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. ► indicates a submenu

Main	Advanced	Chipset	Security
BIOS Information System Information Board Information ► System Date System Time	Serial Port ConsoleRedirection ► PCI Subsystem Settings ► Power Management ► System Management ► Thermal Management ► Watchdog Timer ► Super IO Configuration ► Miscellaneous ► Network Stack Configuration ► Trusted Computing ►	System Agent (SA) Configuration► PCH-IO Configuration►	Password Description Secure Boot Menu

Boot	Save & Exit
Boot Configuration	Save Options Default Options Boot Override

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 screen shot of this menu for details of the submenus and settings.

7.2.1 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
MRC Version	Info only	Display compliancy information
GOP 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.

Board Information	Info only	Description
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 S0 state.
Current Runtime	Read only	The returned value specifies the time in seconds the system is running in 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 Boot counter 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.

Feature	Options
CPU Configuration	submenu
Power & Performance	
Intel(R) Time Coordinated Computing	submenu
Graphics Configuration	submenu
Power Management	submenu
System Management	submenu
Thermal Management	submenu
Watchdog Timer	submenu
USB Configuration	submenu
AMT Configuration	submenu
AMI Graphic Output Protocol Policy	submenu
Super IO Configuration	submenu

Feature	Options
Serial Port Console Redirection	submenu
Miscellaneous Configuration	submenu
Network Configuration	submenu
NVME Configuration	submenu
PCI subsystem Settings	submenu
Trusted Computing	submenu

7.3.1 CPU Configuration

Feature	Options	Description
Efficient-core Information	submenu	
Performance-core Information	submenu	
ID	Info only	Displays the Processor Stepping.
Brand String	Info only	Brand String of the Performance Processor
VMX	Info only	VMX Supported or Not
SMX/TXT	Info only	SMX/TXT Supported or Not
TXT SPAD	Info only	TXT SPAD Register value
Boot Guard Status	Info only	Boot Guard Status Register value
Boot Guard ACM Policy Status	Info only	Boot Guard ACM Policy Status value
C6DRAM	Disabled **Enable**	Enable/Disable moving of DRAM contents to PRM memory when CPU is in C6 state
CPU Flex Ratio Override	**Disabled** Enable	Enable/Disable CPU Flex Ratio Programming

Feature	Options	Description
CPU Flex Ratio Settings		This value must be between Max Efficiency Ratio (LFM) and Maximum non-turbo ratio set by Hardware (HFM).
Hardware Prefetcher	Disabled **Enable**	To turn on/off the MLC streamer prefetcher.
Adjacent Cache Line Prefetch	Disabled **Enable**	To turn on/off prefetching of adjacent cache lines.
Intel (VMX) Virtualization Technology	Disabled **Enable**	When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.
PECI	Disabled **Enable**	Enable/Disable PECI
AVX	Disabled **Enable**	Enable/Disable the Avx 2 Instructions. This is applicable for Performance-core only
Active Performance-cores	**All** 7 6 5 4 3 2 1	Number of P-cores to enable in each processor package. Note: Number of Cores and E-cores are looked at together. When both are {0,0}, Pcode will enable all cores.
Active Efficient-cores	**All** 15 14 13 12 11 10 9 8 7	Number of E-cores to enable in each processor package. Note: Number of Cores and E-cores are looked at together. When both are {0,0}, Pcode will enable all cores.

Feature	Options	Description
	6 5 4 3 2 1	
Hyper-Threading	Disabled **Enable**	Enable or Disable Hyper-Threading Technology.
BIST	**Disabled** Enable	Enable/Disable BIST (Built-In Self Test) on reset
AP threads Idle Manner	HALT Loop **MWAIT Loop** RUN Loop	AP threads Idle Manner for waiting signal to run
AES	Disabled **Enable**	Enable/Disable AES (Advanced Encryption Standard)
MachineCheck	Disabled **Enable**	Enable/Disable Machine Check
MonitorMWait	Disabled **Enable**	Enable/Disable MonitorMWait, if Disable MonitorMwait, the AP threads Idle Manner should not set in MWAIT Loop
Intel Trusted Execution Technology	**Disabled** Enable	Enables utilization of additional hardware capabilities provided by Intel (R) Trusted Execution Technology.Changes require a full power cycle to take effect.
Alias Check Request	**Disabled** Enable	Enables Txt Alias Checking capability Changes require full Txt capability before it will take effect. It is a one time only change, next reboot will be reset.
DPR Memory Size (MB)	**4**	Reserve DPR memory size (0-255) MB
Reset AUX Content	Yes **No**	Reset TPM Aux content. Txt may not functional after AUX content gets reset.
CPU SMM Enhancement	submenu	CPU SMM Enhancement

Feature	Options	Description
Total Memory Encryption	**Disabled** Enable	Configure Total Memory Encryption (TME) to protect DRAM data from physical attacks.
Legacy Game Compatibility Mode	**Disabled** Enable	When enabled, Pressing the scroll lock key will toggle the Efficient-cores between being parked when Scroll Lock LED is on and un-parked when LED is off.

7.3.1.1 CPU Configuration > Efficient-core Information

Feature	Options	Description
L1 Data Cache	Info only	
L1 Instruction Cache	Info only	
L2 Cache	Info only	
L3 Cache	Info only	

7.3.1.2 CPU Configuration > Performance-core Information

Feature	Options	Description
L1 Data Cache	Info only	
L1 Instruction Cache	Info only	
L2 Cache	Info only	
L3 Cache	Info only	

7.3.1.3 CPU Configuration > CPU SMM Enhancement

Feature	Options	Description
SMM Use Delay Indication	Disabled **Enabled**	Enable/Disable usage of SMM_DELAYED MSR for MP sync in SMI
SMM Use Block Indication	Disabled **Enabled**	Enable/Disable usage of SMM_BLOCKED MSR for MP sync in SMI
SMM Use SMM en-US Indication	Disabled **Enabled**	Enable/Disable usage of SMM_ENABLE MSR for MP sync in SMI

7.3.2 Power & Performance

Feature	Options	Description
CPU - Power Management Control	submenu	CPU - Power Management Control Options
GT - Power Management Control	submenu	GT - Power Management Control Options

7.3.2.1 Power & Performance > CPU - Power Management Control

Feature	Options	Description
Boot performance mode	Max Battery Max Non-Turbo Performance **Turbo Performance**	Select the performance state that the BIOS will set starting from reset vector.
Intel(R) Speed Step (tm)	Disabled **Enabled**	Allows more than two frequency ranges to be supported.
Race To Halt (RTH)	Disabled **Enabled**	Enable/Disable Race To Halt feature. RTH will dynamically increase CPU frequency in order to enter pkg C-State faster to reduce overall power. (RTH is controlled through MSR 1FC bit 20)

Feature	Options	Description
Intel(R) Speed Shift Technology	Disabled **Enabled**	Enable/Disable Intel(R) Speed Shift Technology support. Enabling will expose the CPPC v2 interface to allow for hardware controlled P-states.
Per Core P State OS control mode	Disabled **Enabled**	Enable/Disable Per Core P state OS control mode. Disabling will set Bit 31 = 1 command 0x06. When set, the highest core request is used for all other core requests.
HwP Autonomous EPP Grouping	Disabled **Enabled**	Enable EPP grouping (default Bit 29 =0, command 0x11) Autonomous will request the same values for all cores with same EPP. Disable EPP grouping (Bit 29 =1 , command 0x11) autonomous will not necessarily request same values for all cores with same EPP.
EPB override over PECI	**Disabled** Enable	Enable/Disable EPB override over PECI. Enable by sending pcode command 0x2b , subcommand 0x3 to 1. This will allow OOB EPB PECI override control
HwP Lock	Disabled **Enabled**	Enable/Disable HWP Lock support in Misc Power Management MSR.
HDC Control	Disabled **Enabled**	This option allows HDC configuration. Disabled: Disable HDC Enabled: Can be enabled by OS if OS native support is available.
Turbo Mode	Disabled **Enabled**	Enable/Disable processor Turbo Mode (requires EMTTM enabled too). AUTO means enabled.
View/Configure Turbo Options	submenu	View/Configure Turbo Options
CPU VR Settings	submenu	Configure CPU VR Settings
Platform PL1 Enable	**Disabled** Enable	Enable/Disable Platform Power Limit 1 programming. If this option is enabled, it activates the PL1 value to be used by the processor to limit the average power of given time window.
Platform PL2 Enable	**Disabled** Enable	Enable/Disable Platform Power Limit 2 programming. If this option is disabled, BIOS will program the default values for Platform Power Limit 2.
Power Limit 4 Override	**Disabled** Enable	Enable/Disable Power Limit 4 override. If this option is disabled, BIOS will leave the default values for Power Limit 4.
C states	**Disabled** Enable	Enable/Disable CPU Power Management. Allows CPU to go to C states when it's not 100% utilized.
Thermal Monitor	Disabled **Enabled**	Enable/Disable Thermal Monitor

Feature	Options	Description
Interrupt Redirection Mode Selection	**Fixed Priority** Round robin Hash Vector No Change	Interrupt Redirection Mode Select for Logical Interrupts
Timed MWAIT	**Disabled** Enable	Enable/Disable Timed MWAIT Support
Custom P-state Table	submenu	Add Custom P-state Table
Energy Performance Gain	**Disabled** Enable	Enable/disable Energy Performance Gain.
EPG DIMM Idd3N	**26**	Active standby current (Idd3N) in milliamps from datasheet. Must be calculated on a per DIMM basis.
EPG DIMM Idd3P	**11**	Active power-down current (Idd3P) in milliamps from datasheet. Must be calculated on a per DIMM basis.
Power Limit 3 Settings	submenu	Power Limit 3 Settings
CPU Lock Configuration	submenu	CPU Lock Configuration
Dual Tau Boost	**Disabled** Enable	Enable Dual Tau Boost feature. This is only applicable for Desktop 35W/65W/125W sku. When DPTF is enabled this feature is ignored.

7.3.2.1.1 Power & Performance > CPU - Power Management Control > View/Configure Turbo Options

Feature	Options	Description
Turbo Ratio Limit Options	submenu	View/Configure Turbo Ratio Limit Options
Energy Efficient P-state	Disabled **Enabled**	Enable/Disable Energy Efficient P-state feature. When set to 0, will disable access to ENERGY_PERFORMANCE_BIAS MSR and CPUID Function 6 ECX[3] will read 0 indicating no support for Energy Efficient policy setting. When set to 1 will enable access to ENERGY_PERFORMANCE_BIAS MSR 1B0h and CPUID Function 6 ECX[3] will read 1 indicating Energy Efficient policy setting is supported.
Package Power Limit MSR Lock	**Disabled** Enable	Enable/Disable locking of Package Power Limit settings. When enabled, PACKAGE_POWER_LIMIT MSR will be locked and a reset will be required to unlock the register.

Feature	Options	Description
Power Limit 1 Override	**Disabled** Enable	Enable/Disable Power Limit 1 override. If this option is disabled, BIOS will program the default values for Power Limit 1 and Power Limit 1 Time Window.
Power Limit 2 Override	Disabled **Enabled**	Enable/Disable Power Limit 2 override. If this option is disabled, BIOS will program the default values for Power Limit 2.
Power Limit 2	**0**	Power Limit 2 value in Milli Watts. BIOS will round to the nearest 1/8W when programming. If the value is 0, BIOS will program this value as 1.25*Processor Base Power (TDP). For 12.50W, enter 12500. Processor applies control policies such that the package power does not exceed this limit.
Energy Efficient Turbo	Disabled **Enabled**	Enable/Disable Energy Efficient Turbo Feature. This feature will opportunistically lower the turbo frequency to increase efficiency. Recommended only to disable in overclocking situations where turbo frequency must remain constant. Otherwise, leave enabled.

7.3.2.1.2 Power & Performance > CPU - Power Management Control > CPU VR Settings

Feature	Options	Description
Current VccIn Aux Icc Max	Info only	Current VccIn Aux Icc Max
PSYS Slope	**0**	PSYS Slope defined in 1/100 increments. Range is 0-200. For a 1.25 slope, enter 125. 0 = AUTO. Uses BIOS VR mailbox command 0x9.
PSYS Offset	**0**	PSYS Offset defined in 1/1000 increments. Range is 0-63999. For an offset of 25.348, enter 25348. PSYS Uses BIOS VR mailbox command 0x4.
PSYS Prefix	**+** -	Sets the offset value as positive or negative.
PSYS PMax Power	**0**	Psys Pmax power, defined in 1/8 Watt or 1/8 Percent increments. For Watts, range is 0-8191 (ex. For 125W, enter 1000). For ATX12VO Percent, Range is 0-1600 (ex. For recommended value of 200%, enter 1600). Uses BIOS VR mailbox command 0xB.
Min Voltage Override	**Disabled** Enable	Min Voltage Override. Enable to override minimum voltage for runtime and for C8.
VccIn Aux Icc Max	**0**	Sets the Max Icc VccIn Aux value defined in 1/4A increments. Range is 0-512. For an IccMax 32A, enter 128(32*4).

Feature	Options	Description
VccIn Aux IMON Slope	**100**	VccIN Aux IMON Slope defined in 1/100 increments. Range is 0-200. For a 1.25 slope, enter 125. 0 = AUTO. Uses BIOS VR mailbox command 0x18.
VccIN Aux IMON Offset	**0**	VccIN Aux IMON Offset defined in 1/1000 increments. Range is 0-63999. For an offset of 25.348, enter 25348. IMON Uses BIOS VR mailbox command 0x18.
VccIN Aux IMON Prefix	**+** -	Sets the offset value as positive or negative.
Vsys/Psys Critical	**Disabled** Enable	Vsys/Psys Critical Enable or disable
Assertion Deglitch Mantissa	**1**	Assertion Deglitch Mantissa 0x4F[7-3]. Assertion Deglitch = 2µs * Mantissa * 2^(Exponent)
Assertion Deglitch Exponent	**0**	Assertion Deglitch Exponent 0x4F[3-0]. Assertion Deglitch = 2µs * Mantissa * 2^(Exponent)
De assertion Deglitch Mantissa	**13**	De Assertion Deglitch Mantissa 0x49[7-3]. Assertion Deglitch = 2µs * Mantissa * 2^(Exponent)
De assertion Deglitch Exponent	**2**	De Assertion Deglitch Exponent 0x49[3-0]. Assertion Deglitch = 2µs * Mantissa * 2^(Exponent)
VR Power Delivery Design	**AUTO** ADL S 881 35W ADL S 881 125W ADL S 841 35W ADL S 841 65W ADL S 841 125W ADL S 641 35W ADL S 641 65W ADL S 641 125W ADL S 681 35W ADL S 801 35W ADL S 801 65W ADL S 401 35W ADL S 401 65W ADL S 601 35W ADL S 601 65W ADL S 201 35W	Specifies the ADL Desktop board design used for the VR settings override values. By default, BIOS will override the default Desktop VR settings based on the board design. A value of AUTO(0) will use the board ID to determine the board design. Any other value will override the board id logic to provide a custom VR Power Delivery Design value. This is intended primarily for validation.

Feature	Options	Description
	ADL S 201 46W ADL S 201 65W ADL S 401 58W ADL S 401 60W ADL S 401 63W ADL S BGA 881 65W ADL S BGA 841 65W ADL S BGA 441 65W ADL S BGA 601 65W ADL S BGA 681 65W ADL S BGA 401 65W ADL S Mobile BGA 881 55W ADL S Mobile BGA 681 55W ADL S Mobile BGA 481 55W ADL S Mobile BGA 441 55W RPL S 8161 35W RPL S 8161 65W RPL S 8161 95W RPL S 8161 125W RPL S 8161 150W RPL S 881 35W RPL S 881 65W RPL S 881 125W RPL S 681 125W RPL S 641 65W RPL S 641 125W RPL S 801 80W RPL S 801 95W RPL S 641 35W RPL HX SBGA 8161 55W RPL HX SBGA 8121 55W RPL HX SBGA 881 55 RPL HX	

Feature	Options	Description
	SBGA 681 55W W RPL HX SBGA 641 55W RPL HX SBGA 441 55W RPL2 S 681 35W RPL2 S 681 65W RPL2 S 641 35W RPL2 S 641 65W RPL2 S 401 35W RPL2 S 401 58W RPL2 S 401 60W RPL2 S 401 65W RPL2 S 201 35W RPL2 S 201 46W RPL2 S 201 65W RPL2 S 601 65W RPL2 HX SBGA 881 55W RPL2 HX SBGA 681 55W RPL2 HX SBGA 641 55W RPL2 HX SBGA 481 55W RPL2 HX SBGA 441 55W	
Acoustic Noise Settings	submenu	Configure Acoustic Noise Settings for IA, GT and SA domains
Core/IA VR Settings	submenu	Configure Core/IA VR Settings
GT VR Settings	submenu	Configure GT VR Settings
RFI Settings	submenu	Configure RFI Settings

7.3.2.1.2.1 Power & Performance > CPU - Power Management Control > CPU VR Settings > Acoustic Noise Settings

Feature	Options	Description
Acoustic Noise Mitigation	**Disabled** Enable	Enabling this option will help mitigate acoustic noise on certain SKUs when the CPU is in deeper C state
Pre Wake Time	**0**	Set the maximum Pre Wake randomization time in micro ticks. Range is 0-255. This is for acoustic noise mitigation Dynamic Periodicity Alteration (DPA) tuning.
Ramp Up Time	**0**	Set the maximum Ramp Up randomization time in micro ticks. Range is 0-255. This is for acoustic noise mitigation Dynamic Periodicity Alteration (DPA) tuning.
Ramp Down Time	**0**	Set the maximum Ramp Down randomization time in micro ticks. Range is 0-255. This is for acoustic noise mitigation Dynamic Periodicity Alteration (DPA) tuning.
IA VR Domain	Info only	
Disable Fast PKG C State Ramp for IA Domain	**False** True	This option needs to be configured to reduce acoustic noise during deeper C states. False: Don't disable Fast ramp during deeper C states; True: Disable Fast ramp during deeper C state
Slow Slew Rate for IA Domain	**Fast/2** Fast/4 Fast/8 Fast/16	Set VR IA Slow Slew Rate for Deep Package C State ramp time; Slow slew rate equals to Fast divided by number, the number is 2, 4, 8, 16 to slow down the slew rate to help minimize acoustic noise
GT VR Domain	Info only	
Disable Fast PKG C State Ramp for GT Domain	**False** True	This option needs to be configured to reduce acoustic noise during deeper C states. False: Don't disable Fast ramp during deeper C states; True: Disable Fast ramp during deeper C state
Slow Slew Rate for GT Domain	**Fast/2** Fast/4 Fast/8 Fast/16	Set VR GT Slow Slew Rate for Deep Package C State ramp time; Slow slew rate equals to Fast divided by number, the number is 2, 4, 8 to slow down the slew rate to help minimize acoustic noise; divide by 16 is disabled

7.3.2.1.2.2 Power & Performance > CPU - Power Management Control > CPU VR Settings > Core/IA VR Domain

Feature	Options	Description
VR Config Enable	Disabled **Enable**	VR Config Enable
Current AC Loadline	**110**	Current AC Loadline
Current DC Loadline	**110**	Current DC Loadline
Current Psi1 Threshold	**80**	Current Psi1 Threshold
Current Psi2 Threshold	**20**	Current Psi2 Threshold
Current Psi3 Threshold	**4**	Current Psi3 Threshold
Current Imon Slope	**0**	Current Imon Slope
Current Imon Offset	**1**	Current Imon Offset
Current VR Current Limit	**960**	Current VR Current Limit (Current IccMax Value)
Current Tdc Current Limit	**1280**	Current Tdc Current Limit
Current Voltage Limit	**1740**	Current Voltage Limit
AC Loadline	**0**	AC Loadline defined in 1/100 mOhms. A value of 100 = 1.00 mOhm, and 1255 = 12.55 mOhm. Range is 0-6249 (0-62.49 mOhms). 0 = AUTO/HW default. Uses BIOS mailbox command 0x2.
DC Loadline	**0**	DC Loadline defined in 1/100 mOhms. A value of 100 = 1.00 mOhm, and 1255 = 12.55 mOhm. Range is 0-6249 (0-62.49 mOhms). 0 = AUTO/HW default. Uses BIOS mailbox command 0x2.
PS Current Threshold1	**80**	PS Current Threshold1, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO. Uses BIOS VR mailbox command 0x3.
PS Current Threshold2	**20**	PS Current Threshold2, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO. Uses BIOS VR mailbox command 0x3.
PS Current Threshold3	**4**	PS Current Threshold3, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO. Uses BIOS VR mailbox command 0x3.
PS3 Enable	Disabled **Enable**	PS3 Enable/Disable. 0 - Disabled, 1 - Enabled.Uses BIOS VR mailbox command 0x3.

Feature	Options	Description
PS4 Enable	Disabled **Enable**	PS4 Enable/Disable. 0 - Disabled, 1 - Enabled. Uses BIOS VR mailbox command 0x3
IMON Slope	**0**	IMON Slope defined in 1/100 increments. Range is 0-200. For a 1.25 slope, enter 125. 0 = AUTO. Uses BIOS VR mailbox command 0x4.
IMON Offset	**0**	IMON Offset defined in 1/1000 increments. Range is 0-63999. For an offset of 25.348, enter 25348. IMON Uses BIOS VR mailbox command 0x4.
IMON Prefix	**+** -	Sets the offset value as positive or negative.
VR Current Limit	**0**	Voltage Regulator Current Limit (IccMax). This value represents the Maximum instantaneous current allowed at any given time. The value is represented in 1/4 A increments. A value of 400 = 100A. 0 means AUTO. Uses BIOS VR mailbox command 0x6.
VR Voltage Limit	**0**	Voltage Limit (VMAX). This value represents the Maximum instantaneous voltage allowed at any given time. Range is 0 - 7999mV. Uses BIOS VR mailbox command 0x8.
TDC Enable	Disabled **Enable**	TDC Enable. 0- Disable, 1 - Enable
TDC Current Limit	**0**	TDC Current Limit, defined in 1/8A increments. Range 0-32767. For a TDC Current Limit of 125A, enter 1000. 0 = 0 Amps. Uses BIOS VR mailbox command 0x1A.
TDC Time Window	**1 sec** 2 sec 3 sec 4 sec 5 sec 6 sec 7 sec 8 sec 10 sec 12 sec 14 sec 16 sec 20 sec 24 sec	VR TDC Time Window, value in seconds. 1s is default. Range from 1s to 448s.

Feature	Options	Description
	28 sec 32 sec 40 sec 48 sec 56 sec 64 sec 80 sec 96 sec 112 sec 128 sec 160 sec 192 sec 224 sec 256 sec 320 sec 384 sec 448 sec	
TDC Lock	**Disabled** Enable	TDC Lock
IRMS	**Disabled** Enable	Enable/Disable IRMS - Current root mean square

7.3.2.1.2.3 Power & Performance > CPU - Power Management Control > CPU VR Settings > GT VR Settings

Feature	Options	Description
VR Config Enable	Disabled **Enable**	VR Config Enable
Current AC Loadline	**400**	Current AC Loadline
Current DC Loadline	**400**	Current DC Loadline

Feature	Options	Description
Current Psi1 Threshold	**80**	Current Psi1 Threshold
Current Psi2 Threshold	**20**	Current Psi2 Threshold
Current Psi3 Threshold	**4**	Current Psi3 Threshold
Current Imon Slope	**0**	Current Imon Slope
Current Imon Offset	**1**	Current Imon Offset
Current VR Current Limit	**120**	Current VR Current Limit (Current IccMax Value)
Current Tdc Current Limit	**176**	Current Tdc Current Limit
Current Voltage Limit	**1519**	Current Voltage Limit
AC Loadline	**0**	AC Loadline defined in 1/100 mOhms. A value of 100 = 1.00 mOhm, and 1255 = 12.55 mOhm. Range is 0-6249 (0-62.49 mOhms). 0 = AUTO/HW default. Uses BIOS mailbox command 0x2.
DC Loadline	**0**	DC Loadline defined in 1/100 mOhms. A value of 100 = 1.00 mOhm, and 1255 = 12.55 mOhm. Range is 0-6249 (0-62.49 mOhms). 0 = AUTO/HW default. Uses BIOS mailbox command 0x2.
PS Current Threshold1	**80**	PS Current Threshold1, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO. Uses BIOS VR mailbox command 0x3.
PS Current Threshold2	**20**	PS Current Threshold2, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO. Uses BIOS VR mailbox command 0x3.
PS Current Threshold3	**4**	PS Current Threshold3, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO. Uses BIOS VR mailbox command 0x3.
PS3 Enable	Disabled **Enable**	PS3 Enable/Disable. 0 - Disabled, 1 - Enabled. Uses BIOS VR mailbox command 0x3.
PS4 Enable	Disabled **Enable**	PS4 Enable/Disable. 0 - Disabled, 1 - Enabled. Uses BIOS VR mailbox command 0x3
IMON Slope	**0**	IMON Slope defined in 1/100 increments. Range is 0-200. For a 1.25 slope, enter 125. 0 = AUTO. Uses BIOS VR mailbox command 0x4.
IMON Offset	**0**	IMON Offset defined in 1/1000 increments. Range is 0-63999. For an offset of 25.348, enter 25348. IMON Uses BIOS VR mailbox command 0x4.

Feature	Options	Description
IMON Prefix	**+** -	Sets the offset value as positive or negative.
VR Current Limit	**0**	Voltage Regulator Current Limit (IccMax). This value represents the Maximum instantaneous current allowed at any given time. The value is represented in 1/4 A increments. A value of 400 = 100A. 0 means AUTO. Uses BIOS VR mailbox command 0x6.
VR Voltage Limit	**0**	Voltage Limit (VMAX). This value represents the Maximum instantaneous voltage allowed at any given time. Range is 0 - 7999mV. Uses BIOS VR mailbox command 0x8.
TDC Enable	Disabled **Enable**	TDC Enable. 0- Disable, 1 - Enable
TDC Current Limit	**0**	TDC Current Limit, defined in 1/8A increments. Range 0-32767. For a TDC Current Limit of 125A, enter 1000. 0 = 0 Amps. Uses BIOS VR mailbox command 0x1A.
TDC Time Window	**1 sec** 2 sec 3 sec 4 sec 5 sec 6 sec 7 sec 8 sec 10 sec 12 sec 14 sec 16 sec 20 sec 24 sec 28 sec 32 sec 40 sec 48 sec 56 sec 64 sec	VR TDC Time Window, value in seconds. 1s is default. Range from 1s to 448s.

Feature	Options	Description
	80 sec 96 sec 112 sec 128 sec 160 sec 192 sec 224 sec 256 sec 320 sec 384 sec 448 sec	
TDC Lock	**Disabled** Enable	TDC Lock
IRMS	**Disabled** Enable	Enable/Disable IRMS - Current root mean square

7.3.2.1.2.4 Power & Performance > CPU - Power Management Control > CPU VR Settings > RFI Settings

Feature	Options	Description
RFI Current Frequency	**139.200MHz**	RFI Current Frequency
RFI Frequency		Set desired RFI frequency, in increments of 100KHz. (For a frequency of 100.6MHz, enter 1006.)
FIVR Spread Spectrum	Disabled **Enable**	Enable or Disable the FIVR Spread Spectrum
RFI Spread Spectrum	0.5% 1% **1.5%** 2% 3% 4%	Set the Spread Spectrum

Feature	Options	Description
	5% 6%	

7.3.2.1.3 Power & Performance > CPU - Power Management Control > Custom P-state Table

Feature	Options	Description
Number of P states	**0**	Sets the number of custom P-states. At least 2 states must be present.

7.3.2.1.4 Power & Performance > CPU - Power Management Control > Power Limit 3 Settings

Feature	Options	Description
Power Limit 3 Override	**Disabled** Enable	Enable/Disable Power Limit 3 override. If this option is disabled, BIOS will leave the hardware default values for Power Limit 3 and Power Limit 3 Time Window.

7.3.2.1.5 Power & Performance > CPU - Power Management Control > CPU Lock Configuration

Feature	Options	Description
CFG Lock	Disabled **Enable**	Configure MSR 0xE2[15], CFG Lock bit
Overclocking Lock	Disabled **Enable**	Enable/Disable Overclocking Lock (BIT 20) in FLEX_RATIO(194) MSR

7.3.2.2 Power & Performance > GT - Power Management Control

Feature	Options	Description
RC6(Render Standby)	**Disabled** Enable	Check to enable render standby support.

Feature	Options	Description
Maximum GT frequency	**Default Max Frequency** 100Mhz 150Mhz 200Mhz 250Mhz 300Mhz 350Mhz 400Mhz 450Mhz 500Mhz 550Mhz 600Mhz 650Mhz 700Mhz 750Mhz 800Mhz 850Mhz 900Mhz 950Mhz 1000Mhz 1050Mhz 1100Mhz 1150Mhz 1200Mhz	Auto Updated
Disable Turbo GT frequency	**Disabled** Enable	Enabled: Disables Turbo GT frequency. Disabled: GT frequency is not limited

7.3.3 Intel(R) Time Coordinated Computing

Feature	Options	Description
#AC Split Lock	**Disabled** Enable	Enable or Disable Alignment Check Exception (#AC). When enabled, this will assert a #AC when any atomic operation has an operand that crosses two cache lines.
#GP Fault UC Lock	**Disabled** Enable	Enable or Disable GP Fault Exception (GP#). When enabled, this will assert a GP# when encountering a Lock to un-cacheable memory before the bus is locked.
IFU Enable	**Disabled** Enable	Enable or Disable Instruction Fetch Unit(IFU). When enabled, Instructions will be prefetch to the cache.
Software SRAM	**Disabled** Enable	Enable or Disable Software SRAM. Enable will allocate 1 way of LLC; if Cache Configuration subregion is available, it will allocate based on the subregion.
Data Streams Optimizer	**Disabled** Enable	Enable or Disable Data Streams Optimizer (DSO). Enable will utilize DSO Subregion to tune system. DSO settings supersede Intel(R) TCC Mode settings that overlap between the two.
Error Log	Disabled **Enable**	Enable or Disable Error Log. Enable will record errors related to Intel(R) TCC and save them to memory.
Intel(R) TCC Authentication Menu	submenu	Intel(R) TCC Authentication Menu options
Intel(R) TCC Mode	**Disabled** Enable	Enable or Disable Intel(R) TCC Mode. When enabled, this will modify system settings to improve real-time performance. The full list of settings and their current state are displayed below when Intel(R) TCC mode is enabled.
Intel(R) TCC Mode Affected Settings	Info only	
L2 QOS Enumeration	**Disabled** Enable	Enable or Disable L2 QOS Enumerate. When Enable CPUID Enumeration for L2 QOS gets enabled.
IO Fabric Low Latency	**Disabled** Enable	Enable or Disable IO Fabric Low Latency. This will turn off some power management in the PCH IO fabrics. This option provides the most aggressive IO Fabric performance setting. S3 state is NOT supported.
GT CLOS	**Disabled** Enable	Enable or Disable Graphics Technology (GT) Class of Service. Enable will reduce Gfx LLC allocation to minimize impact of Gfx workload on LLC
C states	submenu	Enable/Disable CPU Power Management. Allows CPU to go to C states when it's not 100% utilized.
Intel(R) Speed Shift Technology	submenu	Enable/Disable Intel(R) Speed Shift Technology support. Enabling will expose the CPPC v2 interface to allow for hardware

Feature	Options	Description
		controlled P-states.
Intel(R) SpeedStep(tm)	submenu	Allows more than two frequency ranges to be supported.
Hyper-Threading	submenu	Enable or Disable Hyper-Threading Technology.
ACPI D3Cold Support	submenu	Enable/Disable ACPI D3Cold support to be executed on D3 entry and exit\n\nNote: Disable it would affect the Storage D3 setting
Low Power S0 Idle Capability	submenu	This variable determines if we enable ACPI Lower Power S0 Idle Capability (Mutually exclusive with Smart connect). While this is enabled, it also disable 8254 timer for SLP_S0 support.
SA GV	submenu	System Agent Geyser Ville. Can disable, fix to a specific point, or enable frequency switching.
Page Close Idle Timeout	submenu	Page Close Idle Timeout Control
Power Down Mode	submenu	CKE Power Down Mode Control
RC6(Render Standby)	submenu	Check to enable render standby support.
DMI Link ASPM Control	submenu	The control of Active State Power Management of the DMI Link.
PCH TSN Multi-Vc	submenu	Enable/Disable PCH TSN Multi Virtual Channels.
Legacy IO Low Latency	submenu	Set to enable low latency of legacy IO. Some systems require lower IO latency irrespective of power. This is a tradeoff between power and IO latency.
CPU PCI Express Configuration	submenu	
PCH PCI Express Configuration	submenu	

7.3.3.1 Intel(R) Time Coordinated Computing > Intel(R) TCC Authentication Menu

Feature	Options	Description
Intel(R) TCC Authentication	Disabled Non-OEM Enrolled Key **OEM Enrolled Key**	Intel(R) TCC Authentication determines the key to be used. OEM Enrolled Key is built in by OEM. Non-OEM Enrolled Key can be add by user.

7.3.4 Graphics Configuration

Feature	Options	Description
Graphics Turbo IMON Current	**31**	Graphics turbo IMON current values supported (14-31)
Skip Scaning of External Gfx Card	**Disabled** Enabled	If Enable, it will not scan for External Gfx Card on PEG and PCH PCIE Ports
Primary Display	**Auto** IGFX PEG PCH PCI HG	Select which of IGFX/PEG/PCI Graphics device should be Primary Display Or select HG for Hybrid Gfx.
External Gfx Card Primary Display Configuration	submenu	External Gfx Card Primary Display Configuration
Internal Graphics	Disabled **Enabled**	Keep IGFX enabled based on the setup options.
GTT Size	2MB 4MB **8MB**	Select the GTT Size
Aperture Size	128MB **256MB** 512MB 1024MB	Select the Aperture Size Note: Above 4GB MMIO BIOS assignment is automatically enabled when selecting > 2048MB aperture. To use this feature, please disable CSM Support.
DVMT Pre-Allocated	0M 32M 64M 96M 128M 160M 4M 8M 12M	Select DVMT 5.0 Pre-Allocated (Fixed) Graphics Memory size used by the Internal Graphics Device.

Feature	Options	Description
	20M 24M 28M 32M/F7 36M 40M 44M 48M 52M 56M **60M**	
Intel Graphics Pei Display Peim	**Disabled** Enabled	Enable/Disable Pei (Early) Display
VDD Enable	Disabled **Enabled**	Enable/Disable forcing of VDD in the BIOS
Configure GT for use	Disabled **Enabled**	Enable/Disable GT configuration in BIOS
RC1p Support	**Disabled** Enabled	Enable/Disable RC1p support. If RC1p is enabled, send a RC1p frequency request to PMA based other conditions being met
PAVP Enable	Disabled **Enabled**	Enable/Disable PAVP
Cdynmax Clamping Enable	**Disabled** Enabled	Enable/Disable Cdynmax Clamping
Cd Clock Frequency	192 Mhz 307.2 Mhz 326.4 Mhz 556.8 Mhz 652.8 Mhz **Max CdClock freq**	Select the highest Cd Clock frequency supported by the platform

Feature	Options	Description
	based on Reference Clk	
Skip Full CD Clock Init	**Disabled** Enabled	Enabled: Skip Full CD clock initialization.\nDisabled: Initialize the full CD clock if not initialized by Gfx PEIM
VBT Select	**eDP** MIPI ADLP/RPLP RVP DDR5 ADLP RVP DDR4 RPLP CRB	Select VBT for GOP Driver\nSelect Vbt to MIPI if any of the Display has MIPI
Enable Display Audio Link in Pre-OS	Disabled **Enabled**	Enable: Display Audio Link will be enabled in Pre-OS.\nDisabled : Display Audio Link will be disabled in Pre-OS.
IUER Button Enable	**Disabled** Enabled	Enable/Disable IUER Button Functionality
LCD Control	submenu	LCD Control

7.3.4.1 Graphics Configuration > LCD Control

Feature	Options	Description
Primary IGFX Boot Display	**VBIOS Default** EFP LFP EFP3 EFP2 EFP4	Select the Video Device which will be activated during POST.\nThis has no effect if external graphics present.\nSecondary boot display selection will appear based on your selection.\nVGA modes will be supported only on primary display\n
LCD Panel Type	**VBIOS Default** 640x480 LVDS 800x600 LVDS 1024x768 LVDS 1280x1024 LVDS	Select LCD panel used by Internal Graphics Device by selecting the appropriate setup item.

Feature	Options	Description
	1400x1050 LVDS1 1400x1050 LVDS2 1600x1200 LVDS 1280x768 LVDS 1680x1050 LVDS 1920x1200 LVDS 1600x900 LVDS 1280x800 LVDS 1280x600 LVDS 2048x1536 LVDS 1366x768 LVDS	
Panel Scaling	**Auto** Off Force Scaling	Select the LCD panel scaling option used by the Internal Graphics Device.
Backlight Control	PWM Inverted **PWM Normal**	Back Light Control Setting
Active LFP	No eDP **eDP Port-A**	Select the Active LFP Configuration.\n\nNo LVDS:VBIOS does not enable LVDS.\nInt-LVDS:VBIOS enables LVDS driver by Integrated encoder.\nSDVO LVDS:VBIOS enables LVDS driver by SDVO encoder.\neDP Port-A:LFP Driven by Int-DisplayPort encoder from Port-A.\neDP Port-D:LFP Driven by Int-DisplayPort encoder from Port-D(through PCH).
Panel Color Depth	**18 Bit** 24 Bit	Select the LFP Panel Color Depth
Backlight Brightness	**255**	Set VBIOS Brightness.\nRange : 0-255.

7.3.5 Power Management

Feature	Options	Description
Power Management	Info only	
Enable ACPI Auto Configuration	**Disabled** Enabled	Enables or Disables BIOS ACPI Auto Configuration.
Enable Hibernation	Disabled **Enabled**	Enables or Disables System ability to Hibernate (OS/S4 Sleep State). This option may not be effective with some OSs.
ACPI Sleep State	**S3 (Suspend to RAM)** Suspend Disabled	Select the highest ACPI sleep state the system will enter when the SUSPEND button is pressed.
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 last power state
ATTENTION: The Power-Up Mode only has effect, if the module is in ATX-Mode.	Info only	
Power Consumption	Submenu	

7.3.5.1 Power Management > Power Consumption

Feature	Options	Description
Power Consumption	Info only	
Main Current	Read only	Display input current.

Feature	Options	Description
Current Input Power	Read only	Display input power.
RTC	Read only	Display actual voltage of the RTC.
5VSB	Read only	Display actual voltage of the 5VSB.
VIN	Read only	Display actual voltage of the VIN.
3.3V	Read only	Display actual voltage of the 3.3V.
VMEM	Read only	Display actual voltage of the VMEM.
3.3VSB	Read only	Display actual voltage of the 3.3VSB.
VCORE	Read only	Display actual voltage of the VCORE.

7.3.6 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
Temperatures	Read only
Voltage Monitor	Read only
Display Backlight Control	Read only

Feature	Options
Power-up Watchdog	Read only
Power Monitor (Current Sense)	Read only
Boot Counter	Read only
Dual-BIOS	Read only
I2C Bus 1	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
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
Ext-GPIO Input Interrupt Support	Read only

7.3.6.1 System Management > SEMA Flags

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

7.3.7 Thermal Management

Feature	Options	Description
Passive Cooling Trip Point	**Disable** 90 C 95 C 99 C	This value is the temperature threshold of the passive cooling trip point.
Critical Trip Point	**Disable** 95 C 8 C 100 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	

Feature	Options	Description
CPU Temperature	Info only	
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	

7.3.7.1 Thermal Management > Smart Fan

Feature	Options	Description
Smart Fan	Info only	
CPU Smart Fan Temperature Source	**CPU Sensor** Board Sensor	CPU Smart Fan Temperature Source.
CPU Fan Mode	**AUTO** Fan Off Fan On	CPU Fan Mode
Trigger Point 1	Info only	
Trigger Temperature	40	Trigger Temperature

Feature	Options	Description
PWM Level	30	PWM Level
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

7.3.8 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 amount of time after power up.

7.3.9 USB Configuration

Feature	Options	Description
Legacy USB Support	Disabled **Enabled**	Enables Legacy USB support. AUTO option disables legacy support if no USB devices are connected. DISABLE option will keep USB devices available only for EFI applications.
XHCI Hand-off	Disabled **Enabled**	This is a workaround for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.
USB Mass Storage Driver Support	Disabled **Enabled**	
USB hardware delays and time-outs:	Info only	
USB transfer time-out	1 sec 5 sec 10 sec **20 sec**	The time-out value for Control, Bulk, and Interrupt transfers.
Device reset time-out	10 sec **20 sec** 30 sec 40 sec	USB mass storage device Start Unit command time-out.
Device power-up delay	**Auto** Manual	Maximum time the device will take before it properly reports itself to the Host Controller. 'Auto' uses default value: for a Root port it is 100 ms, for a Hub port the delay is taken from Hub descriptor.

7.3.10 AMT Configuration

Feature	Options	Description
USB Provisioning of AMT	**Disabled** Enabled	Enable/Disable of AMT USB Provisioning.
MAC Pass Through	**Disabled** Enabled	Enable/Disable MAC Pass Through function.

Feature	Options	Description
Activate Remote Assistance Process	**Disabled** Enabled	Trigger CIRA boot\n\nNote:\nNetwork Access must be activated first from MEBx Setup.
Unconfigure ME:	**Disabled** Enabled	Unconfigure ME with resetting MEBx password to default on next boot.
ASF Configuration	submenu	Configure Alert Standard Format parameters.
Secure Erase Configuration	submenu	Secure Erase configuration menu
One Click Recovery(OCR) Configuration	submenu	Configuration setting for One Click Recovery. This allows access for AMT to boot a recovery OS application.

7.3.10.1 AMT Configuration > ASF Configuration

Feature	Options	Description
PET Progress	Disabled **Enabled**	Enable/Disable PET Events Progress to receive PET Events.
WatchDog	**Disabled** Enabled	Enable/Disable WatchDog Timer.
OS Timer	0	Set OS watchdog timer.
BIOS Timer	0	Set BIOS watchdog timer.
ASF Sensors Table	**Disabled** Enabled	Adds ASF Sensor Table into ASF! ACPI Table

7.3.10.2 AMT Configuration > Secure Erase Configuration

Feature	Options	Description
Secure Erase mode	**Simulated** Real	Change Secure Erase module behavior:\nSimulated: Performs SE flow without erasing SSD\nReal: Erase SSD.\n*** If SATA device is used, OEM could use SECURE_ERASE_HOOK_PROTOCOL to remove SATA power to skip G3 cycle. ***

Feature	Options	Description
Force Secure Erase	**Disabled** Enabled	Force Secure Erase on next boot

7.3.10.3 AMT Configuration > One Click Recovery (OCR) Configuration

Feature	Options	Description
OCR Https Boot	Disabled **Enabled**	Enable/Disable One Click Recovery Https Boot
OCR PBA Boot	Disabled **Enabled**	Enable/Disable One Click Recovery PBA Boot
OCR Windows Recovery Boot	Disabled **Enabled**	Enable/Disable One Click Recovery Windows Recovery Boot
OCR Disable Secure Boot	Disabled **Enabled**	Allows CSME to request SecureBoot to be disabled for One Click Recovery

7.3.11 AMI Graphic Output Protocol Policy

Feature	Options	Description
Output Select	Info only	Output Interface

7.3.12 Super IO Configuration

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

Feature	Options
Nct6126dSec Super IO Configuration	submenu

7.3.12.1 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

7.3.12.1.1 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	Select an optimal setting for Super IO device.

Feature	Options	Description
	IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12	
Change Settings	**Normal** High Speed	Select an optimal settings for Super IO Device.

7.3.12.1.2 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.
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.
Change Settings	**Normal** High Speed	Select an optimal settings for Super IO Device.

7.3.12.2 Super IO Configuration > Nct6126dSec Super IO Configuration

Feature	Options
Nct6126dSec Super IO Configuration	Info only
Super IO Chip	Info only
Serial Port 1 Configuration	submenu
Serial Port 2 Configuration	submenu

7.3.12.2.1 Super IO Configuration > Nct6126dSec 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=240h; IRQ=5	Fixed configuration of serial port.
Change Settings	**Auto** IO=240h; IRQ=5 IO=248h; IRQ=3,4,5,6,7,9,10,11,12 IO=250h; IRQ=3,4,5,6,7,9,10,11,12 IO=258h; 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 settings for Super IO Device.

7.3.12.2.2 Super IO Configuration > Nct6126dSec 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=248h; IRQ=7	Fixed configuration of serial port.
Change Settings	**Auto** IO=240h; IRQ=5 IO=248h; IRQ=3,4,5,6,7,9,10,11,12 IO=250h; IRQ=3,4,5,6,7,9,10,11,12 IO=258h; 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 settings for Super IO Device.

7.3.13 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	

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

7.3.13.1 Serial Console Redirection > Console Redirection Settings (COM0)

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 **8**	Data Bits.
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 do not allow for error detection..
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 re-start 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**	With this mode enabled only text will be sent. This is to capture Terminal data.

Feature	Options	Description
	Enable	
Resolution 100x31	**Disabled** Enable	Enables or disables extended terminal resolution
Putty KeyPad	**VT100** LINUX XTERMR6 SCO ESCN VT400	Select FunctionKey and KeyPad on Putty.

7.3.13.2 Serial Console Redirection > Console Redirection Settings (COM1)

Feature	Options	Description
COM1	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 **8**	Data Bits.
Parity	**None**	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

Feature	Options	Description
	Even Odd Mark Space	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 do not allow for error detection..
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 re-start 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.

7.3.13.3 Serial Console Redirection > Console Redirection Settings (COM2)

Feature	Options	Description
COM2	Info only	
Console Redirection Settings	Info only	

Feature	Options	Description
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 **8**	Data Bits.
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 do not allow for error detection..
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 re-start 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**	Select FunctionKey and KeyPad on Putty.

Feature	Options	Description
	LINUX XTERMR6 SCO ESCN VT400	

7.3.13.4 Serial Console Redirection > Console Redirection Settings (COM3)

Feature	Options	Description
COM3	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 **8**	Data Bits.
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 do not allow for error detection..
Stop Bits	**1**	Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1

Feature	Options	Description
	2	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 re-start 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.

7.3.13.5 Serial Console Redirection > Console Redirection Settings (OOB Management)

Feature	Options	Description
Out-of-Band Mgmt Port	**COM0** COM1	Microsoft Windows Emergency Management Services (EMS) allows for 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 Console Redirection Settings page, for more Help with Terminal Type/Emulation.
Bits per second	9600 19200	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.

Feature	Options	Description
	38400 57600 **115200**	
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 re-start the flow. Hardware flow control uses two wires to send start/stop signals.
Data Bits EMS	**8**	
Parity EMS	**None**	
Stop Bits EMS	**1**	

7.3.14 Miscellaneous

Feature	Options	Description
Miscellaneous	Info only	
Power Supply Unit	Emulate AT Mode **ATX Mode**	Select Emulation AT or ATX function. If this option set to [Emulation AT], BIOS will report no suspend functions (S3 & S4) to ACPI OS. In windows XP, it will make OS show shutdown message during system shutdown. ATX: OS will turn off system power when shutdown.
I2C Speed Control	**100 Kbps** 400 Kbps	I2C Speed Control
SMBUS Select Configuration	From EC **From PCH**	SMBUS Select Configuration from PCH or EC.
WOL From S5	**ON** OFF	This Config to control power on/off LAN in S5 State by SEMA(EC).
LID Function	**Disabled** Enabled	Enable/Disable LID Function

Sleep Function	Disabled **Enabled**	Enable/Disable Sleep Button Function
Smart Battery Function	**Disabled** Enabled	Enable/Disable Smart Battery function. Auto: disable Smart Battery function if charger IC not be detected.
eSPI / EC Slave 1 Device Enable	**Disabled** Enabled	Notes: If there is a device to connect the PCH by ESPI_CS1, please enable it. Please make sure the system boots completed after changing the configuration. Do Not Attempt to Shut Down Your Computer, doing that may lead to system malfunction.

7.3.15 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.

7.3.16 PCI Subsystem Settings

Feature	Options	Description
Re-Size BAR Support	Disabled **Enabled**	If system has Resizable BAR capable PCIe Devices, this option Enables or Disables Resizable BAR Support.
BME DMA Mitigation	**Disabled** Enabled	Re-enable Bus Master Attribute disabled during Pci enumeration for PCI Bridges after SMM Locked

7.3.17 Trusted Computing

Feature	Options	Description
TPM 2.0 Device Found	Info only	
Firmware Version	Info only	
Vendor	Info only	
Security Device Support	**Disabled** Enabled	Enables or Disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.
Active PCR banks	Info only	
Available PCR banks	Info only	
SHA256 PCR Bank	Disabled **Enabled**	Enable or Disable SHA256 PCR Bank
SHA384 PCR Bank	**Disabled** Enabled	Enable or Disable SHA384 PCR Bank
SM3_256 PCR Bank	**Disabled** Enabled	Enable or Disable SM3_256 PCR Bank
Pending operation	**None** TPM Clear	Schedule an Operation for the Security Device. NOTE: Your Computer will reboot during restart in order to change State of Security Device.

Feature	Options	Description
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
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

7.3.18 PTT Configuration

Feature	Options	Description
Reminder: Make sure you have dTPM on board before selecting dTPM.	Info only	
TPM Device Selection	dTPM **PTT**	Selects TPM device: PTT or discrete TPM.\nPTT - enables PTT in SkuMgr\ndTPM - disables PTT is SkuMgr\n\nWarning!\nPTT/dTPM will be disabled and all data saved on it will be lost.

7.4 Chipset

Feature	Options
System Agent (SA) Configuration	submenu
PCH-IO Configuration	submenu

7.4.1 Chipset > System Agent (SA) Configuration

Feature	Options	Description
Memory Configuration	submenu	Memory Configuration Parameters
Graphics Configuration	submenu	
VMD setup menu	submenu	VMD Configuration settings
PCI Express Configuration	submenu	PCI Express Configuration settings
Stop Grant Configuration	**Auto** Manual	Automatic/Manual stop grant configuration
VT-d	Disabled **Enabled**	Check to enable VT-d function on MCH.
Control Iommu Pre-boot Behavior	**Disable IOMMU** Enable IOMMU during boot	Enable IOMMU in Pre-boot environment (If DMAR table is installed in DXE and If VTD_INFO_PPI is installed in PEI.)
X2APIC Opt Out	Disabled **Enabled**	Enable/Disable X2APIC_OPT_OUT bit
DMA Control Guarantee	Disabled **Enabled**	Enable/Disable DMA_CONTROL_GUARANTEE bit
Above 4GB MMIO BIOS assignment	Disabled **Enabled**	Enable/Disable above 4GB MemoryMappedIO BIOS assignment\n\nThis is enabled automatically when Aperture Size is set to 2048MB.

7.4.1.1 Chipset > System Agent (SA) Configuration > Memory Configuration

Feature	Options	Description
Memory Configuration	Info only	
Memory RC Version	Info only	
Memory Frequency	Info only	
tCL-tRCD-tRP-tRAS	Info only	
MC0 Ch0 DIMM 0	Info only	
MC0 CH0 DIMM 1	Info only	
MC1 Ch0 DIMM 0	Info only	
Size		
Number of Ranks		
Manufacturer		
MC 1 Ch0 DIMM 1		
Memory Test on Warm Boot	Disabled **Enabled**	Enable Or Disable Base Memory Test Run on Warm Boot

Maximum Memory Frequency	Auto 1067/1333/1400 1600/1800/1867 2000/2133/2200 2400/2600/2667 2800/2933/3000 3200/3467/3733 **3600** 4000/42004267 4400/4600/4800 5000/5200/5400 5600/5800/6000 6200/6400 10000/12800	Maximum Memory Frequency Selections in Mhz.
ECC Support	Disabled **Enabled**	Enable/disable DDR Ecc Support
Error Injection Address Match	**0**	Address to match against for ECC error injection
Error Injection Mask	**0**	Mask to match against for ECC error injection
Error Injection Insertion Count	**15**	Number of transactions between ECC error injection
Max TOLUD	**Dynamic** 1 GB 1.25 GB 1.5 GB 1.75 GB 2 GB 2.25 GB 2.5 GB 2.75 GB 3 GB 3.25 GB 3.5 GB	Maximum Value of TOLUD. Dynamic assignment would adjust TOLUD automatically based on largest MMIO length of installed graphic controller

Controller 0, Channel 0 Control	Disabled **Enabled**	Controller 0, Channel 0 Control - Enable or Disable Controller 0, Channel 0.
Controller 0, Channel 1 Control	Disabled **Enabled**	Controller 0, Channel 1 Control - Enable or Disable Controller 0, Channel 1.
Controller 1, Channel 0 Control	Disabled **Enabled**	Controller 1, Channel 0 Control - Enable or Disable Controller 1, Channel 0.
Controller 1, Channel 1 Control	Disabled **Enabled**	Controller 1, Channel 1 Control - Enable or Disable Controller 1, Channel 1.

7.4.1.2 Chipset > System Agent (SA) Configuration > Graphics Configuration

Feature	Options	Description
Skip Scaning of External Gfx Card	**Disabled** Enabled	If Enable, it will not scan for External Gfx Card on PEG and PCH PCIE Ports
Primary Display	**Auto** IGFX PEG Slot PCH PCI HG	Select which of IGFX/PEG/PCI Graphics device should be Primary Display Or select HG for Hybrid Gfx.
External Gfx Card Primary Display Configuration	submenu	External Gfx Card Primary Display Configuration
Internal Graphics	Disabled **Enabled**	Keep IGFX enabled based on the setup options.
GTT Size	2MB 4MB **8MB**	Select the GTT Size

Aperture Size	128MB **256MB** 512MB 1024MB	Select the Aperture Size\n\nNote : Above 4GB MMIO BIOS assignment is automatically enabled when selecting > 2048MB aperture. To use this feature, please disable CSM Support.
DVMT Pre-Allocated	0M 32M 64M 96M 128M 160M 4M 8M 12M 16M 20M 24M 28M 32M/F7 36M 40M 44M 48M 52M 56M **60M**	Select DVMT 5.0 Pre-Allocated (Fixed) Graphics Memory size used by the Internal Graphics Device.
DVMT Total Gfx Mem	128M **256M** MAX	Select DVMT5.0 Total Graphic Memory size used by the Internal Graphics Device.
Intel Graphics Pei Display Peim	**Disabled** Enabled	Enable/Disable Pei (Early) Display

Enable Display Audio Link in Pre-OS	Disabled **Enabled**	Enable: Display Audio Link will be enabled in Pre-OS. Disabled: Display Audio Link will be disabled in Pre-OS.

7.4.1.3 Chipset > System Agent (SA) Configuration > VMD Setup Menu

Feature	Options	Description
Enable VMD controller	**Disabled** Enabled	Enable/Disable to VMD controller

7.4.1.4 Chipset > System Agent (SA) Configuration > PCI Express Configuration

Feature	Options	Description
Fia Programming	Disabled **Enabled**	Load Fia Configuration if Enabled for each root port.
Compliance Test Mode	**Disabled** Enabled	Enable when using Compliance Load Board
CDR Relock	Disabled **Enabled**	Enable/Disable CDR Relock
Assertion on Link Down GPIOs	**Disabled** Enabled	GPIO Assertion on Link Down
PCI Express Slot Selection	**M2** CEMx4 slot	Select the PCIe M2 or CEMx4 slot
PCI Express Root Port 1	Submenu	
PCI Express Root Port 2	Submenu	
PCI Express Root Port 3	submenu	

7.4.1.4.1 Chipset > System Agent (SA) Configuration > PCIe Configuration > PCIe Root Port 1

Feature	Options	Description
PCI Express Root Port 1	Disabled **Enabled**	Control the PCI Express Root Port.
Connection Type	Built-in **Slot**	Built-In: a built-in device is connected to this root port. Slot Implemented bit will be clear. Slot: this root port connects to user-accessible slot. Slot Implemented bit will be set.
PCI Express Clock Gating	Disabled **Enabled**	PCI Express Clock Gating Enable/Disable for each root port.
PCH PCIE Power Gating	Disabled **Enabled**	PCH PCI Express Power Gating Enable/Disable for all port
ASPM	**Disabled** Enabled	Set the ASPM Level: Force L0 - Force all links to L0 State : AUTO - BIOS auto configure : DISABLE - Disables ASPM
L1 Substates	**Disabled** Enabled	PCI Express L1 Substate settings.
Gen3 Eq Phase3 Method	**Hardware** Static Coeff.	PCIe Gen3 Equalization Phase 3 Method
Gen4 Eq Phase3 Method	**Hardware** Static Coeff.	PCIe Gen4 Equalization Phase 3 Method
ACS	Disabled **Enabled**	Enable/Disable Access Control Services Extended Capability
PTM	Disabled **Enabled**	Enable/Disable Precision Time Measurement
DPC	**Disabled** Enabled	Enable/Disable Downstream Port Containment

FOM Scoreboard Control Policy	**Auto** Gen3 Gen4 Gen3/Gen4 Gen5	Select the FOM Scoreboard Control Policy, when set to Auto, speed is based on TLS
Multi-VC	Disabled **Enabled**	Enable/Disable Multi Virtual Channel
EDPC	Disabled **Enabled**	Enable/Disable Root port extensions for Downstream Port Containment
URR	Disabled **Enabled**	PCI Express Unsupported Request Reporting Enable/Disable.
FER	Disabled **Enabled**	PCI Express Device Fatal Error Reporting Enable/Disable.
NFER	Disabled **Enabled**	PCI Express Device Non-Fatal Error Reporting Enable/Disable.
CER	Disabled **Enabled**	PCI Express Device Correctable Error Reporting Enable/Disable.
CTO	**Disabled** Enabled	PCI Express Completion Timer TO Enable/Disable.
SEFE	**Disabled** Enabled	Root PCI Express System Error on Fatal Error Enable/Disable.
SENFE	**Disabled** Enabled	Root PCI Express System Error on Non-Fatal Error Enable/Disable.
SECE	**Disabled** Enabled	Root PCI Express System Error on Correctable Error Enable/Disable.
PME SCI	Disabled **Enabled**	PCI Express PME SCI Enable/Disable.

Advanced Error Reporting	Disabled **Enabled**	Advanced Error Reporting Enable/Disable.
PCIe Speed	**Auto** Gen1 Gen2 Gen3 Gen4	Configure PCIe Speed
Enable ClockReq Messaging	**Disabled** Enabled	Enable or Disable ClockReq Messaging
Transmitter Half Swing	**Disabled** Enabled	Transmitter Half Swing Enable/Disable.
Detect Timeout	**0**	The number of milliseconds reference code will wait for link to exit Detect state for enabled ports before assuming there is no device and potentially disabling the port.
P2P Support	**Disabled** Enabled	Program P2P Support Registers according to setup option
SA PCIe LTR Configuration	Info only	
LTR	Disabled **Enabled**	SA PCIE Latency Reporting Enable/Disable
Snoop Latency Override	Disabled Manual **Auto**	Snoop Latency Override for SA PCIE. Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.
Non Snoop Latency Override	Disabled Manual **Auto**	Non Snoop Latency Override for PCH PCIE. Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.
Force LTR Override	**Disabled** Enabled	Force LTR Override for PCH PCIE. Disabled: LTR override values will not be forced. Enable: LTR override values will be forced and LTR messages from the device will be ignored.
LTR Lock	**Disabled** Enabled	PCIE LTR Configuration Lock

CPU PCIe Gen3 HWEQ Config	Info only	
UPTP	**5**	Upstream Port Transmitter Preset
DPTP	**7**	Downstream Port Transmitter Preset
CPU PCIe Gen4 HWEQ Config	Info only	
UPTP	**8**	Upstream Port Transmitter Preset
DPTP	**9**	Downstream Port Transmitter Preset

7.4.1.4.2 Chipset > System Agent (SA) Configuration > PCIe Configuration > PCIe Root Port 2

Feature	Options	Description
PCI Express Root Port 1	Disabled **Enabled**	Control the PCI Express Root Port.
Connection Type	Built-in **Slot**	Built-In: a built-in device is connected to this rootport. SlotImplemented bit will be clear. Slot: this rootport connects to user-accessible slot. SlotImplemented bit will be set.
PCI Express Clock Gating	Disabled **Enabled**	PCI Express Clock Gating Enable/Disable for each root port.
PCH PCIE Power Gating	Disabled **Enabled**	PCH PCI Express Power Gating Enable/Disable for all port
ASPM	**Disabled** Enabled	Set the ASPM Level: Force L0 - Force all links to L0 State : AUTO - BIOS auto configure : DISABLE - Disables ASPM
L1 Substates	**Disabled** Enabled	PCI Express L1 Substates settings.
Gen3 Eq Phase3 Method	**Hardware** Static Coeff.	PCIe Gen3 Equalization Phase 3 Method
Gen4 Eq Phase3 Method	**Hardware** Static Coeff.	PCIe Gen4 Equalization Phase 3 Method

ACS	Disabled **Enabled**	Enable/Disable Access Control Services Extended Capability
PTM	Disabled **Enabled**	Enable/Disable Precision Time Measurement
DPC	**Disabled** Enabled	Enable/Disable Downstream Port Containment
FOM Scoreboard Control Policy	**Auto** Gen3 Gen4 Gen3/Gen4 Gen5	Select the FOM Scoreboard Control Policy, when set to Auto, speed is based on TLS
Multi-VC	Disabled **Enabled**	Enable/Disable Multi Virtual Channel
EDPC	Disabled **Enabled**	Enable/Disable Rootport extensions for Downstream Port Containment
URR	Disabled **Enabled**	PCI Express Unsupported Request Reporting Enable/Disable.
FER	Disabled **Enabled**	PCI Express Device Fatal Error Reporting Enable/Disable.
NFER	Disabled **Enabled**	PCI Express Device Non-Fatal Error Reporting Enable/Disable.
CER	Disabled **Enabled**	PCI Express Device Correctable Error Reporting Enable/Disable.
CTO	**Disabled** Enabled	PCI Express Completion Timer TO Enable/Disable.
SEFE	**Disabled** Enabled	Root PCI Express System Error on Fatal Error Enable/Disable.

SENFE	**Disabled** Enabled	Root PCI Express System Error on Non-Fatal Error Enable/Disable.
SECE	**Disabled** Enabled	Root PCI Express System Error on Correctable Error Enable/Disable.
PME SCI	Disabled **Enabled**	PCI Express PME SCI Enable/Disable.
Advanced Error Reporting	Disabled **Enabled**	Advanced Error Reporting Enable/Disable.
PCIe Speed	**Auto** Gen1 Gen2 Gen3 Gen4	Configure PCIe Speed
Enable ClockReq Messaging	**Disabled** Enabled	Enable or Disable ClockReq Messaging
Transmitter Half Swing	**Disabled** Enabled	Transmitter Half Swing Enable/Disable.
Detect Timeout	**0**	The number of milliseconds reference code will wait for link to exit Detect state for enabled ports before assuming there is no device and potentially disabling the port.
P2P Support	**Disabled** Enabled	Program P2P Support Registers according to setup option
SA PCIe LTR Configuration	Info only	
LTR	Disabled **Enabled**	SA PCIE Latency Reporting Enable/Disable
Snoop Latency Override	Disabled Manual **Auto**	Snoop Latency Override for SA PCIE. Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.

Non Snoop Latency Override	Disabled Manual **Auto**	Non Snoop Latency Override for PCH PCIE.Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.
Force LTR Override	**Disabled** Enabled	Force LTR Override for PCH PCIE. Disabled: LTR override values will not be forced. Enable: LTR override values will be forced and LTR messages from the device will be ignored.
LTR Lock	**Disabled** Enabled	PCIE LTR Configuration Lock
CPU PCIe Gen3 HWEQ Config	Info only	
UPTP	**7**	Upstream Port Transmitter Preset
DPTP	**7**	Downstream Port Transmitter Preset
CPU PCIe Gen4 HWEQ Config	Info only	
UPTP	**7**	Upstream Port Transmitter Preset
DPTP	**5**	Downstream Port Transmitter Preset
CPU PCIe Gen5 HWEQ Config	Info only	
UPTP	**5**	Upstream Port Transmitter Preset
DPTP	**7**	Downstream Port Transmitter Preset

7.4.1.4.3 Chipset > System Agent (SA) Configuration > PCIe Configuration > PCIe Root Port 3

Feature	Options	Description
PCI Express Root Port 1	Disabled **Enabled**	Control the PCI Express Root Port.
Connection Type	Built-in **Slot**	Built-In: a built-in device is connected to this rootport. SlotImplemented bit will be clear. Slot: this rootport connects to user-accessible slot. SlotImplemented bit will be set.
PCI Express Clock Gating	Disabled **Enabled**	PCI Express Clock Gating Enable/Disable for each root port.

PCH PCIE Power Gating	Disabled **Enabled**	PCH PCI Express Power Gating Enable/Disable for all port
ASPM	**Disabled** Enabled	Set the ASPM Level: Force L0 - Force all links to L0 State : AUTO - BIOS auto configure : DISABLE - Disables ASPM
L1 Substates	**Disabled** Enabled	PCI Express L1 Substates settings.
Gen3 Eq Phase3 Method	**Hardware** Static Coeff.	PCIe Gen3 Equalization Phase 3 Method
Gen4 Eq Phase3 Method	**Hardware** Static Coeff.	PCIe Gen4 Equalization Phase 3 Method
ACS	Disabled **Enabled**	Enable/Disable Access Control Services Extended Capability
PTM	Disabled **Enabled**	Enable/Disable Precision Time Measurement
DPC	**Disabled** Enabled	Enable/Disable Downstream Port Containment
FOM Scoreboard Control Policy	**Auto** Gen3 Gen4 Gen3/Gen4 Gen5	Select the FOM Scoreboard Control Policy, when set to Auto, speed is based on TLS
Multi-VC	Disabled **Enabled**	Enable/Disable Multi Virtual Channel
EDPC	Disabled **Enabled**	Enable/Disable Rootport extensions for Downstream Port Containment
URR	Disabled **Enabled**	PCI Express Unsupported Request Reporting Enable/Disable.

FER	Disabled **Enabled**	PCI Express Device Fatal Error Reporting Enable/Disable.
NFER	Disabled **Enabled**	PCI Express Device Non-Fatal Error Reporting Enable/Disable.
CER	Disabled **Enabled**	PCI Express Device Correctable Error Reporting Enable/Disable.
CTO	**Disabled** Enabled	PCI Express Completion Timer TO Enable/Disable.
SEFE	**Disabled** Enabled	Root PCI Express System Error on Fatal Error Enable/Disable.
SENFE	**Disabled** Enabled	Root PCI Express System Error on Non-Fatal Error Enable/Disable.
SECE	**Disabled** Enabled	Root PCI Express System Error on Correctable Error Enable/Disable.
PME SCI	Disabled **Enabled**	PCI Express PME SCI Enable/Disable.
Advanced Error Reporting	Disabled **Enabled**	Advanced Error Reporting Enable/Disable.
PCIe Speed	**Auto** Gen1 Gen2 Gen3 Gen4	Configure PCIe Speed
Enable ClockReq Messaging	**Disabled** Enabled	Enable or Disable ClockReq Messaging
Transmitter Half Swing	**Disabled** Enabled	Transmitter Half Swing Enable/Disable.

Detect Timeout	**0**	The number of milliseconds reference code will wait for link to exit Detect state for enabled ports before assuming there is no device and potentially disabling the port.
P2P Support	**Disabled** Enabled	Program P2P Support Registers according to setup option
SA PCIe LTR Configuration	Info only	
LTR	Disabled **Enabled**	SA PCIE Latency Reporting Enable/Disable
Snoop Latency Override	Disabled Manual **Auto**	Snoop Latency Override for SA PCIE. Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.
Non Snoop Latency Override	Disabled Manual **Auto**	Non Snoop Latency Override for PCH PCIE.Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.
Force LTR Override	**Disabled** Enabled	Force LTR Override for PCH PCIE. Disabled: LTR override values will not be forced. Enable: LTR override values will be forced and LTR messages from the device will be ignored.
LTR Lock	**Disabled** Enabled	PCIE LTR Configuration Lock
CPU PCIe Gen3 HWEQ Config	Info only	
UPTP	**7**	Upstream Port Transmitter Preset
DPTP	**7**	Downstream Port Transmitter Preset
CPU PCIe Gen4 HWEQ Config	Info only	
UPTP	**7**	Upstream Port Transmitter Preset
DPTP	**5**	Downstream Port Transmitter Preset
CPU PCIe Gen5 HWEQ Config	Info only	
UPTP	**5**	Upstream Port Transmitter Preset
DPTP	**7**	Downstream Port Transmitter Preset

7.4.2 Chipset > PCH-IO Configuration

Feature	Options	Description
PCI Express Configuration	submenu	PCI Express Configuration settings
SATA Configuration	submenu	SATA Device Options settings
USB Configuration	submenu	USB Configuration settings
Security Configuration	submenu	Security Configuration settings
HD Audio Configuration	submenu	HD Audio Configuration Settings
Seriallo Configuration	submenu	Seriallo Configuration Settings
TSN GBE Configuration	Info only	
Port 80h Redirection	**LPC Bus** PCIE Bus	Control where the Port 80h cycles are sent.
Enhance Port 80h LPC Decoding	Disabled **Enabled**	Support the word/dword decoding of port 80h behind LPC
Enable TCO Timer	**Disabled** Enabled	Enable/Disable TCO timer. When disabled, it disables PCH ACPI timer, stops TCO timer, and ACPI WDAT table will not be published.
Pcie Pll SSC	**Auto** 0.0% 0.1% 0.2% 0.3% 0.4% 0.5% 0.6% 0.7% 0.8% 0.9% 1.0% 1.1%	Pcie Pll SSC percentage.AUTO - Keep hw default, no BIOS override. Range is 0.0%-2.0%.

Feature	Options	Description
	1.2% 1.3% 1.4% 1.5% 1.6% 1.7% 1.8% 1.9% 2.0% Disable	
SPD Write Disable	**TRUE** FALSE	Enable/Disable setting SPD Write Disable. For security recommendations, SPD write disable bit must be set.

7.4.2.1 Chipset > PCH-IO Configuration > PCIe Configuration

Feature	Options	Description
DMI Link ASPM Control	**Disabled** L1 Auto	The control of Active State Power Management of the DMI Link.
Port8xh Decode	**Disabled** Enabled	PCI Express Port8xh Decode Enable/Disable.
PCH PCIE Clock Gating	Disabled **Enabled**	PCH PCI Express Clock Gating Enable/Disable for all port
PCH PCIE Power Gating	Disabled **Enabled**	PCH PCI Express Power Gating Enable/Disable for all port

PCIE Ports 1-4 Configuration	4x1 Port 1x2 2x1 Port 2x2 Port **1x4 Port**	Notes: Please make sure the system boots completed after changing the configuration. Do Not Attempt to Shut Down Your Computer, doing that may lead to system malfunction.
PCIE Ports 5-8 Configuration	**4x1 Port** 1x2 2x1 Port 2x2 Port 1x4 Port	Notes: Please make sure the system boots completed after changing the configuration. Do Not Attempt to Shut Down Your Computer, doing that may lead to system malfunction.
PCIE Ports 13-16 Configuration	4x1 Port 1x2 2x1 Port 2x2 Port **1x4 Port**	Notes: Please make sure the system boots completed after changing the configuration. Do Not Attempt to Shut Down Your Computer, doing that may lead to system malfunction.
PCIE Ports 21-24 Configuration	4x1 Port 1x2 2x1 Port 2x2 Port **1x4 Port**	Notes: Please make sure the system boots completed after changing the configuration. Do Not Attempt to Shut Down Your Computer, doing that may lead to system malfunction.
PCIE Ports 25-28 Configuration	4x1 Port 1x2 2x1 Port 2x2 Port **1x4 Port**	Notes: Please make sure the system boots completed after changing the configuration. Do Not Attempt to Shut Down Your Computer, doing that may lead to system malfunction.
PCI Express Root Port 1	submenu	PCI Express Root Port Settings.
PCI Express Root Port 2	submenu	PCI Express Root Port Settings.
PCI Express Root Port 3	submenu	PCI Express Root Port Settings.
PCI Express Root Port 4	submenu	PCI Express Root Port Settings.
PCI Express Root Port 5	submenu	PCI Express Root Port Settings.
PCI Express Root Port 6	submenu	PCI Express Root Port Settings.
PCI Express Root Port 7	submenu	PCI Express Root Port Settings.
PCI Express Root Port 8	submenu	PCI Express Root Port Settings.

PCI Express Root Port 13	submenu	PCI Express Root Port Settings.
PCI Express Root Port 14	submenu	PCI Express Root Port Settings.
PCI Express Root Port 15	submenu	PCI Express Root Port Settings.
PCI Express Root Port 16	submenu	PCI Express Root Port Settings.
PCI Express Root Port 21	submenu	PCI Express Root Port Settings.
PCI Express Root Port 22	submenu	PCI Express Root Port Settings.
PCI Express Root Port 23	submenu	PCI Express Root Port Settings.
PCI Express Root Port 24	submenu	PCI Express Root Port Settings.
PCI Express Root Port 25	submenu	PCI Express Root Port Settings.
PCI Express Root Port 26	submenu	PCI Express Root Port Settings.
PCI Express Root Port 27	submenu	PCI Express Root Port Settings.
PCI Express Root Port 28	submenu	PCI Express Root Port Settings.

7.4.2.1.1 Chipset >PCH-IO Configuration > PCIe Configuration > PCIe Root Port 1/5/6/7/8/13/14/15/16/21/22/23/24/25/26/27/28

Feature	Options	Description
PCI Express Root Port 1/5/6/7/8/13/14/15/16/21/22/23/24/25/26/27/28	Disabled **Enabled**	Control the PCI Express Root Port.
Connection Type	Built-in **Slot**	Built-In: a built-in device is connected to this rootport. SlotImplemented bit will be clear. Slot: this rootport connects to user-accessible slot. SlotImplemented bit will be set.
ASPM	**Disabled** Enabled	Set the ASPM Level: Force L0 - Force all links to L0 State : AUTO - BIOS auto configure : DISABLE - Disables ASPM
L1 Substates	**Disabled** Enabled	PCI Express L1 Substates settings.

L1 Low	**Disabled** Enabled	PCI Express L1 Low Substate Enable/Disable.
ACS	Disabled **Enabled**	Enable/Disable Access Control Services Extended Capability
PTM	Disabled **Enabled**	Enable/Disable Precision Time Measurement
DPC	**Disabled** Enabled	Enable/Disable Downstream Port Containment
EDPC	Disabled **Enabled**	Enable/Disable Rootport extensions for Downstream Port Containment
URR	Disabled **Enabled**	PCI Express Unsupported Request Reporting Enable/Disable.
FER	Disabled **Enabled**	PCI Express Device Fatal Error Reporting Enable/Disable.
NFER	Disabled **Enabled**	PCI Express Device Non-Fatal Error Reporting Enable/Disable.
CER	Disabled **Enabled**	PCI Express Device Correctable Error Reporting Enable/Disable.
SEFE	**Disabled** Enabled	Root PCI Express System Error on Fatal Error Enable/Disable.
SENFE	**Disabled** Enabled	Root PCI Express System Error on Non-Fatal Error Enable/Disable.
SECE	**Disabled** Enabled	Root PCI Express System Error on Correctable Error Enable/Disable.
PME SCI	Disabled **Enabled**	PCI Express PME SCI Enable/Disable.
Hot Plug	**Disabled** Enabled	PCI Express Hot Plug Enable/Disable.

Advanced Error Reporting	Disabled **Enabled**	Advanced Error Reporting Enable/Disable.
PCIe Speed	**Auto** Gen1 Gen2 Gen3 Gen4	Configure PCIe Speed
Transmitter Half Swing	**Disabled** Enabled	Transmitter Half Swing Enable/Disable.
Detect Timeout	**0**	The number of milliseconds reference code will wait for link to exit Detect state for enabled ports before assuming there is no device and potentially disabling the port.
Extra Bus Reserved	**0**	Extra Bus Reserved (0-7) for bridges behind this Root Bridge.
Reserved Memory	**10**	Reserved Memory for this Root Bridge (1-20) MB
Reserved I/O	**4**	Reserved I/O (4K/8K/12K/16K/20K) Range for this Root Bridge.
PCH PCIe LTR Configuration	Info only	
LTR	Disabled **Enabled**	PCH PCIE Latency Reporting Enable/Disable
Snoop Latency Override	Disabled Manual **Auto**	Snoop Latency Override for PCH PCIE.Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.
Non Snoop Latency Override	Disabled Manual **Auto**	Non Snoop Latency Override for PCH PCIE.Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.
LTR Lock	**Disabled** Enabled	PCIE LTR Configuration Lock
Peer Memory Write Enable	**Disabled** Enabled	Peer Memory Write Enable/Disable

7.4.2.2 Chipset > PCH-IO Configuration > SATA Configuration

Feature	Options	Description
SATA Controller(s)	Disabled **Enabled**	Enable/Disable SATA Device.
SATA Mode Selection	**AHCI**	Determines how SATA controller(s) operate.
SATA Controller Speed	Default Gen1 **Gen2** Gen3	Indicates the maximum speed the SATA controller can support.
SATA Test Mode	**Disabled** Enabled	Test Mode Enable/Disable (Loop Back).
Aggressive LPM Support	Disabled **Enabled**	Enable PCH to aggressively enter link power state.
Serial ATA Port 4	**Info only**	
Software Preserve	**Info only**	
Port 4	Disabled **Enabled**	Enable or Disable SATA Port
Hot Plug	**Disabled** Enabled	Designates this port as Hot Pluggable.
Configured as eSATA	Info only	
External	**Disabled** Enabled	Marks this port as external.
Spin Up Device	**Disabled** Enabled	If enabled for any of ports Staggerred Spin Up will be performed and only the drives which have this option enabled will spin up at boot. Otherwise all drives spin up at boot.
SATA Device Type	**Hard Disk Drive** Solid State Drive	Identify the SATA port is connected to Solid State Drive or Hard Disk Drive

Topology	**Unknown** ISATA Direct Connect Flex M2	Identify the SATA Topology if it is Default or ISATA or Flex or DirectConnect or M2
SATA Port 4 DevSlp	Disabled **Enabled**	Enable/Disable SATA Port 4 DevSlp. For DevSlp to work, both hard drive and SATA port need to support DevSlp function, otherwise an unexpected behavior might happen. Please check board design before enabling it.
DITO Configuration	**Disabled** Enabled	Enable/Disable DITO Configuration
DITO Value	**625**	DITO Value
DM Value	**15**	DM Value
Serial ATA Port 5	Info only	
Software Preserve	Info only	
Port 5	Disabled **Enabled**	Enable or Disable SATA Port
Hot Plug	**Disabled** Enabled	Designates this port as Hot Pluggable.
Configured as eSATA	Info only	
External	**Disabled** Enabled	Marks this port as external.
Spin Up Device	**Disabled** Enabled	If enabled for any of ports Staggerred Spin Up will be performed and only the drives which have this option enabled will spin up at boot. Otherwise all drives spin up at boot.
SATA Device Type	**Hard Disk Drive** Solid State Drive	Identify the SATA port is connected to Solid State Drive or Hard Disk Drive

Topology	**Unknown** ISATA Direct Connect Flex M2	Identify the SATA Topology if it is Default or ISATA or Flex or DirectConnect or M2
SATA Port 5 DevSlp	Disabled **Enabled**	Enable/Disable SATA Port 5 DevSlp. For DevSlp to work, both hard drive and SATA port need to support DevSlp function, otherwise an unexpected behavior might happen. Please check board design before enabling it.
DITO Configuration	**Disabled** Enabled	Enable/Disable DITO Configuration
DITO Value	**625**	DITO Value
DM Value	**15**	DM Value

7.4.2.3 Chipset > PCH-IO Configuration > USB Configuration

Feature	Options	Description
xDCI Support	**Disabled** Enabled	Enable/Disable xDCI (USB OTG Device).
USB PDO Programming	Disabled **Enabled**	Select 'Enabled' if Port Disable Override functionality is used.
USB Overcurrent	Disabled **Enabled**	Select 'Disabled' for pin-based debug. If pin-based debug is enabled but USB overcurrent is not disabled, USB DbC does not work.
USB Overcurrent Lock	Disabled **Enabled**	Select 'Enabled' if Overcurrent functionality is used. Enabling this will make xHCI controller consume the Overcurrent mapping data
USB Audio Offload	Disabled **Enabled**	Enable/Disable USB Audio Offload functionality
Enable HSII on xHCI	Disabled **Enabled**	Enable/Disable HSII feature. It may lead to increased power consumption.
USB3.1 Portx Speed Selection	**0**	Port Selection value in decimal for Gen1; Default - Gen2; Bit 0 corresponds to Port 0 and so on

USB Port Disable Override	**Disabled** Select Per-Pin	Selectively Enable/Disable the corresponding USB port from reporting a Device Connection to the controller.

7.4.2.4 Chipset > PCH-IO Configuration > Security Configuration

Feature	Options	Description
RTC Memory Lock	Disabled **Enabled**	Enable will lock bytes 38h-3Fh in the lower/upper 128-byte bank of RTC RAM
BIOS Lock	**Disabled** Enabled	Enable/Disable the PCH BIOS Lock Enable feature. Required to be enabled to ensure SMM protection of flash.
Force unlock on all GPIO pads	**Disabled** Enabled	If Enabled BIOS will force all GPIO pads to be in unlocked state

7.4.2.5 Chipset > PCH-IO Configuration > HD Audio Configuration

Feature	Options	Description
HD Audio	**Disabled** Enabled	Control Detection of the HD-Audio device.\n\nDisabled = HDA will be unconditionally disabled\n\nEnabled = HDA will be unconditionally enabled.

7.4.2.6 Chipset > PCH-IO Configuration > Serial IO Configuration

Feature	Options	Description
I2C0 Controller	Disabled **Enabled**	Enables/Disables Serial IO Controller If given device is Function 0 PSF disabling is skipped. PSF default will remain and device PCI CFG Space will still be visible. This is needed to allow PCI enumerator access functions above 0 in a multifunction device. The following devices depend on each other:I2C0 and I2C1,2,3 UART0 and UART1,SPI0,1 UART2 and I2C4,5 UART 0 (00:30:00) cannot be disabled when:1. Child device is enabled like CNVi Bluetooth (_SB.PC00.UA00.BTH0)UART 0 (00:30:00) cannot be enabled when:1. I2S Audio codec is enabled (_SB.PC00.I2C0.HDAC)

I2C1 Controller	Disabled **Enabled**	Enables/Disables Serial IO Controller If given device is Function 0 PSF disabling is skipped. PSF default will remain and device PCI CFG Space will still be visible. This is needed to allow PCI enumerator access functions above 0 in a multifunction device. The following devices depend on each other:I2C0 and I2C1,2,3 UART0 and UART1,SPI0,1 UART2 and I2C4,5 UART 0 (00:30:00) cannot be disabled when:1. Child device is enabled like CNVi Bluetooth (_SB.PC00.UA00.BTH0)UART 0 (00:30:00) cannot be enabled when:1. I2S Audio codec is enabled (_SB.PC00.I2C0.HDAC)
UART0 Controller	**Disabled** Enabled	Enables/Disables Serial IO Controller If given device is Function 0 PSF disabling is skipped. PSF default will remain and device PCI CFG Space will still be visible. This is needed to allow PCI enumerator access functions above 0 in a multifunction device. The following devices depend on each other:I2C0 and I2C1,2,3 UART0 and UART1,SPI0,1 UART2 and I2C4,5 UART 0 (00:30:00) cannot be disabled when:1. Child device is enabled like CNVi Bluetooth (_SB.PC00.UA00.BTH0)UART 0 (00:30:00) cannot be enabled when:1. I2S Audio codec is enabled (_SB.PC00.I2C0.HDAC)
UART1 Controller	**Disabled** Enabled	Enables/Disables Serial IO Controller If given device is Function 0 PSF disabling is skipped. PSF default will remain and device PCI CFG Space will still be visible. This is needed to allow PCI enumerator access functions above 0 in a multifunction device. The following devices depend on each other:I2C0 and I2C1,2,3 UART0 and UART1,SPI0,1 UART2 and I2C4,5 UART 0 (00:30:00) cannot be disabled when:1. Child device is enabled like CNVi Bluetooth (_SB.PC00.UA00.BTH0)UART 0 (00:30:00) cannot be enabled when:1. I2S Audio codec is enabled (_SB.PC00.I2C0.HDAC)
GPIO IRQ Route	**IRQ14** IRQ15	Route all GPIOs to one of the IRQ.

7.5 Security

Feature	Options	Description
Administrator Password	Enter password	Set Administrator Password
User Password	Enter password	Set User Password
Secure Boot	submenu	

7.5.1 Security > Secure Boot Menu

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 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

7.6 Boot

7.6.1 Boot Configuration

Feature	Options	Description
Boot Configuration	Info only	
Setup Prompt Timeout	**1**	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 active boot option. Has no effect for BBS boot options.
SATA Support	Last Boot SATA Devices Only **All Sata Devices**	If Last Boot SATA Devices Only, Only last boot SATA device will be available in Post. If All Sata Devices, all SATA devices will be available in OS and Post.
VGA Support	Auto **EFI Driver**	If Auto, only install Legacy OpRom with Legacy OS and logo would 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 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 Link** Enabled	If Disabled, PS2 devices will be skipped.
NetWork Stack Driver Support	**Disabled Link** Enabled	If Disabled, NetWork Stack Driver will be skipped.
Redirection Support	Disabled **Enabled**	If disable, Redirection function will be disabled.

7.7 Save & Exit

7.7.1 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 Options	Info only	
Save Changes		Save changes done so far to any of the setup options.
Discard Changes		Discard Changes done so far to any of the setup options.
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.

8. BIOS Checkpoints, Beep Codes

A status code is a data value used to provide diagnostic information about the boot process. Progress codes are status codes that signify successful progression to an initialization step. Error codes signify error conditions encountered in the process of system initialization. The Aptio 5.x core can be configured to send status codes to a variety of sources. The two most commonly used types of status codes are checkpoint codes and beep codes. Checkpoint codes are byte length data values. Checkpoints are typically output to I/O port 80h, but the Aptio 5.x core can be configured to send checkpoints to a variety of sources. The Aptio 5.x core outputs checkpoints throughout the boot process to indicate the task the system is currently executing. Checkpoints are very useful in aiding software developers or technicians in debugging problems that occur during the pre-boot process on production hardware. A beep code is a series of short sound signals. Beep codes are typically error codes that do not occur during normal boot process.

Note: Beep codes are not just sounds generated during the boot process. Some firmware components may use sounds to notify the user about other events such as detection of a hot-pluggable device. These sounds are typically generated using a frequency that is different from the frequency of the beep codes.

Viewing Checkpoints

Checkpoints generated by the Aptio firmware can be viewed using a PCI checkpoint card, also referred to as a "POST Card" or "POST Diagnostic Card". These PCI add-on cards show the value of I/O port 80h on an LED display.

Aptio V Checkpoint and Beep Codes

You can download the Aptio V Checkpoint and Beep Codes from the AMI website at: www.ami.com/download/aptio-v-checkpoint-and-beep-codes

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
Progress Codes	
0x01	Power on. Reset type detection (soft/hard).

Status Code	Description
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 PEI Phase

Status Code	Description
Progress Codes	
0x10	PEI Core is started
0x11	Pre-memory CPU initialization is started
0x12 – 0x14	Reserved for CPU

Status Code	Description
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
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

Status Code	Description
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
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

8.2.2.1 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

8.2.3 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

Status Code	Description
0x9E – 0x9F	Reserved for future AMI codes
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

Status Code	Description
0xB5	PCI bus hot plug
0xB6	Clean-up of NVRAM
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

8.2.4 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)

8.2.5 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.

Status Code	Description
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 10 IoT Enterprise 2021 LTSC 64-bit

9.2 Ubuntu 20.04

9.3 Yocto Project* BSP tool-based embedded Linux distribution

https://github.com/ADLINK/meta-adlink-x86-64bit (TBC)

10. Mechanical

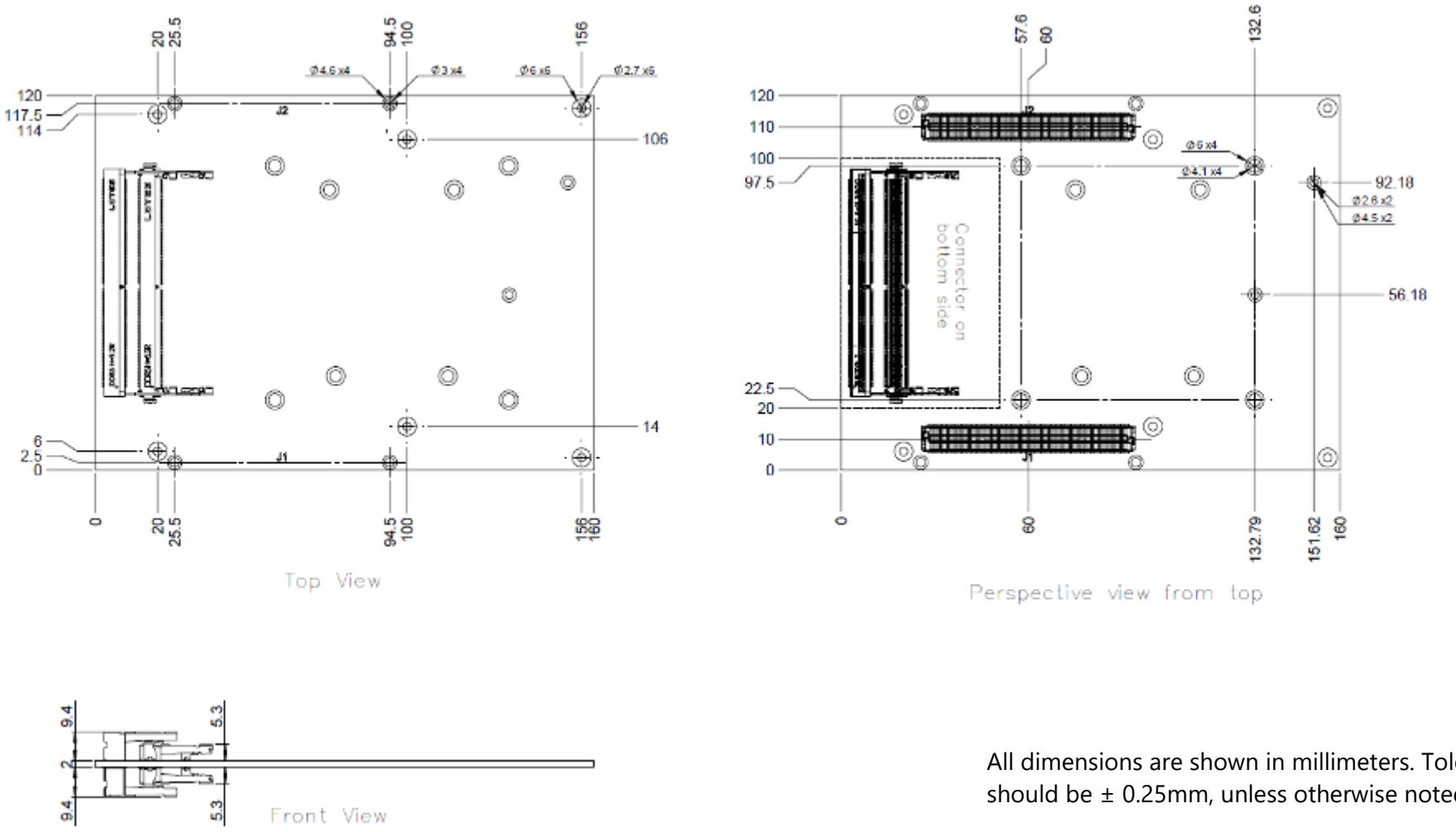


Figure 5 – Module mechanical dimensions

All dimensions are shown in millimeters. Tolerances should be ± 0.25mm, unless otherwise noted.

Dimensions: mm

11. Thermal

11.1 Thermal Solutions

11.1.1 Heatspreader: HTS

Dimensions: mm

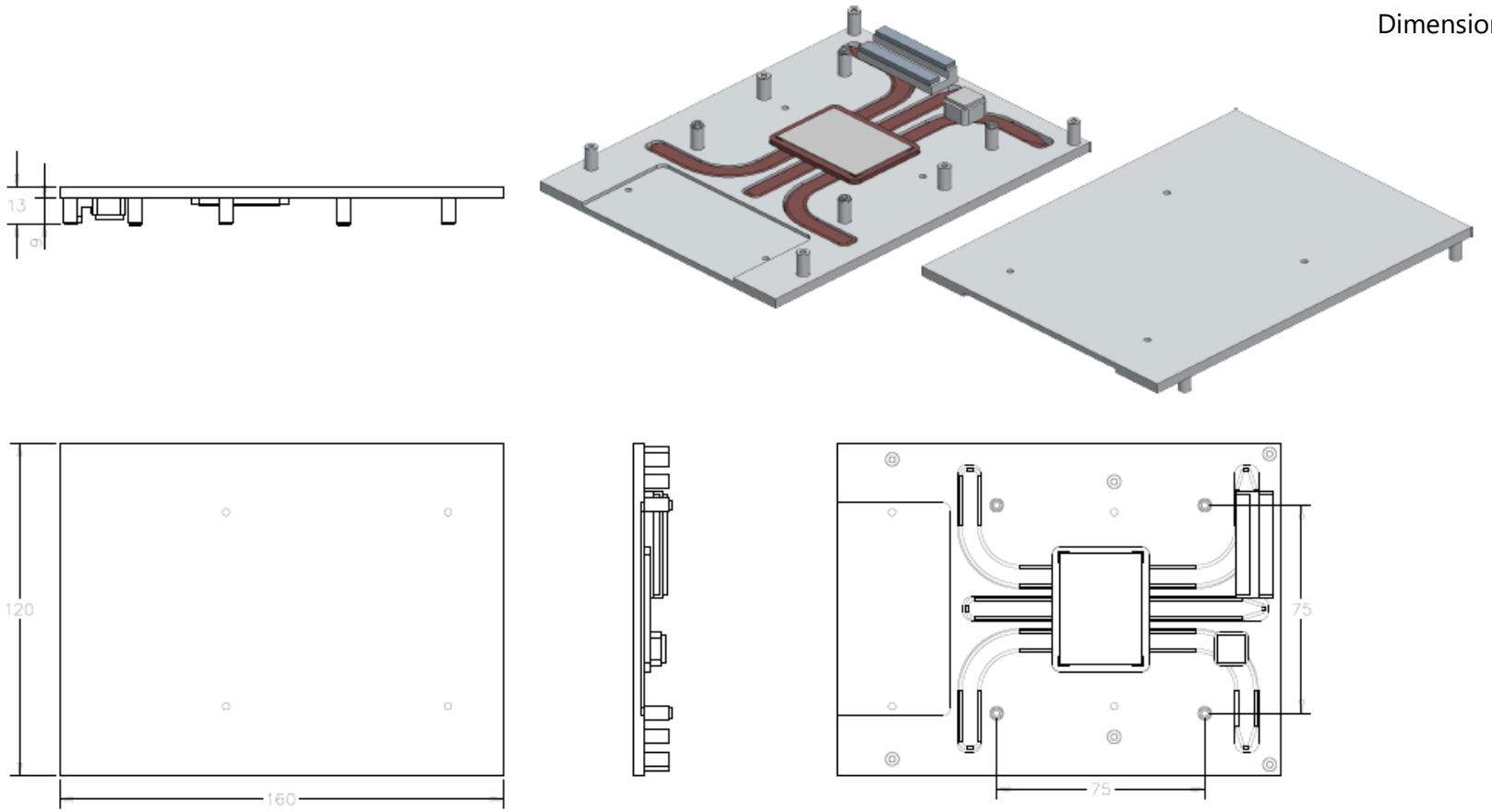


Figure 6 – Heatspreader: HTS

11.1.2 Heatsink: THS-BL

Dimensions: mm

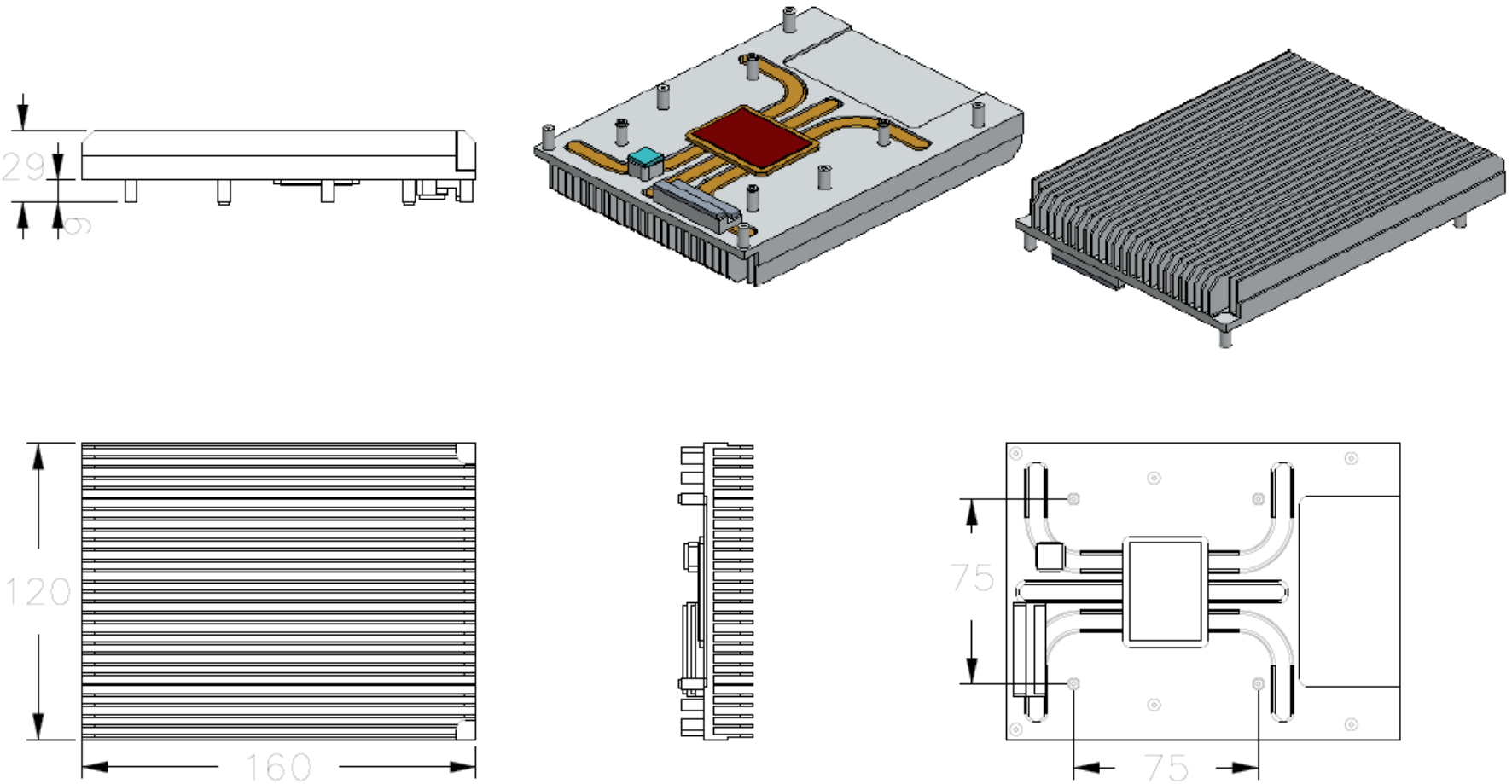


Figure 7 – Heatsink: THS-BL

11.1.3 Heatsink with Fan: THSF-BL-S

Dimensions: mm

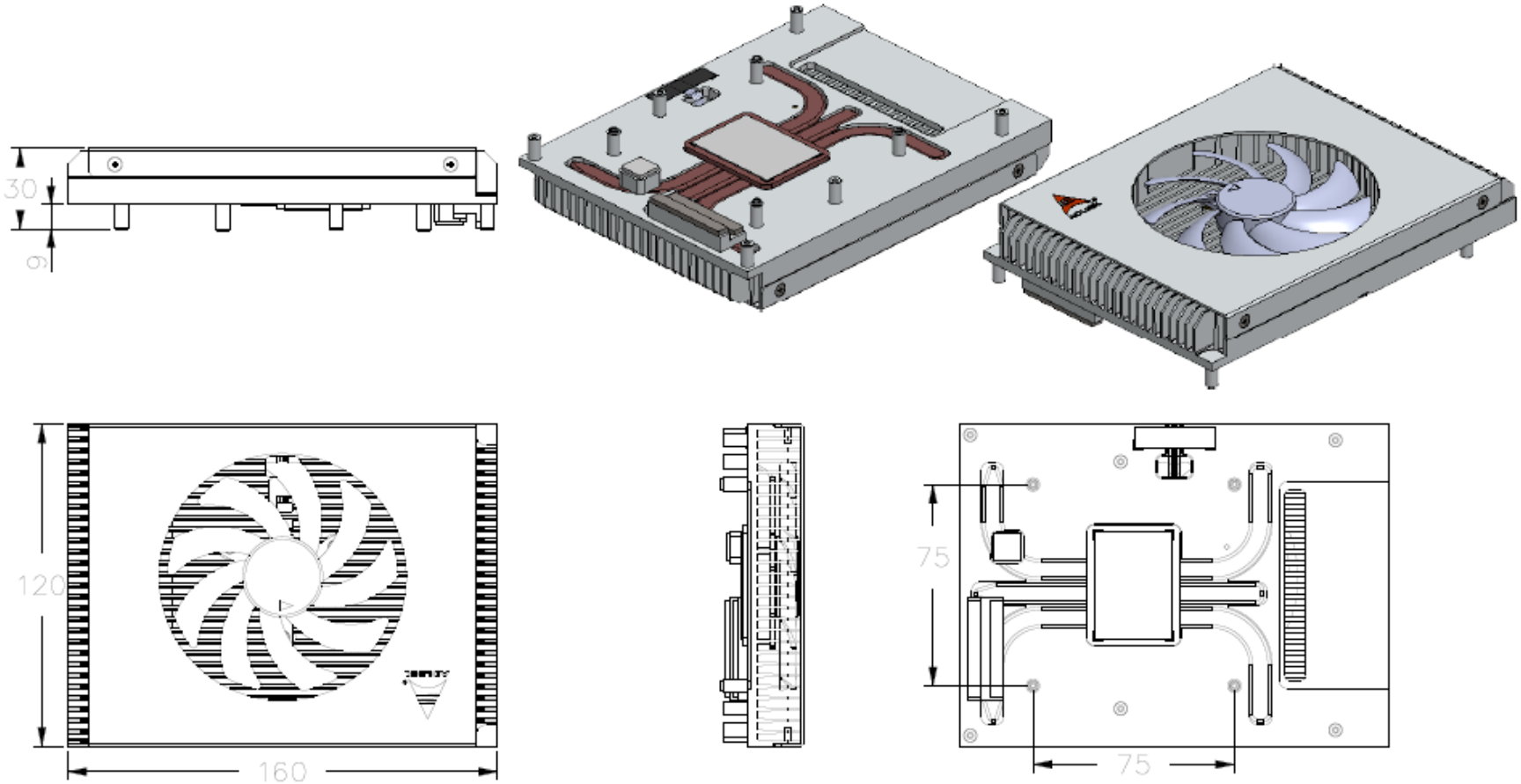


Figure 8 – Heatsink with Fan: THSF-BL-S