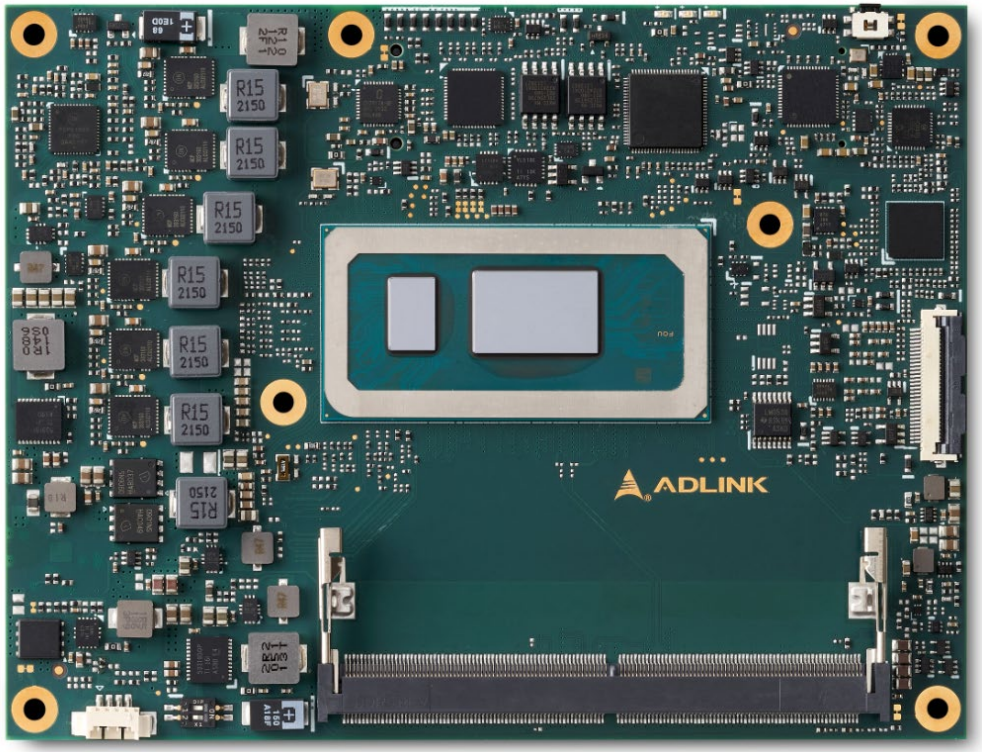
Express-ADP

User's Guide



COM Express®

Revision: Rev. 1.1
Date: 2024-06-17
Part Number: 50M-72139-1010

ADLINK
LEADING EDGE COMPUTING

Revision History

Revision	Description	Date	Author
1.0	Initial release	2023-11-15	CC
1.1	BIOS tables and graphics and PCIe suitability added	2024-06-17	AL

Preface

Disclaimer

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

Environmental Responsibility

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

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

Trademarks

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

Copyright © 2024 ADLINK Technology Incorporated

Safety Instructions

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

Read these safety instructions carefully.

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

Conventions

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

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

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

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

Getting Service

Ask an Expert: http://askanexpert.adlinktech.com

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

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

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

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

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

Table of Contents

List of Figures

1. Introduction

The Express-ADP is a COM.0 R3.1 compliant COM Express® Basic Size Type 6 module based on 12th Gen Intel® Core™ and Intel® Celeron® SoC utilizing Intel's advanced hybrid architecture (formerly "Alder Lake-P"). It features up to 6 Performance-cores (P-cores) for IoT workloads, maximum responsiveness and 8 Efficient-cores (E-cores) for offload multi-tasking at background, and is integrated with up to 96 Intel® Iris® Xe high performance graphics cores that boost productivity and fueling IoT innovation across a wide variety of deployments. Typical industries in need of such high performance, low power characteristics include industrial automation and control, medical ultra sound, image processing and analysis, high-speed video encoding and streaming, predictive traffic analysis, and multi camera-based AI.

The Express-ADP supports up to 64GB (2x 32GB) DDR5 memory, maximum 4800 MT/s memory frequency at two SODIMM sockets, and suits power envelopes ranging across 15, 28, and 45W, making it well suited for mission-critical applications for both stationary and mobile edge use cases.

The integrated Intel® Iris® Xe Graphics includes features such as OpenGL 4.5, DirectX 12, OpenCL 2.1/2.0/1.2, Intel® Clear Video HD Technology, and DirectX Video Acceleration (DXVA) support for full H.265/HEVC 10-bit, VP9 hardware codecs. In addition, High Dynamic Range is supported for enhanced picture color and quality, and digital content protection has been upgraded to HDCP 2.3. Graphics outputs include LVDS and three DDI ports supporting HDMI/DVI/DisplayPort and eDP/VGA as a build option, with a maximum of four 4K displays supported. In addition, maximum 2x USB4 that can transfer media and data through a single tunnel is a build option supported by project basis in place of DDI 1/2. The Express-ADP is specifically designed for customers with high-performance processing graphics requirements who want to outsource the custom core logic of their systems for reduced development time. Adding to the onboard integrated graphics, a multiplexed 16 PCIe Gen4 graphics bus at one x8 plus two x4 configuration is available for discrete graphics expansion.

Input/output features include up to eight PCIe Gen3 lanes via PCIe switch that can be used for NVMe SSD, allowing application access to the highest speed storage solutions, as well as a single onboard 2.5Gigabit Ethernet port with optional Time Sensitive Network (TSN) support, four USB 3.2 Gen2/2.0 ports, four USB 2.0 ports, and two SATA 6 Gb/s ports. Optional onboard PCIe NVMe SSD is offered by project basis. Support is provided for SMBus and I2C. 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

12th Gen Intel® Core™ Processor (formerly Alder Lake-P)

- Intel® Core™ i7-12800HE, 2.4(4.6) GHz, 24MB, 45W(35W cTDP), 6P+8E/20T
- Intel® Core™ i5-12600HE, 2.5(4.5) GHz, 18MB, 45W(35W cTDP), 4P+8E/16T
- Intel® Core™ i3-12300HE, 1.9(4.3) GHz, 12MB, 45W(35W cTDP), 4P+4E/12T
- Intel® Core™ i7-1270PE, 1.8(4.5) GHz, 18MB, 28W(20W cTDP), 4P+8E/16T
- Intel® Core™ i5-1250PE, 1.7(4.4) GHz, 12MB, 28W(20W cTDP), 4P+8E/16T
- Intel® Core™ i3-1220PE, 1.5(4.2) GHz, 12MB, 28W(20W cTDP), 4P+4E/12T
- Intel® Core™ i7-1265UE, 1.7(4.7) GHz, 12MB, 15W(12W cTDP), 2P+8E/12T
- Intel® Core™ i5-1245UE, 1.5(4.4) GHz, 12MB, 15W(12W cTDP), 2P+8E/12T
- Intel® Core™ i3-1215UE, 1.2(4.4) GHz, 10MB, 15W(12W cTDP), 2P+4E/8T
- Intel® Celeorn™ 7305E, 1.0 GHz, 8MB, 15W(12W cTDP), 1P+4E/6T

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

Memory

Up to 64GB (2x 32GB) non-ECC DDR5 in two SODIMM sockets (one on top, one on bottom), maximum 32GB per socket, maximum 4800 MT/s.

Note: It is recommended to check that the bottom side specifications are suitable for your application purposes.

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

2.2. Video

GPU

Intel® Iris Xe Graphics architecture with up to 96 execution units

Feature Support

- 4 independent and simultaneous combinations of DisplayPort/HDMI/LVDS/eDP/VGA and display alternative mode through USB4/Thunderbolt4 graphics outputs (4x 4K @60Hz, up to 8K@60Hz)
- (eDP optional in place of LVDS, VGA optional in place of DDI 3)
- Playback of high-definition content including Blu-ray Disc and Blu-ray Disc 3D content using HDMI (1.4a spec compliant with 3D)
- DirectX Video Acceleration (DXVA) support for accelerated video processing
- HEVC/H.265, H.264, M/JPEG, MPEG2, AV1, WMV9, VP9 HW decode
- HEVC/H.265, H.264, JPEG, VP9 HW encode, up to 8K60 HEVC
- Advanced Scheduler 2.0, 1.0, XPDM support
- DirectX up to 12
- OpenGL up to 4.6 and ES 2.0 support
- OpenCL up to 2.1 support

Note: Availability of features is dependent on the operating system used (Windows 10 64-bit, Linux 64-bit).

2.2.1 Display Interface Support

LVDS: Single/dual channel 18/24-bit LVDS through eDP to LVDS IC, supports DE mode and Hsync/Vsync mode.
Max. resolution 1920x1200@60Hz in dual mode. Pixel clock frequency up to 112 MHz. VESA and JEIDA panel data formats supported.

eDP: eDP 1.4b up to 4 lane support, in place of LVDS (BOM option), up to 4096x2304@60Hz bpp with DSC

DDI x3: Digital Display Ports (DDI) support DisplayPort 1.4a, HDMI 2.0b or DVI

VGA: VGA BOM option support in place of DDI 3; max. resolution 1920x1200@60Hz

Note: USB4 is a build option (HW and BIOS) supported by project basis in place of DDI channels. Maximum 2x USB4 by using DDI 1 and DDI 2 channels. USB4 support also requires re-timer and PD on carrier.

2.3. Audio

Intel® HD Audio integrated

Located on carrier Express-BASE6 or Express-BASE6 R3.1 (ALC886 standard support)

2.4. Expansion Busses

1 PCI Express x8 Gen4 (45W CPU only): Lanes 16-23 (configurable to 1 x8). Gen4 support dependent on carrier design (suitable for GPU, NVMe SSD).

2 PCI Express x4 Gen4: Lanes 24-27 and 28-31 (configurable to 2 x4). Gen4 support dependent on carrier design (suitable for GPU, NVMe SSD).

8 PCI Express x1 Gen3: Lanes 0-3 (configurable to 4 x1, 2 x2, 1 x4, 1 x2 + 2 x1) and Lanes 4-7 (configurable to 4 x1, via PCIe switch)

Other: SMBus (system), I^2C (user), LPC bus (via eSPI to LPC bridge IC)

2.5. Ethernet

2.5GbE Intel® Ethernet Controller I225 Series (V, IT or LM version)

Supports up to 2.5GbE and 1000/100/10 Mbit/s connections

IT version supports TSN feature on Linux OS, GbE0_SDP available if TSN support enabled

2.6. Multi I/O and Storage

USB 4

2x USB4: build option (HW and BIOS) supported by project basis in place of DDI channels. Maximum 2x USB4 by using DDI 1 and DDI 2 channels. USB4 support also requires re-timer and PD on carrier.

Note: Capable of **TBT4**. Please contact your local ADLINK representative for details.

USB

4x USB 3.2 Gen2/2.0/1.1 (USB 0,1,2,3), 4x USB 2.0/1.1 (USB 4,5,6,7)

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

Note: Carrier board must be designed for Gen2 operation.
USB 0,1,2,3 are backward compatible with USB 2.0/1.1.

SATA

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

Note: For SATA 6Gb/s compatibility, it is strongly recommended to use a SATA redriver on the carrier board

GPIO ~~or SD~~

4 GPO and 4 GPI (GPI with interrupt)

On-board Storage

Soldered type PCIe NVMe SSD, available capacities: 60GB/120GB/240GB. Build option support by project basis

PCIe NVMe SSD co-lay 1 PCI Express x4 Gen4 : PEG12-15

Note: For the NVMe SSD build option, DIMM support is limited to 2 slots. Please contact your local ADLINK representative for details.

UART

Two UART interfaces SER0 and SER1 RX/TX on module

Console Redirection via COM 1 or COM 2 selectable in BIOS

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

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

Note: SER0, SER1 from SoC HSUART are BOM option support by project basis

2.7. Trusted Platform Module (TPM)

Chipset: Infineon solution

Type: TPM 2.0 (SPI bus based)

2.8. SEMA Board controller

Supports: Voltage/current monitoring, power sequence debug support, AT/ATX mode control, logistics and forensic information, flat panel control, general purpose I^2C, failsafe BIOS (dual BIOS, opt. support), watchdog timer and fan control.

2.9. Debug

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

Supports embedded controller access, SPI BIOS flashing, internal power rail test points, debug LEDs

2.10. Power

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

Standard Voltage Input:	ATX: 12V±5% / 5Vsb ±5%	or	AT: 12V±5%
Wide Voltage Input:	ATX: 8.5-20V, 5Vsb ±5%	or	AT: 8.5-20V

Power Management: ACPI 5.0 compliant, Smart Battery support
Power States: C1-C6, S0, S1, S3, S4, S5, S5 ECO mode (Wake-on-USB S3/S4, WoL S3/S4/S5)
ECO Mode support for deep S5 for 5Vsb power saving

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

2.11. Mechanical and Environmental

Form Factor and specification

PICMG COM Express Rev 3.1 (COM.0 R3.1), Type 6, Basic size 125 x 95 mm

Operating Temperature

Standard	0°C to 60°C (wide voltage input)	Storage: -20°C to 80°C
Extreme Rugged	-40°C to 85°C (selected SKUs, TBC)	Storage: -40°C to 85°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

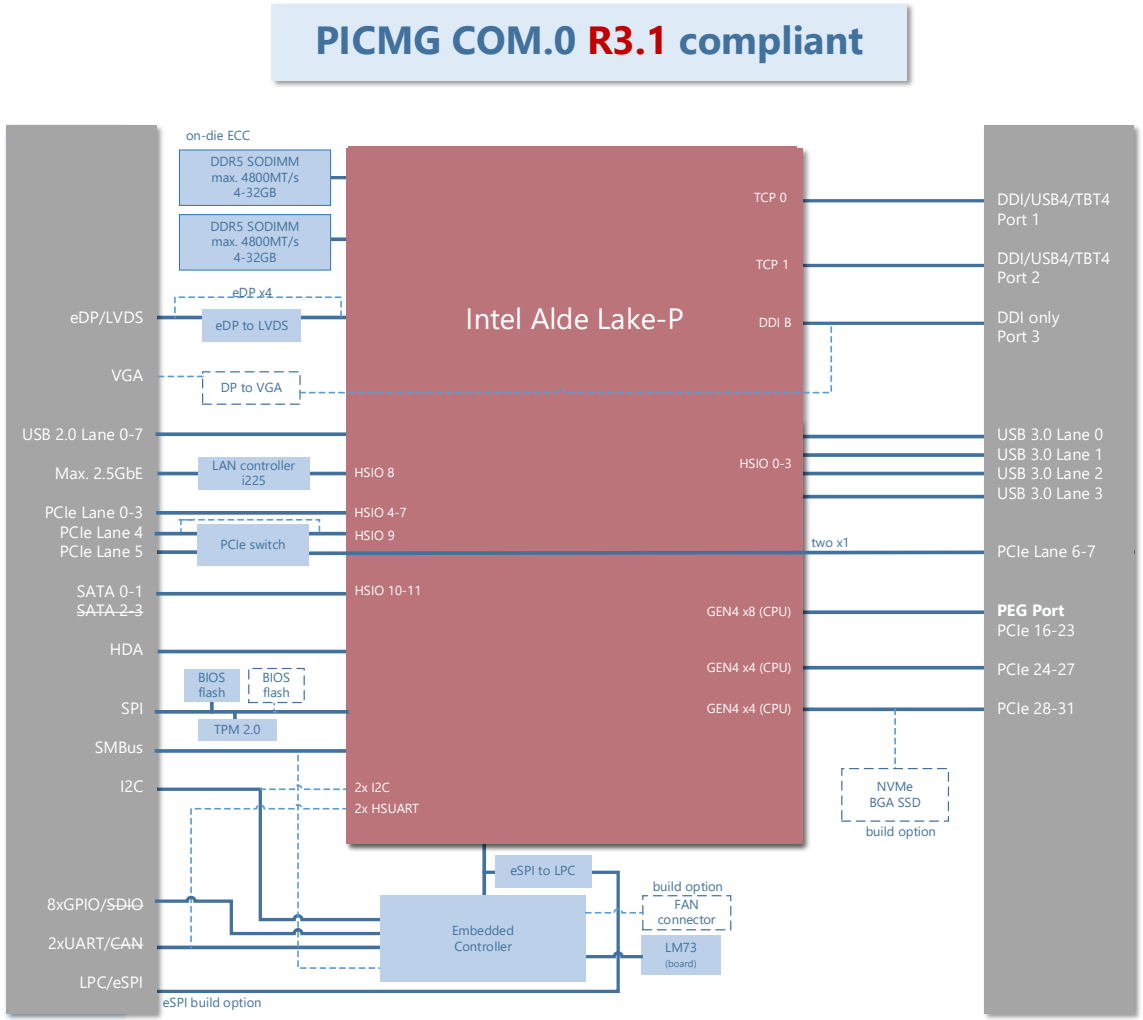


Figure 1 – Module function diagram

4. Pinout and Signal Descriptions

4.1. Pin Summary

The table below is a comprehensible list of all signal pins supported on the dual 220-pin COM Express connectors as defined for Type 6 in the PICMG COM.0 R3.1 specification. Signals described in the specification but not supported on the Express-ADP are marked with ~~strikethrough.~~

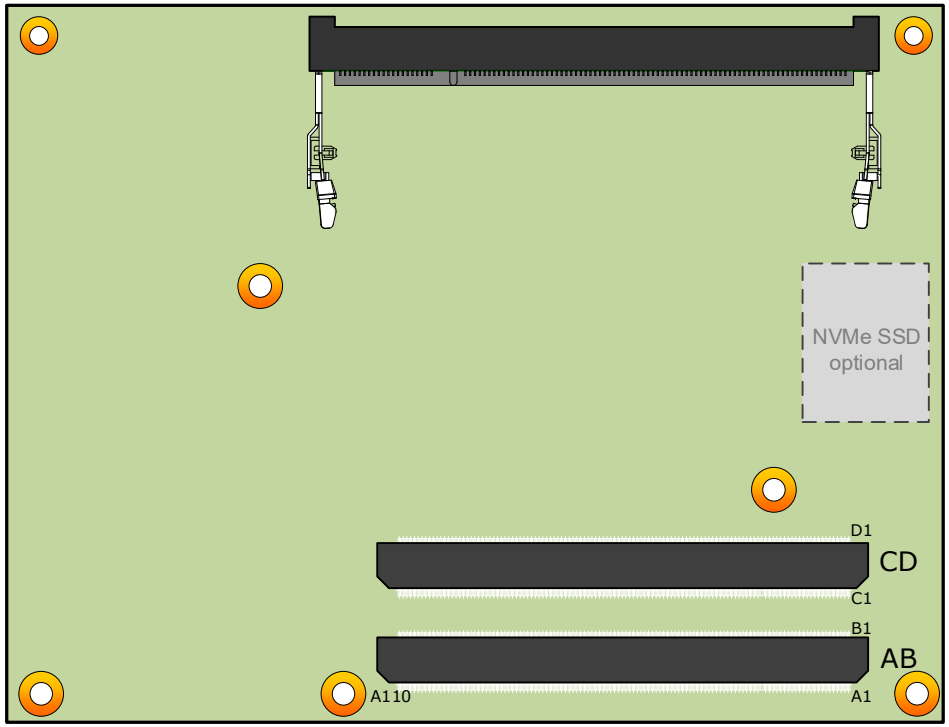


Figure 2 - Module rear side row and pin numbering

Row A			Row B			Row C			Row D	
A1	GND (FIXED)		B1	GND (FIXED)		C1	GND FIXED)		D1	GND FIXED)
A2	GBE0_MDI3-		B2	GBE0_ACT#		C2	GND		D2	GND
A3	GBE0_MDI3+		B3	LPC_FRAME#/ESPI_CS0#[1]		C3	USB_SSRX0-		D3	USB_SSTX0-
A4	GBE0_LINK_MID#		B4	LPC_AD0/ESPI_IO_0[1]		C4	USB_SSRX0+		D4	USB_SSTX0+
A5	GBE0_LINK_MAX#		B5	LPC_AD1/ESPI_IO_1[1]		C5	GND		D5	GND
A6	GBE0_MDI2-		B6	LPC_AD2/ESPI_IO_2[1]		C6	USB_SSRX1-		D6	USB_SSTX1-
A7	GBE0_MDI2+		B7	LPC_AD3/ESPI_IO_3[1]		C7	USB_SSRX1+		D7	USB_SSTX1+
A8	GBE0_LINK#		B8	~~LPC_DRQ0#/ESPI_ALERT0#~~		C8	GND		D8	GND
A9	GBE0_MDI1-		B9	~~LPC_DRQ1#/ESPI_ALERT1#~~		C9	USB_SSRX2-		D9	USB_SSTX2-
A10	GBE0_MDI1+		B10	LPC_CLK/ESPI_CK[1]		C10	USB_SSRX2+		D10	USB_SSTX2+
A11	GND (FIXED)		B11	GND (FIXED)		C11	GND (FIXED)		D11	GND (FIXED)
A12	GBE0_MDI0-		B12	PWRBTN#		C12	USB_SSRX3-		D12	USB_SSTX3-
A13	GBE0_MDI0+		B13	SMB_CK		C13	USB_SSRX3+		D13	USB_SSTX3+
A14	GBE0_CTREF		B14	SMB_DAT		C14	GND		D14	GND
A15	SUS_S3#		B15	SMB_ALERT#		C15	USB4_1_LSTX[1]		D15	DDI1_CTRLCLK_AUX+ /USB4_1_AUX+[1]
A16	SATA0_TX+		B16	SATA1_TX+		C16	USB4_1_LSRX[1]		D16	DDI1_CTRLDATA_AUX- /USB4_1_AUX-[1]
A17	SATA0_TX-		B17	SATA1_TX-		C17	USB4_RT_ENA[1]		D17	USB4_PD_I2C_ALERT#[1]
A18	SUS_S4#		B18	SUS_STAT#/ESPI_RESET#[1]		C18	GND		D18	PMCALERT#[1]
A19	SATA0_RX+		B19	SATA1_RX+		C19	PCIE_RX6+[1]		D19	PCIE_TX6+
A20	SATA0_RX-		B20	SATA1_RX-		C20	PCIE_RX6-[1]		D20	PCIE_TX6-
A21	GND (FIXED)		B21	GND (FIXED)		C21	GND (FIXED)		D21	GND (FIXED)
A22	~~SATA2_TX+~~		B22	~~SATA3_TX+~~		C22	PCIE_RX7+[1]		D22	PCIE_TX7+
A23	~~SATA2_TX-~~		B23	~~SATA3_TX-~~		C23	PCIE_RX7-[1]		D23	PCIE_TX7-
A24	SUS_S5#		B24	PWR_OK		C24	DDI1_HPD		D24	GND
A25	~~SATA2_RX+~~		B25	~~SATA3_RX+~~		C25	SML0_CLK[1]		D25	GND
A26	~~SATA2_RX-~~		B26	~~SATA3_RX-~~		C26	SML0_DAT[1]		D26	DDI1_PAIR0+ /USB4_1_SSTX0+[1]
A27	BATLOW#		B27	WDT		C27	SML1_CLK[1]		D27	DDI1_PAIR0- /USB4_1_SSTX0-[1]
A28	(S)ATA_ACT#		B28	~~HDA_SDIN2~~/SNDW0_CLK[2]		C28	SML1_DAT[1]		D28	GND
A29	HDA_SYNC		B29	HDA_SDIN1/SNDW0_DAT[2]		C29	USB4_PD_I2C_CLK[1]		D29	DDI1_PAIR1+ /USB4_1_SSRX0+[1]
A30	HDA_RST#		B30	HDA_SDIN0		C30	USB4_PD_I2C_DAT[1]		D30	DDI1_PAIR1- /USB4_1_SSRX0-[1]

Row A			Row B			Row C			Row D	
A31	GND (FIXED)		B31	GND (FIXED)		C31	GND (FIXED)		D31	GND (FIXED)
A32	HDA_BITCLK		B32	SPKR		C32	DDI2_CTRLCLK_AUX+ /USB4_2_AUX+[1]		D32	DDI1_PAIR2+ /USB4_1_SSTX1+[1]
A33	HDA_SDOUT		B33	I2C_CK		C33	DDI2_CTRLDATA_AUX- /USB4_2_AUX-[1]		D33	DDI1_PAIR2- /USB4_1_SSTX1-[1]
A34	BIOS_DIS0#/ESPI_SAFS[1]		B34	I2C_DAT		C34	DDI2_DDC_AUX_SEL		D34	DDI1_DDC_AUX_SEL
A35	THRMTRIP#		B35	THRM#		C35	USB4_2_LSTX[1]		D35	USB4_2_LSRX[1]
A36	USB6-		B36	USB7-		C36	DDI3_CTRLCLK_AUX+		D36	DDI1_PAIR3+ /USB4_1_SSRX1+[1]
A37	USB6+		B37	USB7+		C37	DDI3_CTRLDATA_AUX-		D37	DDI1_PAIR3- /USB4_1_SSRX1-[1]
A38	USB_6_7_OC#		B38	USB_4_5_OC#		C38	DDI3_DDC_AUX_SEL		D38	GND
A39	USB4-		B39	USB5-		C39	DDI3_PAIR0+		D39	DDI2_PAIR0+ /USB4_2_SSTX0+[1]
A40	USB4+		B40	USB5+		C40	DDI3_PAIR0-		D40	DDI2_PAIR0- /USB4_2_SSTX0-[1]
A41	GND (FIXED)		B41	GND (FIXED)		C41	GND (FIXED)		D41	GND (FIXED)
A42	USB2-		B42	USB3-		C42	DDI3_PAIR1+		D42	DDI2_PAIR1+ /USB4_2_SSRX0+[1]
A43	USB2+		B43	USB3+		C43	DDI3_PAIR1-		D43	DDI2_PAIR1- /USB4_2_SSRX0-[1]
A44	USB_2_3_OC#		B44	USB_0_1_OC#		C44	DDI3_HPD		D44	DDI2_HPD
A45	USB0-		B45	USB1-		C45	GP_SPI_CS#[2]		D45	GND
A46	USB0+		B46	USB1+		C46	DDI3_PAIR2+		D46	DDI2_PAIR2+ /USB4_2_SSTX1+[1]
A47	VCC_RTC		B47	ESPI_EN#[1]		C47	DDI3_PAIR2-		D47	DDI2_PAIR2- /USB4_2_SSTX1-[1]
A48	~~RSMRST_OUT#~~		B48	~~USB0_HOST_PRSNT~~		C48	RSVD		D48	GND
A49	GBE0_SDP[1]		B49	SYS_RESET#		C49	DDI3_PAIR3+		D49	DDI2_PAIR3+ /USB4_2_SSRX1+[1]
A50	LPC_SERIRQ/ESPI_CS1#[1]		B50	CB_RESET#		C50	DDI3_PAIR3-		D50	DDI2_PAIR3- /USB4_2_SSRX1-[1]
A51	GND (FIXED)		B51	GND (FIXED)		C51	GND (FIXED)		D51	GND (FIXED)
A52	PCIE_TX5+[1]		B52	PCIE_RX5+[1]		C52	PEG_RX0+		D52	PEG_TX0+
A53	PCIE_TX5-[1]		B53	PCIE_RX5-[1]		C53	PEG_RX0-		D53	PEG_TX0-
A54	GPI0		B54	GPO1		C54	TYPE0#		D54	PEG_LANE_RV#
A55	PCIE_TX4+		B55	PCIE_RX4+		C55	PEG_RX1+		D55	PEG_TX1+

Row A			Row B			Row C			Row D	
A56	PCIE_TX4-		B56	PCIE_RX4-		C56	PEG_RX1-		D56	PEG_TX1-
A57	GND		B57	GPO2		C57	TYPE1#		D57	TYPE2#
A58	PCIE_TX3+		B58	PCIE_RX3+		C58	PEG_RX2+		D58	PEG_TX2+
A59	PCIE_TX3-		B59	PCIE_RX3-		C59	PEG_RX2-		D59	PEG_TX2-
A60	GND (FIXED)		B60	GND (FIXED)		C60	GND (FIXED)		D60	GND (FIXED)
A61	PCIE_TX2+		B61	PCIE_RX2+		C61	PEG_RX3+		D61	PEG_TX3+
A62	PCIE_TX2-		B62	PCIE_RX2-		C62	PEG_RX3-		D62	PEG_TX3-
A63	GPI1		B63	GPO3		C63	GND		D63	GND
A64	PCIE_TX1+		B64	PCIE_RX1+		C64	GND		D64	GND
A65	PCIE_TX1-		B65	PCIE_RX1-		C65	PEG_RX4+		D65	PEG_TX4+
A66	GND		B66	WAKE0#		C66	PEG_RX4-		D66	PEG_TX4-
A67	GPI2		B67	WAKE1#		C67	~~RAPID_SHUTDOWN~~		D67	GND
A68	PCIE_TX0+		B68	PCIE_RX0+		C68	PEG_RX5+		D68	PEG_TX5+
A69	PCIE_TX0-		B69	PCIE_RX0-		C69	PEG_RX5-		D69	PEG_TX5-
A70	GND (FIXED)		B70	GND (FIXED)		C70	GND (FIXED)		D70	GND (FIXED)
A71	LVDS_A0+ / eDP_TX2+[1]		B71	LVDS_B0+		C71	PEG_RX6+		D71	PEG_TX6+
A72	LVDS_A0- / eDP_TX2-[1]		B72	LVDS_B0-		C72	PEG_RX6-		D72	PEG_TX6-
A73	LVDS_A1+ / eDP_TX1+[1]		B73	LVDS_B1+		C73	GND		D73	GND
A74	LVDS_A1- / eDP_TX1-[1]		B74	LVDS_B1-		C74	PEG_RX7+		D74	PEG_TX7+
A75	LVDS_A2+ / eDP_TX0+[1]		B75	LVDS_B2+		C75	PEG_RX7-		D75	PEG_TX7-
A76	LVDS_A2- / eDP_TX0-[1]		B76	LVDS_B2-		C76	GND		D76	GND
A77	LVDS_VDD_EN / eDP_VDD_EN[1]		B77	LVDS_B3+		C77	GND		D77	GND
A78	LVDS_A3+		B78	LVDS_B3-		C78	PEG_RX8+		D78	PEG_TX8+
A79	LVDS_A3-		B79	LVDS_BKLT_EN		C79	PEG_RX8-		D79	PEG_TX8-
A80	GND (FIXED)		B80	GND (FIXED)		C80	GND (FIXED)		D80	GND (FIXED)
A81	LVDS_A_CK+ / eDP_TX3+[1]		B81	LVDS_B_CK+		C81	PEG_RX9+		D81	PEG_TX9+
A82	LVDS_A_CK- / eDP_TX3-[1]		B82	LVDS_B_CK-		C82	PEG_RX9-		D82	PEG_TX9-
A83	LVDS_I2C_CK / eDP_AUX+[1]		B83	LVDS_BKLT_CTRL / eDP_BKLT_CTRL[1]		C83	GND		D83	GND
A84	LVDS_I2C_DAT / eDP_AUX-[1]		B84	VCC_5V_SBY		C84	GND		D84	GND
A85	GPI3		B85	VCC_5V_SBY		C85	PEG_RX10+		D85	PEG_TX10+
A86	GP_SPI_MOSI[2]		B86	VCC_5V_SBY		C86	PEG_RX10-		D86	PEG_TX10-
A87	eDP_HPD		B87	VCC_5V_SBY		C87	GND		D87	GND
A88	PCIE_CK_REF+		B88	BIOS_DIS1#		C88	PEG_RX11+		D88	PEG_TX11+
A89	PCIE_CK_REF-		B89	VGA_RED[1]		C89	PEG_RX11-		D89	PEG_TX11-
A90	GND (FIXED)		B90	GND (FIXED)		C90	GND (FIXED)		D90	GND (FIXED)
A91	SPI_POWER		B91	VGA_GRN[1]		C91	PEG_RX12+		D91	PEG_TX12+
A92	SPI_MISO		B92	VGA_BLU[1]		C92	PEG_RX12-		D92	PEG_TX12-

Row A			Row B			Row C			Row D	
A93	GPO0		B93	VGA_HSYNC[1]		C93	GND		D93	GND
A94	SPI_CLK		B94	VGA_VSYNC[1]		C94	PEG_RX13+		D94	PEG_TX13+
A95	SPI_MOSI		B95	VGA_I2C_CK[1]		C95	PEG_RX13-		D95	PEG_TX13-
A96	TPM_PP		B96	VGA_I2C_DAT[1]		C96	GND		D96	GND
A97	TYPE10#		B97	SPI_CS#		C97	GND		D97	GND
A98	SER0_TX		B98	GP_SPI_MISO[2]		C98	PEG_RX14+		D98	PEG_TX14+
A99	SER0_RX		B99	GP_SPI_CK[2]		C99	PEG_RX14-		D99	PEG_TX14-
A100	GND (FIXED)		B100	GND (FIXED)		C100	GND (FIXED)		D100	GND (FIXED)
A101	SER1_TX~~/CAN_TX~~		B101	FAN_PWMOUT		C101	PEG_RX15+		D101	PEG_TX15+
A102	SER1_RX~~/CAN_RX~~		B102	FAN_TACHIN		C102	PEG_RX15-		D102	PEG_TX15-
A103	LID#		B103	SLEEP#		C103	GND		D103	GND
A104	VCC_12V		B104	VCC_12V		C104	VCC_12V		D104	VCC_12V
A105	VCC_12V		B105	VCC_12V		C105	VCC_12V		D105	VCC_12V
A106	VCC_12V		B106	VCC_12V		C106	VCC_12V		D106	VCC_12V[1]
A107	VCC_12V		B107	VCC_12V		C107	VCC_12V		D107	VCC_12V
A108	VCC_12V		B108	VCC_12V		C108	VCC_12V		D108	VCC_12V
A109	VCC_12V		B109	VCC_12V		C109	VCC_12V		D109	VCC_12V
A110	GND (FIXED)		B110	GND (FIXED)		C110	GND (FIXED)		D110	GND (FIXED)

Note: ~~Strike-through~~ entries are not supported functions on this product.

PEG 0-7 are available only for 45W CPU SKUs.

1. eDP (in place of LVDS), VGA (in place of DDI 3), eSPI (in place of LPC), PCIe lane5-7 (via PCIe switch), USB4_1/2 (in place of DDI 1/2), and GBE0_SDP (for selected LAN controller versions) are BOM options supported by project basis.
2. GP_SPI and SNDW0 support TBC.

4.2. Signal Terminology Descriptions

Meaning of the terms used for signal description tables

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

4.3. AB Connector Signal Descriptions

4.3.1 Audio

Name	Pin #	Description	I/O	PU / PD	Comment
AC_RST# / HDA_RST#	A30	Reset output to CODEC, active low.	O 3.3VSB		
AC_SYNC / HDA_SYNC	A29	Sample-synchronization signal to the CODEC(s).	O 3.3VSB		PCH internal PD 20Kohm
AC_BITCLK / HDA_BITCLK	A32	Serial data clock generated by the external CODEC(s).	I/O 3.3VSB		
AC_SDOUT / HDA_SDOUT	A33	Serial TDM data output to the CODEC.	O 3.3VSB		PCH internal PD 20Kohm
AC_SDIN[2:0] / HDA_SDIN[2:0]	~~B28~~ B29 B30	Serial TDM data inputs from up to 3 CODECs.	I/O 3.3VSB		PCH internal PD 20Kohm AC_SDNI2/HDA_SDIN2 not supported

4.3.2 Analog VGA

Name	Pin #	Description	I/O	PU / PD	Comment
VGA_RED	B89	Red for monitor. Analog DAC output, designed to drive a 37.5-Ohm equivalent load.	O Analog	PD 150R	
VGA_GRN	B91	Green for monitor. Analog DAC output, designed to drive a 37.5-Ohm equivalent load.	O Analog	PD 150R	
VGA_BLU	B92	Blue for monitor. Analog DAC output, designed to drive a 37.5-Ohm equivalent load.	O Analog	PD 150R	
VGA_HSYNC	B93	Horizontal sync output to VGA monitor	O 3.3V		
VGA_VSYNC	B94	Vertical sync output to VGA monitor	O 3.3V		
VGA_I2C_CK	B95	DDC clock line (I^2C port dedicated to identifying VGA monitor capabilities)	I/O OD 3.3V	PU 2k2 3.3V	
VGA_I2C_DAT	B96	DDC data line.	I/O OD 3.3V	PU 2k2 3.3V	

Note: VGA is BOM option support (in place of DDI 3) by project basis

4.3.3 LVDS or eDP

The module default supports a single or dual channel LVDS display panel with up to 24-bit colors. A BOM option that removes the eDP to LVDS bridge IC and outputs the eDP signals directly is available. eDP vs LVDS pin mapping is described below.

Pin #	LVDS mode	eDP mode
A71	LVDS_A0+	eDP_TX2+
A72	LVDS_A0-	eDP_TX2-
A73	LVDS_A1+	eDP_TX1+
A74	LVDS_A1-	eDP_TX1-
A75	LVDS_A2+	eDP_TX0+
A76	LVDS_A2-	eDP_TX0-
A78	LVDS_A3+	-
A79	LVDS_A3-	-
A81	LVDS_A_CK+	eDP_TX3+
A82	LVDS_A_CK-	eDP_TX3-
B71	LVDS_B0+	-
B72	LVDS_B0-	-
B73	LVDS_B1+	-
B74	LVDS_B1-	-
B75	LVDS_B2+	-
B76	LVDS_B2-	-
B77	LVDS_B3+	-
B78	LVDS_B3-	-
B81	LVDS_B_CK+	-
B82	LVDS_B_CK-	-
A77	LVDS_VDD_EN	eDP_VDD_EN
B79	LVDS_BKLT_EN	eDP_BKLT_EN
B83	LVDS_BKLT_CTRL	eDP_BKLT_CTRL
A83	LVDS_I2C_CK	eDP_AUX+
A84	LVDS_I2C_DAT	eDP_AUX-
A87	-	eDP_HPD

Note: LVDS is the default mode and eDP is a BOM option

4.3.3.1. Single/Dual Channel LVDS (default)

Name	Pin #	Description	I/O	PU / PD	Comment
LVDS_A0+ LVDS_A0- LVDS_A1+ LVDS_A1- LVDS_A2+ LVDS_A2- LVDS_A3+ LVDS_A3-	A71 A72 A73 A74 A75 A76 A78 A79	LVDS Channel A differential pairs	O LVDS		
LVDS_A_CK+ LVDS_A_CK-	A81 A82	LVDS Channel A differential clock	O LVDS		
LVDS_B0+ LVDS_B0- LVDS_B1+ LVDS_B1- LVDS_B2+ LVDS_B2- LVDS_B3+ LVDS_B3-	B71 B72 B73 B74 B75 B76 B77 B78	LVDS Channel B differential pairs	O LVDS		
LVDS_B_CK+ LVDS_B_CK-	B81 B82	LVDS Channel B differential clock	O LVDS		
LVDS_VDD_EN	A77	LVDS panel power enable	O 3.3V	PD 100K	
LVDS_BKLT_EN	B79	LVDS panel backlight enable	O 3.3V	PD 100K	
LVDS_BKLT_CTRL	B83	LVDS panel backlight brightness control	O 3.3V	PD 100K	
LVDS_I2C_CK	A83	DDC lines used for flat panel detection and control.	O 3.3V	PU 2k2 3.3V	
LVDS_I2C_DAT	A84	DDC lines used for flat panel detection and control.	I/O 3.3V	PU 2k2 3.3V	

4.3.3.2. 4-lane eDP

Name	Pin #	Description	I/O	PU / PD	Comment
eDP_TX3+ eDP_TX3- eDP_TX2+ eDP_TX2- eDP_TX1+ eDP_TX1- eDP_TX0+ eDP_TX0-	A81 A82 A71 A72 A73 A74 A75 A76	eDP differential pairs	O PCIE		AC coupled off module
eDP_VDD_EN	A77	eDP power enable	O 3.3V	PD 100K	
eDP_BKLT_EN	B79	eDP backlight enable	O 3.3V	PD 100K	
eDP_BKLT_CTRL	B83	eDP backlight brightness control	O 3.3V	PD 100K	
eDP_AUX+	A83	eDP AUX+	I/O PCIE		AC coupled off module
eDP_AUX-	A84	eDP AUX-	I/O PCIE		AC coupled off module
eDP_HPD	A87	Detection of Hot Plug / Unplug and notification of the link layer	I 3.3V	PD 100K	PD 100K on this pin when eDP is supported

4.3.4 Gigabit Ethernet

Name	Pin #	Description	I/O	PU / PD	Comment
GBE0_MDI0+ GBE0_MDI0- GBE0_MDI1+ GBE0_MDI1- GBE0_MDI2+ GBE0_MDI2- GBE0_MDI3+ GBE0_MDI3-	A13 A12 A10 A9 A7 A6 A3 A2	Gigabit Ethernet Controller 0: Media Dependent Interface Differential Pairs 0, 1, 2, 3. The MDI can operate in 1000, 100, and 10Mbit/sec modes. Some pairs are unused in some modes according to the following: **1000 / 100 / 10** MDI[0]+/- B1_DA+/- TX+/- TX+/- MDI[1]+/- B1_DB+/- RX+/- RX+/- MDI[2]+/- B1_DC+/- MDI[3]+/- B1_DD+/-	I/O Analog		Twisted pair signals for external transformer.
GBE0_ACT#	B2	Gigabit Ethernet Controller 0 activity indicator, active low.	OD 3.3VSB		
GBE0_LINK#	A8	Gigabit Ethernet Controller 0 link indicator, active low.	OD 3.3VSB		
GBE0_LINK100# *	A4	Gigabit Ethernet Controller 0 100Mbit/sec link indicator, active low.	OD 3.3VSB		
GBE0_LINK1000# *	A5	Gigabit Ethernet Controller 0 1000Mbit/sec link indicator, active low.	OD 3.3VSB		
~~GBE0_CTREF~~	~~A14~~	~~Reference voltage for Carrier Board Ethernet channel 1 and 2 magnetics center tap. The reference voltage is determined by the requirements of the Module PHY and may be as low as 0V and as high as 3.3V. The reference voltage output shall be current limited on the Module. In the case in which the reference is shorted to ground, the current shall be 250 mA or less.~~	~~REF~~ ~~GND min~~ ~~3.3V max~~		Not supported
GBE0_SDP	A49	Gigabit Ethernet Controller 0 Software-Definable Pin. Can also be used for IEEE1588 support such as 1pps signal.	IO 3.3VSB	GBE0_SDP	Depends on the selection of LAN controller. i225-IT support this pin

Note: This product supports up to 2.5GbE. The LAN LED behavior is optimized for maximum 2.5GbE speed.
GBE0_LINK1000# will be active for 2.5GbE speed indication.
GBE0_LINK100# will be active for 1GbE speed indication or lower.
GBE0_ACT# and GBE0_LINK# share the same source from the LAN controller.
For 100Mbit/sec and 10Mbit/sec speed, the LAN LED will be OFF.

4.3.5 SATA

Name	Pin #	Description	I/O	PU / PD	Comment
SATA0_TX+ SATA0_TX-	A16 A17	Serial ATA channel 0, Transmit Output differential pair.	O SATA		AC coupled on Module
SATA0_RX+ SATA0_RX-	A19 A20	Serial ATA channel 0, Receive Input differential pair.	I SATA		AC coupled on Module
SATA1_TX+ SATA1_TX-	B16 B17	Serial ATA channel 1, Transmit Output differential pair.	O SATA		AC coupled on Module
SATA1_RX+ SATA1_RX-	B19 B20	Serial ATA channel 1, Receive Input differential pair.	I SATA		AC coupled on Module
~~SATA2_TX+ SATA2_TX-~~	~~A22 A23~~	~~Serial ATA channel 2, Transmit Output differential pair.~~	~~O SATA~~		Not supported
~~SATA2_RX+ SATA2_RX-~~	~~A25 A26~~	~~Serial ATA channel 2, Receive Input differential pair.~~	~~I SATA~~		Not supported
~~SATA3_TX+ SATA3_TX-~~	~~B22 B23~~	~~Serial ATA channel 3, Transmit Output differential pair.~~	~~O SATA~~		Not supported
~~SATA3_RX+ SATA3_RX-~~	~~B25 B26~~	~~Serial ATA channel 3, Receive Input differential pair.~~	~~I SATA~~		Not supported
(S)ATA_ACT#	A28	ATA (parallel and serial) or SAS activity indicator, active low.	O 3.3V	PU 10K 3.3V	AC coupled on Module

4.3.5.1. PCH HSIO Lane Assignments

Name	HSIO name on SOC	Comment
SATA0	HSIO 26	
SATA1	HSIO 27	
~~SATA2~~	~~HSIO 28~~	Not supported
~~SATA3~~	~~HSIO 29~~	Not supported

4.3.6 PCI Express

Name	Pin #	Description	I/O	PU / PD	Comment
PCIE_TX0+ PCIE_TX0-	A68 A69	PCI Express channel 0, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX0+ PCIE_RX0-	B68 B69	PCI Express channel 0, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX1+ PCIE_TX1-	A64 A65	PCI Express channel 1, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX1+ PCIE_RX1-	B64 B65	PCI Express channel 1, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX2+ PCIE_TX2-	A61 A62	PCI Express channel 2, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX2+ PCIE_RX2-	B61 B62	PCI Express channel 2, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX3+ PCIE_TX3-	A58 A59	PCI Express channel 3, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX3+ PCIE_RX3-	B58 B59	PCI Express channel 3, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX4+ PCIE_TX4-	A55 A56	PCI Express channel 4, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX4+ PCIE_RX4-	B55 B56	PCI Express channel 4, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_TX5+ PCIE_TX5-	A52 A53	PCI Express channel 5, Transmit Output differential pair.	O PCIE		AC coupled on Module
PCIE_RX5+ PCIE_RX5-	B52 B53	PCI Express channel 5, Receive Input differential pair.	I PCIE		AC coupled off Module
PCIE_CLK_REF+ PCIE_CLK_REF-	A88 A89	PCI Express Reference Clock output for all PCI Express and PCI Express Graphics Lanes.	O PCIE		

4.3.6.1. PCH HSIO Lane Assignments

Name	HSIO name on SOC / Switch IC	Comment
PCIE0	HSIO 22	
PCIE1	HSIO 23	
PCIE2	HSIO 24	
PCIE3	HSIO 25	
PCIE4	PCIe SW DPE_0	
PCIE5	PCIe SW DPE_1	
PCIE6	PCIe SW DPE_6	
PCIE7	PCIe SW DPE_14	

4.3.7 LPC Bus

Name	Pin #	Description	I/O	PU / PD	Comment
LPC_AD0 LPC_AD1 LPC_AD2 LPC_AD3	B4 B5 B6 B7	LPC multiplexed address, command and data bus	I/O 3.3VSB		
LPC_FRAME#	B3	LPC frame indicates the start of an LPC cycle	O 3.3VSB		
LPC_DRQ0# LPC_DRQ1#	B8 B9	LPC serial DMA request	I 3.3V		Not connected
LPC_SERIRQ	A50	LPC serial interrupt	I/O 3.3VSB	PU 8.2K 3.3VSB	
LPC_CLK	B10	LPC clock output –33MHz nominal	O 3.3VSB		The LPC_CLK frequency is 24MHz on this platform

Note: LPC Bus is supported by an eSPI to LPC bridge IC

4.3.8 USB

Name	Pin #	Description	I/O	PU / PD	Comment
USB0+ USB0-	A46 A45	USB differential data pairs for Port 0	I/O 3.3VSB		USB 1.1/ 2.0 compliant
USB1+ USB1-	B46 B45	USB differential data pairs for Port 1	I/O 3.3VSB		USB 1.1/ 2.0 compliant
USB2+ USB2-	A43 A42	USB differential data pairs for Port 1	I/O 3.3VSB		USB 1.1/ 2.0 compliant
USB3+ USB3-	B43 B42	USB differential data pairs for Port 2	I/O 3.3VSB		USB 1.1/ 2.0 compliant
USB4+ USB4-	A40 A39	USB differential data pairs for Port 3	I/O 3.3VSB		USB 1.1/ 2.0 compliant
USB5+ USB5-	B40 B39	USB differential data pairs for Port 4	I/O 3.3VSB		USB 1.1/ 2.0 compliant
USB6+ USB6-	A37 A36	USB differential data pairs for Port 5	I/O 3.3VSB		USB 1.1/ 2.0 compliant
USB7+ USB7-	B37 B37	USB differential data pairs for Port 6	I/O 3.3VSB		USB 1.1/ 2.0 compliant
USB_0_1_OC#	B44	USB over-current sense, USB ports 0 and 1 (see *Note)	I 3.3VSB	PU 10K 3.3VSB	Do not pull high on carrier
USB_2_3_OC#	A44	USB over-current sense, USB ports 2 and 3 (see *Note)	I 3.3VSB	PU 10K 3.3VSB	Do not pull high on carrier
USB_4_5_OC#	B38	USB over-current sense, USB ports 4 and 5 (see *Note)	I 3.3VSB	PU 10K 3.3VSB	Do not pull high on carrier
USB_6_7_OC#	A38	USB over-current sense, USB ports 6 and 7 (see *Note)	I 3.3VSB	PU 10K 3.3VSB	Do not pull high on carrier
USB0_HOST_PRSNT	B48	Module USB client may detect the presence of a USB host on USB0. A high value indicates that a host is present.	I 3.3VSB		Not supported

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

4.3.9 SPI Bus (BIOS only)

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

4.3.10 Miscellaneous

Name	Pin #	Description	I/O	PU / PD	Comment
SPKR	B32	Output for audio enunciator, the "speaker" in PC-AT systems	O 3.3V		
WDT	B27	Output indicating that a watchdog time-out event has occurred.	O 3.3V	PU 10K 3.3V	
THRM#	B35	Input from off-module temp sensor indicating an over-temp situation.	I 3.3VSB		
THRMTRIP#	A35	Active low output indicating that the CPU has entered thermal shutdown.	O 3.3VSB	PU 100K 3.3VSB	
FAN_PWMOUT	B101	Fan speed control. Uses the Pulse Width Modulation (PWM) technique to control the fan's RPM.	O OD 3.3V		There shall be PD on carrier board
FAN_TACHIN	B102	Fan tachometer input for a fan with a two-pulse output.	I OD 3.3V	PU 47K 3.3V	
TPM_PP	A96	Trusted Platform Module (TPM) Physical Presence pin. Active high. TPM chip has an internal pull down. This signal is used to indicate Physical Presence to the TPM.	I 3.3V	PD 100K	PD only when TPM on module. Modules implementing a TPM shall pull down

4.3.11 SMBus

Name	Pin #	Description	I/O	PU / PD	Comment
SMB_CK	B13	System Management Bus bidirectional clock line. Power sourced through 3.3V standby rail and main power rails.	I/O OD 3.3VSB	PU 4.7K 3.3VSB	
SMB_DAT#	B14	System Management Bus bidirectional data line. Power sourced through 3.3V standby rail and main power rails.	I/O OD 3.3VSB	PU 4.7K 3.3VSB	
SMB_ALERT#	B15	System Management Bus Alert – active low input can be used to generate an SMI# (System Management Interrupt) or to wake the system. Power sourced through 3.3V standby rail and main power rails.	I 3.3VSB	PU 10K 3.3VSB	

4.3.12 I^2C Bus

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

4.3.13 General Purpose I/O (GPIO)

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

4.3.14 Serial Interface Signals

Name	Pin #	Description	I/O	PU / PD	Comment
SER0_TX	A98	General purpose serial port transmitter	O CMOS 3.3V		Power rail tolerance 5V, 12V There shall be PD on carrier board
SER0_RX	A99	General purpose serial port receiver	I CMOS 3.3V	PU 10K 3.3V	Power rail tolerance 5V, 12V
SER1_TX	A101	General purpose serial port transmitter	O CMOS 3.3V		Power rail tolerance 5V, 12V There shall be PD on carrier board
SER1_RX	A102	General purpose serial port receiver	I CMOS 3.3V	PU 10K 3.3V	Power rail tolerance 5V, 12V

4.3.15 Power and System Management

Name	Pin #	Description	I/O	PU / PD	Comment
PWRBTN#	B12	Power button to bring system out of S5 (soft off), active on falling edge.	I 3.3VSB	PU 10K 3.3VSB	
SYS_RESET#	B49	Reset button input. Active low request for module to reset and reboot. May be falling edge sensitive. For situations when SYS_RESET# is not able to reestablish control of the system, PWR_OK or a power cycle may be used.	I 3.3VSB	PU 10K 3.3VSB	
CB_RESET#	B50	Reset output from module to Carrier Board. Active low. Issued by module chipset and may result from a low SYS_RESET# input, a low PWR_OK input, a VCC_12V power input that falls below the minimum specification, a watchdog timeout, or may be initiated by the module software.	O 3.3V		
PWR_OK	B24	Power OK from main power supply. A high value indicates that the power is good. This signal can be used to hold off Module startup to allow carrier-based FPGAs or other configurable devices time to be programmed.	I 3.3VSB	PU 10K 3.3VSB	Should have weak pull up.
SUS_STAT#	B18	Indicates imminent suspend operation; used to notify LPC devices.	O 3.3VSB		
SUS_S3#	A15	Indicates system is in Suspend to RAM state. Active-low output. An inverted copy of SUS_S3# on the carrier board (also known as "PS_ON") may be used to enable the non-standby power on a typical ATX power supply.	O 3.3VSB	PD 100K	
SUS_S4#	A18	Indicates system is in Suspend to Disk state. Active low output.	O 3.3VSB	PD 100K	
SUS_S5#	A24	Indicates system is in Soft Off state.	O 3.3VSB	PD 100K	
WAKE0#	B66	PCI Express wake up signal.	I 3.3VSB	PU 10K 3.3VSB	
WAKE1#	B67	General purpose wake-up signal. May be used to implement wake-up on PS/2 keyboard or mouse activity.	I 3.3VSB	PU 10K 3.3VSB	Connect to WAKE 0#
BATLOW#	A27	Battery low input. This signal may be driven low by external circuitry to signal that the system battery is low or may be used to signal some other external power-management event.	I 3.3VSB	PU 10K 3.3VSB	
LID#	A103	LID button. Low active signal used by the ACPI operating system for a LID switch.	I OD 3.3VSB	PU 47K 3.3VSB	Emulated on GPIO (BIOS)
SLEEP#	B103	Sleep button. Low active signal used by the ACPI operating system to bring the system to sleep state or to wake it up again.	I OD 3.3VSB	PU 47K 3.3VSB	Emulated on GPIO (BIOS)
RAPID_ SHUTDOWN	C67	~~Trigger for Rapid Shutdown. Must be driven to 5V though a <=50-ohm source impedance for ≥ 20 µs.~~	I CMOS 5VSB		Not supported

4.3.16 Power and Ground

Name	Pin #	Description	I/O	PU / PD	Comment
VCC_12V	A104, A105, A106, A107, A108, A109, B104, B105, B106, B107, B109	Primary power input supports wide range 5— 20V input. All available VCC_12V pins on the connector(s) shall be used.	P		8.5-20 V
VCC_5V_SBY	B84, B85, B86, B87	Standby power input: +5.0V nominal. If VCC5_SBY is used, all available VCC_5V_SBY pins on the connector(s) shall be used. Only used for standby and suspend functions. May be left unconnected if these functions are not used in the system design.	P		5Vsb ±5%
VCC_RTC	A47	Real-time clock circuit-power input. Nominally +3.0V.	P		
GND	A1, A11, A21, A31, A41, A51, A57, A60, A66, A70, A80, A90, A100, A110, B1, B11, B21, B31, B41, B51, B60, B70, B80, B90, B100, B110	Ground - DC power and signal and AC signal return path.	P		

4.4. CD Connector Signal Descriptions

4.4.1 USB 3.0 Extensions

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

4.4.1.1. USB Root Segmentation

All USB interfaces are derived from the xHCI controller.

4.4.2 PCI Express

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

4.4.2.1. PCH HSIO Lane Assignments

Refer to Section 4.3.6.1 PCH HSIO Lane Assignments on page 35.

4.4.3 DDI1 Port

Name	Pin #	DisplayPort (DP)	HDMI
DDI1_PAIR0+ DDI1_PAIR0-	D26 D27	DP1_LANE0+ DP1_LANE0-	TMDS1_DATA2+ TMDS1_DATA2-
DDI1_PAIR1+ DDI1_PAIR1-	D29 D30	DP1_LANE1+ DP1_LANE1-	TMDS1_DATA1+ TMDS1_DATA1-
DDI1_PAIR2+ DDI1_PAIR2-	D32 D33	DP1_LANE2+ DP1_LANE2-	TMDS1_DATA0+ TMDS1_DATA0-
DDI1_PAIR3+ DDI1_PAIR3-	D36 D37	DP1_LANE3+ DP1_LANE3-	TMDS1_CLK+ TMDS1_CLK-
DDI1_PAIR4+ DDI1_PAIR4-	C25 C26	-	-
DDI1_PAIR5+ DDI1_PAIR5-	C29 C30	-	-
DDI1_PAIR6+ DDI1_PAIR6-	C15 C16	-	-
DDI1_HPD	C24	DP1_HPD	HDMI1_HPD
DDI1_CTRLCLK_AUX+	D15	DP1_AUX+	HMDI1_CTRLCLK
DDI1_CTRLCLK_AUX-	D16	DP1_AUX-	HMDI1_CTRLDATA
DDI1_DDC_AUX_SEL	D34	DDI1_DDC_AUX_SEL	DDI1_DDC_AUX_SEL

Note: Dual Mode (HDMI and DisplayPort on the same pins) implementations may be realized. This is desirable for SOCs that natively implement this capability. With such SOCs, the primary Dual Mode implementation challenge is that the HDMI_CTRL_DAT and HDMI_CTRL_CK lines are DC coupled, but the DP_AUX+ /- pair must be AC coupled. A set of FET switches is usually used to sort this out. The FET gates can be controlled by the AUX_SEL pin function.

4.4.3.1. DisplayPort (DP) Mode

Name	Pin #	Description	I/O	PU / PD	Comment
DP1_LANE0+ DP1_LANE0- DP1_LANE1+ DP1_LANE1- DP1_LANE2+ DP1_LANE2- DP1_LANE3+ DP1_LANE3-	D26 D27 D29 D30 D32 D33 D36 D37	DP Port 1, differential pair data lines	O PCIE		AC coupled off Module 100 nF DC blocking capacitors shall be placed on the Carrier
DP1_HPD	C24	DP Port 1, detection of Hot Plug / Unplug and notification of the link layer	I 3.3V	PD 100K	Module must tolerate high level in stand-by mode. The carrier board shall include a blocking FET on DP1_HPD to prevent back-drive current from damaging the Module.
DP1_AUX+	D15	DP Port 1, Bidirectional Channel used for Link Management and Device Control	I/O PCIE	PD 100K	AC coupled on Module
DP1_AUX-	D16	DP Port 1, Bidirectional Channel used for Link Management and Device Control	I/O PCIE	PU 100K	AC coupled on Module
DDI1_DDC_AUX_SEL	D34	Strapping Signal to select HDMI or DP output 1M pull-down on the module and floating on the carrier that enables DisplayPort mode	I 3.3V	PD 1M	DP mode enabled

4.4.3.2. HDMI Mode

Name	Pin #	Description	I/O	PU / PD	Comment
TMDS1_DATA2+ TMDS1_DATA2- TMDS1_DATA1+ TMDS1_DATA1- TMDS1_DATA0+ TMDS1_DATA0-	D26 D27 D29 D30 D32 D33	HDMI / DVI Port, Differential Pair Data Lines	O PCIE		AC coupled off Module 100 nF DC blocking capacitors shall be placed on the Carrier
TMDS1_CLK+ TMDS1_CLK-	D36 D37	HDMI Port, Differential Pair Clock Lines			
HDMI_HPD	C24	Detection of Hot Plug / Unplug and notification of the link layer	I 3.3V	PD 100K	
HDMI1_CTRLCLK	D15	I2C_CLK Line for HDMI	I/O PCIE	PU 2.2K	AC couple on Module
HDMI1_CTRLDATA	D16	I2C_DAT Line for HDMI	I/O PCIE	PU 2.2K	AC couple on Module
DDI1_DDC_AUX_SEL	D34	Strapping Signal to select HDMI or DP output 1M pull-down on the module and floating on the carrier that enables DisplayPort mode	I 3.3V	PD 1M	HDMI mode enabled

4.4.4 DDI2 Port

Name	Pin #	DisplayPort (DP)	HDMI
DDI2_PAIR0+ DDI2_PAIR0-	D39 D40	DP2_LANE0+ DP2_LANE0-	TMDS2_DATA2+ TMDS2_DATA2-
DDI2_PAIR1+ DDI2_PAIR1-	D42 D43	DP2_LANE1+ DP2_LANE1-	TMDS2_DATA1+ TMDS2_DATA1-
DDI2_PAIR2+ DDI2_PAIR2-	D46 D47	DP2_LANE2+ DP2_LANE2-	TMDS2_DATA0+ TMDS2_DATA0-
DDI2_PAIR3+ DDI2_PAIR3-	D49 D50	DP2_LANE3+ DP2_LANE3-	TMDS2_CLK+ TMDS2_CLK-
DDI2_HPD	D44	DP2_HPD	HDMI2_HPD
DDI2_CTRLCLK_AUX+	C32	DP2_AUX+	HMDI2_CTRLCLK
DDI2_CTRLCLK_AUX-	C33	DP2_AUX-	HMDI2_CTRLDATA
DDI2_DDC_AUX_SEL	C34	DDI2_DDC_AUX_SEL	DDI2_DDC_AUX_SEL

Note:
Dual Mode (HDMI and DisplayPort on the same pins) implementations may be realized. This is desirable for SOCs that natively implement this capability. With such SOCs, the primary Dual Mode implementation challenge is that the HDMI_CTRL_DAT and HDMI_CTRL_CK lines are DC coupled, but the DP_AUX+ /- pair must be AC coupled. A set of FET switches is usually used to sort this out. The FET gates can be controlled by the AUX_SEL pin function.

4.4.4.1. DisplayPort (DP) Mode

Name	Pin #	Description	I/O	PU / PD	Comment
DP2_LANE0+ DP2_LANE0- DP2_LANE1+ DP2_LANE1- DP2_LANE2+ DP2_LANE2- DP2_LANE3+ DP2_LANE3-	D39 D40 D42 D43 D46 D47 D49 D50	DP Port 2, differential pair data lines	O PCIE		AC coupled off Module 100 nF DC blocking capacitors shall be placed on the Carrier
DP2_HPD	D44	DP Port 2, detection of Hot Plug / Unplug and notification of the link layer	I 3.3V	PD 100K	Module must tolerate high level in stand-by mode. The carrier board shall include a blocking FET on DP1_HPD to prevent back-drive current from damaging the Module.
DP2_AUX+	C32	DP Port 2, Bidirectional Channel used for Link Management and Device Control	I/O PCIE	PD 100K	AC coupled on Module
DP2_AUX-	C33	DP Port 2, Bidirectional Channel used for Link Management and Device Control	I/O PCIE	PU 100K	AC coupled on Module
DDI2_DDC_AUX_SEL	C34	Strapping Signal to select HDMI or DP output 1M pull-down on the module and floating on the carrier that enables DisplayPort mode	I 3.3V	PD 1M	DP mode enabled

4.4.4.2. HDMI Mode

Name	Pin #	Description	I/O	PU / PD	Comment
TMDS2_DATA2+ TMDS2_DATA2- TMDS2_DATA1+ TMDS2_DATA1- TMDS2_DATA0+ TMDS2DATA0-	D39 D40 D42 D43 D46 D47	HDMI / DVI Port, Differential Pair Data Lines	O PCIE		AC coupled off Module 100 nF DC blocking capacitors shall be placed on the Carrier
TMDS2_CLK+ TMDS2_CLK-	D49 D50	HDMI Port, Differential Pair Clock Lines			
HDM2_HPD	D44	Detection of Hot Plug / Unplug and notification of the link layer	I 3.3V	PD 100K	
HDMI2_CTRLCLK	C32	I2C_CLK Line for HDMI	I/O PCIE	PU 2.2K	AC couple on Module
HDMI2_CTRLDATA	C33	I2C_DAT Line for HDMI	I/O PCIE	PU 2.2K	AC couple on Module
DDI2_DDC_AUX_SEL	C34	Strapping Signal to select HDMI or DP output 1M pull-down on the module and floating on the carrier that enables DisplayPort mode	I 3.3V	PD 1M	HDMI mode enabled

4.4.5 DDI3 Port

Name	Pin #	DisplayPort (DP)	HDMI
DDI3_PAIR0+ DDI3_PAIR0-	C39 C40	DP3_LANE0+ DP3_LANE0-	TMDS3_DATA2+ TMDS3_DATA2-
DDI3_PAIR1+ DDI3_PAIR1-	C42 C43	DP3_LANE1+ DP3_LANE1-	TMDS3_DATA1+ TMDS3_DATA1-
DDI3_PAIR2+ DDI3_PAIR2-	C46 C47	DP3_LANE2+ DP3_LANE2-	TMDS3_DATA0+ TMDS3_DATA0-
DDI3_PAIR3+ DDI3_PAIR3-	C49 C50	DP3_LANE3+ DP3_LANE3-	TMDS3_CLK+ TMDS3_CLK-
DDI3_HPD	C44	DP3_HPD	HDMI3_HPD
DDI3_CTRLCLK_AUX+	C36	DP3_AUX+	HMDI3_CTRLCLK
DDI3_CTRLCLK_AUX-	C37	DP3_AUX-	HMDI3_CTRLDATA
DDI3_DDC_AUX_SEL	C38	DDI3_DDC_AUX_SEL	DDI3_DDC_AUX_SEL

Note:
Dual Mode (HDMI and DisplayPort on the same pins) implementations may be realized. This is desirable for SOCs that natively implement this capability. With such SOCs, the primary Dual Mode implementation challenge is that the HDMI_CTRL_DAT and HDMI_CTRL_CK lines are DC coupled, but the DP_AUX+ /- pair must be AC coupled. A set of FET switches is usually used to sort this out. The FET gates can be controlled by the AUX_SEL pin function.

4.4.5.1. DisplayPort (DP) Mode

Name	Pin #	Description	I/O	PU / PD	Comment
DP3_LANE0+ DP3_LANE0- DP3_LANE1+ DP3_LANE1- DP3_LANE2+ DP3_LANE2- DP3_LANE3+ DP3_LANE3-	C39 C40 C42 C43 C46 C47 C49 C50	DP Port 3, differential pair data lines	O PCIE		AC coupled off Module 100 nF DC blocking capacitors shall be placed on the Carrier
DP3_HPD	C44	DP Port 3, detection of Hot Plug / Unplug and notification of the link layer	I 3.3V	PD 100K	Module must tolerate high level in stand-by mode. The carrier board shall include a blocking FET on DP1_HPD to prevent back-drive current from damaging the Module.
DP3_AUX+	C36	DP Port 3, Bidirectional Channel used for Link Management and Device Control	I/O PCIE	PD 100K	AC coupled on Module
DP3_AUX-	C37	DP Port 3, Bidirectional Channel used for Link Management and Device Control	I/O PCIE	PU 100K	AC coupled on Module
DDI3_DDC_AUX_SEL	C38	Strapping Signal to select HDMI or DP output 1M pull-down on the module and floating on the carrier that enables DisplayPort mode	I 3.3V	PD 1M	DP mode enabled

4.4.5.2. HDMI Mode

Name	Pin #	Description	I/O	PU / PD	Comment
TMDS3_DATA2+ TMDS3_DATA2- TMDS3_DATA1+ TMDS3_DATA1- TMDS3_DATA0+ TMDS3_DATA0-	C39 C40 C42 C43 C46 C47	HDMI / DVI Port, Differential Pair Data Lines	O PCIE		AC coupled off Module 100 nF DC blocking capacitors shall be placed on the Carrier
TMDS3_CLK+ TMDS3_CLK-	C49 C50	HDMI Port, Differential Pair Clock Lines			
HDM3_HPD	C44	Detection of Hot Plug / Unplug and notification of the link layer	I 3.3V	PD 100K	
HDMI3_CTRLCLK	C36	I2C_CLK Line for HDMI	I/O PCIE	PU 2.2K	AC couple on Module
HDMI3_CTRLDATA	C37	I2C_DAT Line for HDMI	I/O PCIE	PU 2.2K	AC couple on Module
DDI3_DDC_AUX_SEL	C38	Strapping Signal to select HDMI or DP output 1M pull-down on the module and floating on the carrier that enables DisplayPort mode	I 3.3V	PD 1M	HDMI mode enabled

4.4.6 PCIe Graphics Port (PEG)

Name	Pin #	Description	I/O	PU / PD	Comment
PEG_TX0+ PEG_TX0-	D52 D53	PCI Express Graphics transmit differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	O PCIE		AC coupled on Module
PEG_RX0+ PEG_RX0-	C52 C53	PCI Express Graphics receive differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	I PCIE		AC coupled off Module
PEG_TX1+ PEG_TX1-	D55 D56	PCI Express Graphics transmit differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	O PCIE		AC coupled on Module
PEG_RX1+ PEG_RX1-	C55 C56	PCI Express Graphics receive differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	I PCIE		AC coupled off Module
PEG_TX2+ PEG_TX2-	D58 D59	PCI Express Graphics transmit differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	O PCIE		AC coupled on Module
PEG_RX2+ PEG_RX2-	C58 C59	PCI Express Graphics receive differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	I PCIE		AC coupled off Module
PEG_TX3+ PEG_TX3-	D61 D62	PCI Express Graphics transmit differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	O PCIE		AC coupled on Module
PEG_RX3+ PEG_RX3-	C61 C62	PCI Express Graphics receive differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	I PCIE		AC coupled off Module
PEG_TX4+ PEG_TX4-	D65 D66	PCI Express Graphics transmit differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	O PCIE		AC coupled on Module
PEG_RX4+ PEG_RX4-	C65 C66	PCI Express Graphics receive differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	I PCIE		AC coupled off Module
PEG_TX5+ PEG_TX5-	D68 D69	PCI Express Graphics transmit differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	O PCIE		AC coupled on Module

Name	Pin #	Description	I/O	PU / PD	Comment
PEG_RX5+ PEG_RX5-	C68 C69	PCI Express Graphics receive differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	I PCIE		AC coupled off Module
PEG_TX6+ PEG_TX6-	D71 D72	PCI Express Graphics transmit differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	O PCIE		AC coupled on Module
PEG_RX6+ PEG_RX6-	C71 C72	PCI Express Graphics receive differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	I PCIE		AC coupled off Module
PEG_TX7+ PEG_TX7-	D74 D75	PCI Express Graphics transmit differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	O PCIE		AC coupled on Module
PEG_RX7+ PEG_RX7-	C74 C75	PCI Express Graphics receive differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	I PCIE		AC coupled off Module
PEG_TX8+ PEG_TX8-	D78 D79	PCI Express Graphics transmit differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	O PCIE		AC coupled on Module
PEG_RX8+ PEG_RX8-	C78 C79	PCI Express Graphics receive differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	I PCIE		AC coupled off Module
PEG_TX9+ PEG_TX9-	D81 D82	PCI Express Graphics transmit differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	O PCIE		AC coupled on Module
PEG_RX9+ PEG_RX9-	C81 C82	PCI Express Graphics receive differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	I PCIE		AC coupled off Module
PEG_TX10+ PEG_TX10-	D85 D86	PCI Express Graphics transmit differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	O PCIE		AC coupled on Module
PEG_RX10+ PEG_RX10-	C85 C86	PCI Express Graphics receive differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	I PCIE		AC coupled off Module

Name	Pin #	Description	I/O	PU / PD	Comment
PEG_TX11+ PEG_TX11-	D88 D89	PCI Express Graphics transmit differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	O PCIE		AC coupled on Module
PEG_RX11+ PEG_RX11-	C88 C89	PCI Express Graphics receive differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	I PCIE		AC coupled off Module
PEG_TX12+ PEG_TX12-	D91 D92	PCI Express Graphics transmit differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	O PCIE		AC coupled on Module
PEG_RX12+ PEG_RX12-	C91 C92	PCI Express Graphics receive differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	I PCIE		AC coupled off Module
PEG_TX13+ PEG_TX13-	D94 D95	PCI Express Graphics transmit differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	O PCIE		AC coupled on Module
PEG_RX13+ PEG_RX13-	C94 C95	PCI Express Graphics receive differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	I PCIE		AC coupled off Module
PEG_TX14+ PEG_TX14-	D98 D99	PCI Express Graphics transmit differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	O PCIE		AC coupled on Module
PEG_RX14+ PEG_RX14-	C98 C99	PCI Express Graphics receive differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	I PCIE		AC coupled off Module
PEG_TX15+ PEG_TX15-	D101 D102	PCI Express Graphics transmit differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	O PCIE		AC coupled on Module
PEG_RX15+ PEG_RX15-	C101 C102	PCI Express Graphics receive differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	I PCIE		AC coupled off Module
PEG_LANE_RV#	D54	PCI Express Graphics lane reversal input strap. Pull low on the Carrier Board to reverse lane order.	I 3.3V		

Note: PEG slot is suitable for GPU, NVMe SSD.

4.4.7 Module Type Definition

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

4.4.8 Power and Ground

Name	Pin #	Description	I/O	PU / PD	Comment
VCC_12V	C104, C105, C106, C107, C108, C109, D104, D105, D106, D107, D108, D109	Primary power input supports wide range 5~ 20V input. All available VCC_12V pins on the connector(s) shall be used.	P		8.5-20 V
GND	C1, C2, C5, C8, C11, C14, C21, C31, C41, C51, C60, C70, C73, C76, C80, C84, C87, C90, C93, C96, C100, C103, C110, D1, D2, D5, D8, D11, D14, D21, D31, D41, D51, D60, D67, D70, D73, D76, D80, D84, D87, D90, D93, D96, D100, D103, D110	Ground - DC power and signal and AC signal return path.	P		

5. Additional Features

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

5.1. Module Feature Locations

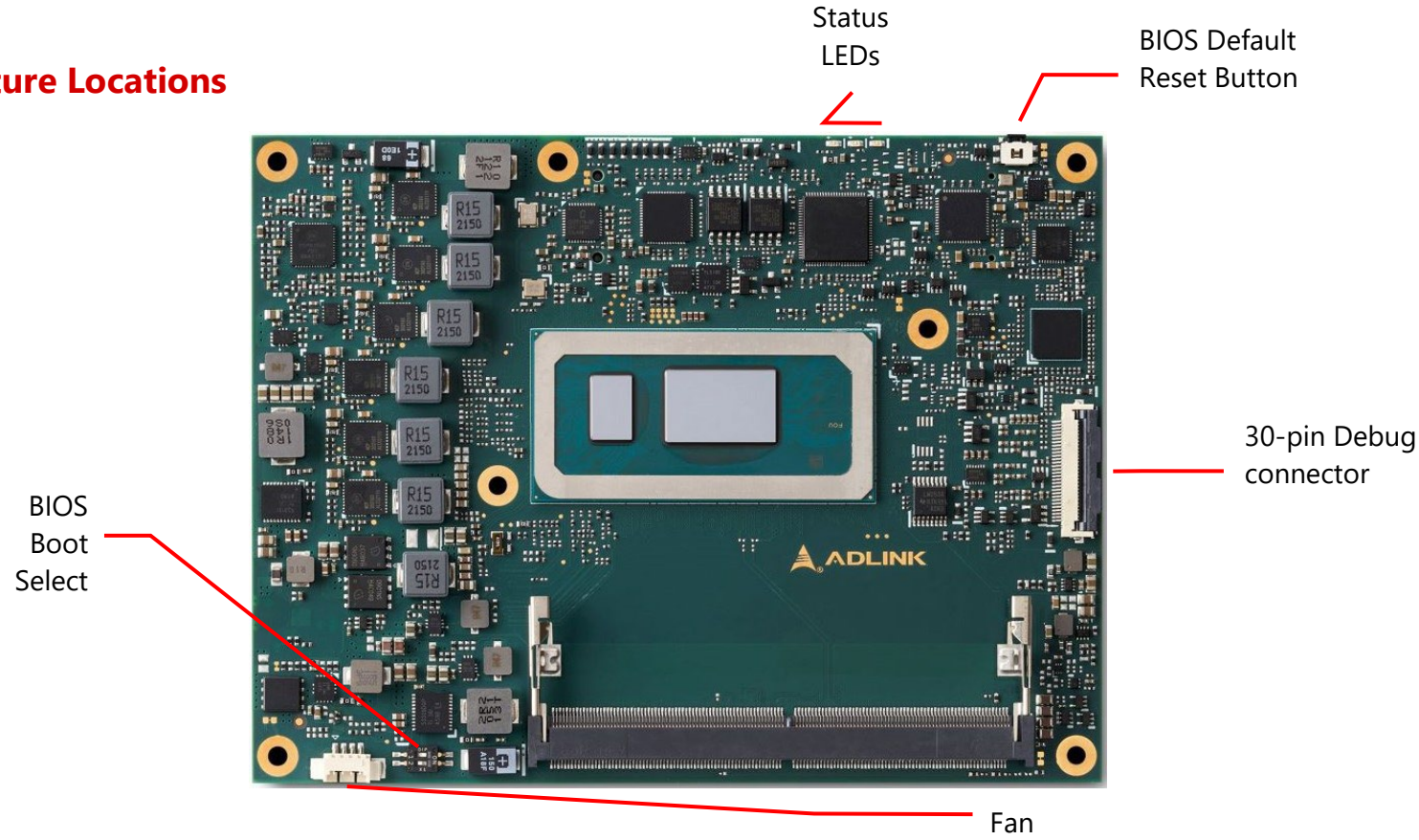


Figure 3 – Module feature locations (top side)

5.2. Debug Connector

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

- Test points measurement of internal power rails
- SPI BIOS programming interface
- Embedded Controller programming interface

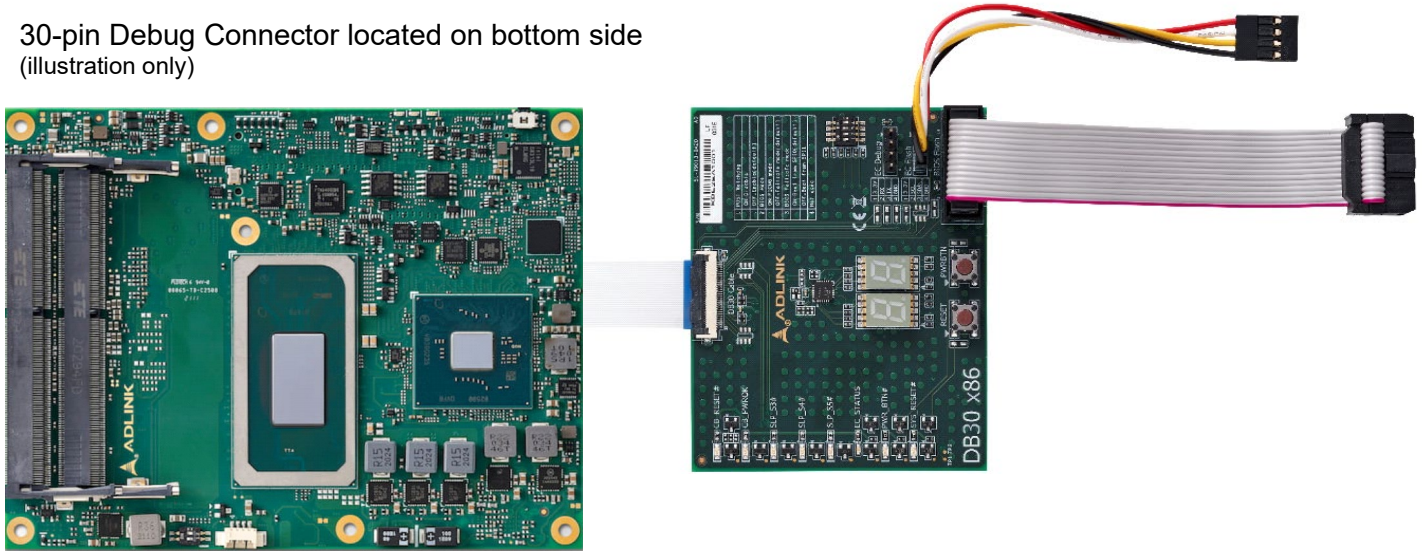
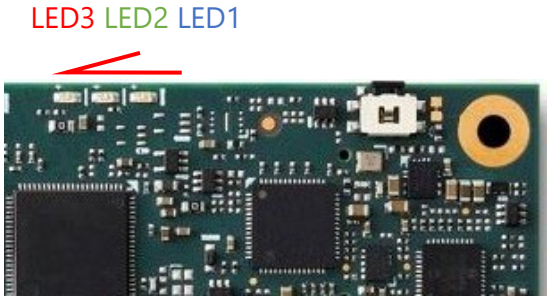


Figure 4 – Express-ADP and Debug Module

5.3. Status LEDs

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



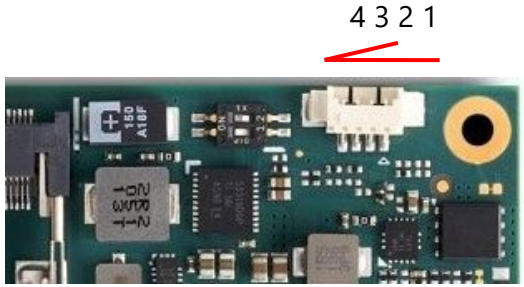
Name	Color	Connection	Function
LED1	Blue	EC output	Power Sequence Status Code (EC) Power Changes, RESET (see Exception Codes below)
LED2	Green	Power Source 3Vcc	S0 LED ON S3/S4/S5 LED OFF ECO mode LED OFF
LED3	Red	EC output and same signal as WDT (B27) on BtB connector	Module power up WD LED = LED OFF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

5.4. 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

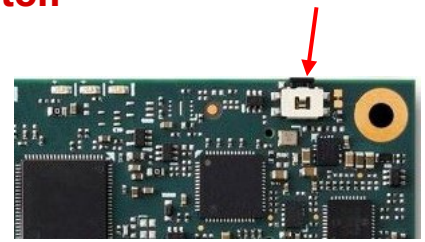
5.5. Fan Connector

Connector type: JVE 24W1125A-04M00



Name	Description
1	FAN_PWMOUT
2	FAN_TACHIN
3	GND
4	12V

5.6. BIOS Default Reset Button



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

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

5.7. BIOS Boot Select

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

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

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

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

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

6. System Resources

6.1. System Memory Map

Address Range (hex)	Description
FFE00000 – FFFFFFFF	High BIOS Area
FEE00000 – FEEFFFFF	MSI Interrupt
FEC00000 – FECFFFFF	APIC Configuration Space
F00000 – FFFFFF	ISA Hole
100000 – EFFFFF	Main Memory
0K – 1MB	DOS Compatibility Memory

6.2. I/O Map

Hex Range	Device
000h-CF7h	PCIe Root Complex
020h – 02Dh & 030h – 03Dh	Programmable Interrupt Controller
02Eh – 02Fh	Motherboard Resource
040h – 043h & 050h – 053h	System Timer
04Eh – 04Fh	Motherboard Resource
060h, 064h	8042 Equivalent (keyboard)
061h, 063h, 065h, 067h, 070h,080h,92h	Motherboard Resource
062h, 066h	Embedded Controller

Hex Range	Device
0A0h – 0A1h & 0A4h – 0A5h, 0A8h – 0A9h & 0ACh – 0ADh, & 0B0h – 0B1h & 0B4h – 0B5h & 0B8h – 0B9h & 0BCh – 0BDh	Programmable Interrupt Controller
240h – 247h	Serial Port 3
248h – 24Fh	Serial Port 4
2F8h – 2FFh	Serial Port 2
3F8h – 3FFh	Serial Port 1
4D0h-4D1h	Programmable Interrupt Controller
680h-69Fh, A00h-A1Fh, A20h-A2Fh, A30h-A3Fh, A40h-A4Fh, A50h-A5Fh, A60h-A6Fh	Motherboard Resource
0D00h- – FFFFh	PCIe Root Complex
164Eh – 164Fh,1800h-18FEh,1854h-1857h,2000h-20FEh	Motherboard Resource
03000h-303Fh	Intel Graphics Driver
03060h – 307Fh, 03080h-03083h, 3090h-3097h	SATA AHCI Controller
EFA0h-EFBFh	SMBUS
FFF8h-FFFFh	AMT SOL Serial COM 5

6.3. Interrupt Request (IRQ) Lines

APIC Mode

IRQ#	Typical Interrupt Resource	Connected to Pin	Available
0	Counter 0	N/A	No
1	Keyboard Controller	IRQ1 via SERIRQ	No
2	N/A	N/A	No
3	Serial Port 2 (COM2)	IRQ3 via SERIRQ	Note (1)
4	Serial Port 1 (COM1)	IRQ4 via SERIRQ	Note (1)
5	Serial Port 3 (COM3)	IRQ5 via SERIRQ	Note (1)
6	N/A	N/A	Note (1)
7	Serial Port 4 (COM4)	IRQ7 via SERIRQ	Note (1)
8	Real-Time clock	N/A	No
9	Generic	N/A	Note (1)
10	N/A	N/A	Note (1)
11	N/A	N/A	Note (1)
12	PS/2 Mouse	IRQ12 via SERIRQ	Note (1)
13	Numeric data processor	N/A	Note (1)
14	Generic	IRQ14 via SERIRQ	Note (1)
15	N/A	IRQ15 via SERIRQ	Note (1)
16-511	Microsoft ACPI-Compliant System	P.E.G Root Port, Intel HDA, PCIE Port 0/1/2/3/4/5/6, I.G.D., XHCI Controller	Note (1)

Note (1): These IRQs can be used for PCI devices when onboard device is disabled.

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	Processor Graphics
00h	04h	00h	Internal	Intel Data Acquisition/Signal Processor
00h	06h	00h	Internal	PCI Express* Controller (x4 PCIe)
00h	06h	02h	Internal	PCI Express* Controller (x4 PCIe)
00h	08h	00h	Internal	Intel System Peripherals
00h	14h	00h	Internal	Intel USB 3.0 XHCI
00h	14h	02h	Internal	Intel RAM
00h	15h	00h	Internal	Intel Serial Bus Controller
00h	15h	01h	Internal	Intel Serial Bus Controller
00h	16h	00h	Internal	Intel Communication Device
00h	16h	03h	Internal	Intel 16550 Serial Controller
00h	17h	00h	Internal	Intel AHCI 1.0 Controller
00h	1Ch	00h	Internal	Intel PCI Express
00h	1Dh	00h	Internal	Intel PCI Express
00h	1Dh	01h	Internal	Intel PCI Express
00h	1Fh	00h	Internal	Intel ISA Bridge
00h	1Fh	03h	Internal	Intel Multimedia
00h	1Fh	04h	Internal	Intel SMBUS
00h	1Fh	05h	Internal	Intel Serial BUS Controller

6.5. PCI Interrupt Routing Map

INT Line	Audio Controller	xHCI Controller	CSME Controller	eSPI Controller	SATA Controller	SMBus Controller
Int0	INTA: 16	INTA: 16	INTA: 16	INTA: None	INTA: 16	INTA: 16
Int1		INTB: 17	INTB: 17			
Int2		INTC: 18	INTC: 18			
Int3		INTD: 19	INTD: 19			

INT Line	PCIe Port 5	PCIe Port6	PCIe Port 7	PCIe Port 8	PCIe Port 9	PCIe Port 10
Int0	INTA: 16	INTB: 17	INTC: 18	INTD: 19	INTA: 16	INTB: 17
Int1	INTB: 17	INTC: 18	INTD: 19	INTA: 16	INTB: 17	INTC: 18
Int2	INTC: 18	INTD: 19	INTA: 16	INTB: 17	INTC: 18	INTD: 19
Int3	INTD: 19	INTA: 16	INTB: 17	INTC: 18	INTD: 19	INTA: 16

6.6. SMBus Address Table

Device	Address
DIMM A	0A0h
DIMM B	0A4h
PTN3460	0C0h

7. BIOS Setup

7.1. Menu Structure

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

Main	Advanced	Chipset	Security	Boot	Save & Exit
BIOS Information System Information Board Information ► System Date System Time	CPU Configuration ► Power & Performance ► Graphics Configuration ► Power Management ► System Management ► Thermal Management ► Watchdog Timer ► Super IO Configuration ► Miscellaneous ► USB Configuration ► NVMe Configuration ► AMI Graphic Output Protocol Policy ► Serial Port Console Redirection ► Network Stack Configuration ► Trusted Computing ►	System Agent (SA) Configuration ► PCH-IO Configuration ►	Password Description Secure Boot Menu ►	Boot Configuration	Save Options Boot Override

Note: indicates a submenu Gray text indicates info only

7.2. Main

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

7.2.1 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	ADLINK BIOS Version
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
Stepping	Info only	Display CPU Stepping
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 PCH Information.
Board Information	Submenu	

7.2.3 Board Information

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

7.3. Advanced

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

7.3.1 CPU Configuration

Feature	Options	Description
ID	Info only	Display CPU information.
Brand String	Info only	Display CPU brand string.
Microcode Revision	Info only	Display CPU microcode revision.
VMX	Info only	Display Intel Virtualization Technology support status.
SMX/TXT	Info only	Display Intel SMX Technology support status.
Intel (VMX) Virtualization Technology	Disabled, **Enabled**	When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.
Active Performance-Cores	**All,** 3, 2, 1	Number of P-cores to enable in each processor package.
Active Processor Cores	**All**, 7, 6, 5, 4, 3, 2, 1, 0	Number of E-cores to enable in each processor package.
Hyper-Threading	Disabled, **Enabled**	Enable or Disable Hyper-Threading Technology.

Feature	Options	Description
Intel Trusted Execution Technology	**Disabled**, Enabled	Enables utilization of additional hardware capabilities provided by Intel (R) Trusted Execution Technology.
Total Memory Encryption	**Disabled,** Enabled	Configure Toral Memory Encryption (TME) to protect DRAM data from physical attacks.

7.3.2 Power & Performance Configuration

7.3.2.1. CPU - Power Management Control

Feature	Options	Description
Boot Performance Mode	Max Battery, Max Non-Turbo Performance, **Turbo Performance**	Selects the performance state that the BIOS will set starting from the reset vector.
Intel(R) SpeedStep(TM)	Disabled, **Enabled**	Allows more than two frequency ranges to be supported.
Race To Halt (RTH)	Disabled, **Enabled**	Enables/Disables the 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)
Intel(R) Speed Shift Technology	Disabled, **Enabled**	Enables/Disables Intel(R) Speed Shift Technology support. Enabling it will expose the CPPC v2 interface to allow for hardware-controlled P-states.
Per Core P State OS control mode	Disabled, **Enabled**	Enables/Disables Per Core P state OS control mode. Disabling it will set Bit 31 = 1 command 0x06. When set, the highest core request is used for all other core requests.
HwP Autonomous Per Core P state	Disabled, **Enabled**	Disabling Autonomous PCPS (Bit 30 = 1, command 0x11) means it will request the same value for all cores at all times. Enable PCPS (default Bit 30 = 0, command 0x11)
HwP Autonomous EPP Grouping	Disabled, **Enabled**	Enables EPP grouping (default Bit 29 =0, command 0x11) Autonomous will request the same values for all cores with the same EPP. Disables EPP grouping (Bit 29 =1 , command 0x11) autonomous will not necessarily request the same values for all cores with the same EPP.
EPB override over PECI	**Disabled**, Enabled	Enables/Disables EPB override over PECI. Enable it by sending pcode command 0x2b , subcommand 0x3 to 1. This will allow OOB EPB PECI override control.

Feature	Options	Description
HwP Lock	Disabled, **Enabled**	Enables/Disables HwP Lock support in Misc Power Management MSR
HDC Control	Disabled, **Enabled**	This option allows HDC configuration. Disabled: Disables HDC Enabled: Can be enabled by OS if OS native support is available.
Turbo Mode	Disabled, **Enabled**	Enables/Disables processor Turbo Mode (requires EMTTM enabled too). AUTO means enabled.
View/Configure Turbo Options	Submenu	
Turbo Ratio Limit Options	Submenu	
Current Turbo Ratio Limit Settings	Current Turbo Ratio Limit Settings	Current Turbo Ratio Limit Settings
P-core Turbo Ratio Limit Numcore0	1	
P-core Turbo Ratio Limit Numcore1	2	
P-core Turbo Ratio Limit Numcore2	3	
P-core Turbo Ratio Limit Numcore3	4	
P-core Turbo Ratio Limit Numcore4	5	
P-core Turbo Ratio Limit Numcore5	6	
P-core Turbo Ratio Limit Numcore6	7	
P-core Turbo Ratio Limit Numcore7	8	
P-core Turbo Ratio Limit Ratio0	45	
P-core Turbo Ratio Limit Ratio1	45	

Feature	Options	Description
P-core Turbo Ratio Limit Ratio2	38	
P-core Turbo Ratio Limit Ratio3	35	
P-core Turbo Ratio Limit Ratio4	35	
P-core Turbo Ratio Limit Ratio5	35	
P-core Turbo Ratio Limit Ratio6	35	
P-core Turbo Ratio Limit Ratio7	35	
E-core Turbo Ratio Limit Numcore0	1	
E-core Turbo Ratio Limit Numcore1	2	
E-core Turbo Ratio Limit Numcore2	3	
E-core Turbo Ratio Limit Numcore3	4	
E-core Turbo Ratio Limit Numcore4	5	
E-core Turbo Ratio Limit Numcore5	6	
E-core Turbo Ratio Limit Numcore6	7	
E-core Turbo Ratio Limit Numcore7	8	
E-core Turbo Ratio Limit Ratio0	33	
E-core Turbo Ratio Limit Ratio1	33	
E-core Turbo Ratio Limit Ratio2	33	

Feature	Options	Description
E-core Turbo Ratio Limit Ratio3	33	
E-core Turbo Ratio Limit Ratio4	31	
E-core Turbo Ratio Limit Ratio5	31	
E-core Turbo Ratio Limit Ratio6	31	
E-core Turbo Ratio Limit Ratio7	31	
P-core Turbo Ratio Limit Numcore0	1	Performance-core Turbo Ratio Limit Numcore0 defines the core range, the turbo ratio is defined in Turbo Ratio Limit Ratio0. If value is zero, this entry is ignored.
P-core Turbo Ratio Limit Numcore1	2	Performance-core Turbo Ratio Limit Numcore1 defines the core range, the turbo ratio is defined in Turbo Ratio Limit Ratio1. If value is zero, this entry is ignored.
P-core Turbo Ratio Limit Numcore2	3	Performance-core Turbo Ratio Limit Numcore2 defines the core range, the turbo ratio is defined in Turbo Ratio Limit Ratio2. If value is zero, this entry is ignored.
P-core Turbo Ratio Limit Numcore3	4	Performance-core Turbo Ratio Limit Numcore3 defines the core range, the turbo ratio is defined in Turbo Ratio Limit Ratio3. If value is zero, this entry is ignored.
P-core Turbo Ratio Limit Numcore4	5	Performance-core Turbo Ratio Limit Numcore4 defines the core range, the turbo ratio is defined in Turbo Ratio Limit Ratio4. If value is zero, this entry is ignored.
P-core Turbo Ratio Limit Numcore5	6	Performance-core Turbo Ratio Limit Numcore5 defines the core range, the turbo ratio is defined in Turbo Ratio Limit Ratio5. If value is zero, this entry is ignored.
P-core Turbo Ratio Limit Numcore6	7	Performance-core Turbo Ratio Limit Numcore6 defines the core range, the turbo ratio is defined in Turbo Ratio Limit Ratio6. If value is zero, this entry is ignored.
P-core Turbo Ratio Limit Numcore7	8	Performance-core Turbo Ratio Limit Numcore7 defines the core range, the turbo ratio is defined in Turbo Ratio Limit Ratio7. If value is zero, this entry is ignored.
P-core Turbo Ratio Limit Ratio0	45	Performance-core Turbo Ratio Limit Ratio0 defines the turbo ratio (max is 85 in normal mode and 120 in core extension mode), the core range is defined in Turbo Ratio Limit Numcore0.
P-core Turbo Ratio Limit Ratio1	45	Performance-core Turbo Ratio Limit Ratio1 defines the turbo ratio (max is 85 in normal mode and 120 in core extension mode), the core range is defined in Turbo Ratio Limit Numcore1.

Feature	Options	Description
P-core Turbo Ratio Limit Ratio2	38	Performance-core Turbo Ratio Limit Ratio2 defines the turbo ratio (max is 85 in normal mode and 120 in core extension mode), the core range is defined in Turbo Ratio Limit Numcore2.
P-core Turbo Ratio Limit Ratio3	35	Performance-core Turbo Ratio Limit Ratio3 defines the turbo ratio (max is 85 in normal mode and 120 in core extension mode), the core range is defined in Turbo Ratio Limit Numcore3.
P-core Turbo Ratio Limit Ratio4	35	Performance-core Turbo Ratio Limit Ratio4 defines the turbo ratio (max is 85 in normal mode and 120 in core extension mode), the core range is defined in Turbo Ratio Limit Numcore4.
P-core Turbo Ratio Limit Ratio5	35	Performance-core Turbo Ratio Limit Ratio5 defines the turbo ratio (max is 85 in normal mode and 120 in core extension mode), the core range is defined in Turbo Ratio Limit Numcore5.
P-core Turbo Ratio Limit Ratio6	35	Performance-core Turbo Ratio Limit Ratio6 defines the turbo ratio (max is 85 in normal mode and 120 in core extension mode), the core range is defined in Turbo Ratio Limit Numcore6.
P-core Turbo Ratio Limit Ratio7	35	Performance-core Turbo Ratio Limit Ratio7 defines the turbo ratio (max is 85 in normal mode and 120 in core extension mode), the core range is defined in Turbo Ratio Limit Numcore7.
E-core Turbo Ratio Limit Numcore0	1	Efficient-core Turbo Ratio Limit Numcore0 defines the core range, the turbo ratio is defined in E-core Turbo Ratio Limit Ratio0. If value is zero, this entry is ignored.
E-core Turbo Ratio Limit Numcore1	2	Efficient-core Turbo Ratio Limit Numcore1 defines the core range, the turbo ratio is defined in E-core Turbo Ratio Limit Ratio1. If value is zero, this entry is ignored.
E-core Turbo Ratio Limit Numcore2	3	Efficient-core Turbo Ratio Limit Numcore2 defines the core range, the turbo ratio is defined in E-core Turbo Ratio Limit Ratio2. If value is zero, this entry is ignored.
E-core Turbo Ratio Limit Numcore3	4	Efficient-core Turbo Ratio Limit Numcore3 defines the core range, the turbo ratio is defined in E-core Turbo Ratio Limit Ratio3. If value is zero, this entry is ignored.
E-core Turbo Ratio Limit Numcore4	5	Efficient-core Turbo Ratio Limit Numcore4 defines the core range, the turbo ratio is defined in E-core Turbo Ratio Limit Ratio4. If value is zero, this entry is ignored.
E-core Turbo Ratio Limit Numcore5	6	Efficient-core Turbo Ratio Limit Numcore5 defines the core range, the turbo ratio is defined in E-core Turbo Ratio Limit Ratio5. If value is zero, this entry is ignored.
E-core Turbo Ratio Limit Numcore6	7	Efficient-core Turbo Ratio Limit Numcore6 defines the core range, the turbo ratio is defined in E-core Turbo Ratio Limit Ratio6. If value is zero, this entry is ignored.
E-core Turbo Ratio Limit Numcore7	8	Efficient-core Turbo Ratio Limit Numcore7 defines the core range, the turbo ratio is defined in E-core Turbo Ratio Limit Ratio7. If value is zero, this entry is ignored.

Feature	Options	Description
E-core Turbo Ratio Limit Ratio0	80	Efficient-core Turbo Ratio Limit Ratio0 defines the turbo ratio (max is 85 irrespective of the core extension mode), the core range is defined in E-core Turbo Ratio Limit Numcore0.
E-core Turbo Ratio Limit Ratio1	80	Efficient-core Turbo Ratio Limit Ratio1 defines the turbo ratio (max is 85 irrespective of the core extension mode), the core range is defined in E-core Turbo Ratio Limit Numcore1.
E-core Turbo Ratio Limit Ratio2	80	Efficient-core Turbo Ratio Limit Ratio2 defines the turbo ratio (max is 85 irrespective of the core extension mode), the core range is defined in E-core Turbo Ratio Limit Numcore2.
E-core Turbo Ratio Limit Ratio3	80	Efficient-core Turbo Ratio Limit Ratio3 defines the turbo ratio (max is 85 irrespective of the core extension mode), the core range is defined in E-core Turbo Ratio Limit Numcore3.
E-core Turbo Ratio Limit Ratio4	80	Efficient-core Turbo Ratio Limit Ratio4 defines the turbo ratio (max is 85 irrespective of the core extension mode), the core range is defined in E-core Turbo Ratio Limit Numcore4.
E-core Turbo Ratio Limit Ratio5	80	Efficient-core Turbo Ratio Limit Ratio5 defines the turbo ratio (max is 85 irrespective of the core extension mode), the core range is defined in E-core Turbo Ratio Limit Numcore5.
E-core Turbo Ratio Limit Ratio6	80	Efficient-core Turbo Ratio Limit Ratio6 defines the turbo ratio (max is 85 irrespective of the core extension mode), the core range is defined in E-core Turbo Ratio Limit Numcore6.
E-core Turbo Ratio Limit Ratio7	80	Efficient-core Turbo Ratio Limit Ratio7 defines the turbo ratio (max is 85 irrespective of the core extension mode), the core range is defined in E-core Turbo Ratio Limit Numcore7.
Energy Efficient P-state	Disabled, **Enabled**	Enables/Disables Energy Efficient P-state feature. When set to 0, it 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, it will enable access to ENERGY_PERFORMANCE_BIAS MSR 1B0h and CPUID Fun
Package Power Limit MSR Lock	**Disabled**, Enabled	Enables/Disables 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.
Energy Efficient Turbo	Disabled, **Enabled**	Enables/Disables 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.
Config TDP Configurations	Submenu	
Config TDP Configurations	Config TDP Configurations	Config TDP Configurations

Feature	Options	Description
Enable Configurable TDP	Applies to non-cTDP, **Applies to cTDP**	Applies TDP initialization settings based on non-cTDP or cTDP. Default is 1: Applies to cTDP; if 0 then applies non-cTDP and BIOS will bypass cTDP initialization flow
Configurable TDP Boot Mode	**Nominal**, Down2, Down1, Deactivate	Configurable Processor Base Power (cTDP) Mode as Nominal/Up/Down/Deactivate TDP selection. Deactivate option will set MSR to Nominal and MMIO to Zero.
Configurable TDP Lock	Enabled, **Disabled**	Configurable TDP Mode Lock sets the Lock bits on TURBO_ACTIVATION_RATIO and CONFIG_TDP_CONTROL. Note: When cTDP Lock is enabled Custom Config TDP Count will be forced to 1 and Custom Config TDP Boot Index will be forced to 0.
Config TDP Levels	3	
Config TDP Turbo Activation Ratio	27 (Unlocked)	
Power Limit 1	28.0W (MSR:28.0)	
Power Limit 2	64.0W (MSR:64.0)	
Custom Settings Nominal		
Config TDP Nominal	Ratio:28 TAR:27 PL1:28.0W	
Power Limit 1	[Max-Value, Min-Value, Step-Value] = [0x003E7F83, 0x00000000, 0x0000007D]	Power Limit 1 in Milli Watts. BIOS will round to the nearest 1/8W when programming. 0 = no custom override. For 12.50W, enter 12500. Overclocking SKU: Value must be between Max and Min Power Limits (specified by PACKAGE_POWER_SKU_MSR). Other SKUs: This value must be between Min Power Limit and TDP
Power Limit 2	[Max-Value, Min-Value, Step-Value] = [0x003E7F83, 0x00000000, 0x0000007D]	Power Limit 2 value in Milli Watts. BIOS will round to the nearest 1/8W when programming. 0 = no custom override. For 12.50W, enter 12500. Processor applies control policies such that the package power does not exceed this limit.
Power Limit 1 Time Window	0, 1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 14, 16, 20, 24, 28, 32, 40, 48, 56, 64,	Power Limit 1 Time Window value in seconds. The value may vary from 0 to 128. 0 = default value (28 sec for Mobile and 8 sec for Desktop). Defines the time window in which the TDP value should be maintained.

Feature	Options	Description
	80, 96, 112, 128	
Config TDP Turbo Activation Ratio	[Max-Value, Min-Value, Step-Value] = [0xFF, 0x00, 0x01]	Custom value for Turbo Activation Ratio. Needs to be configured with valid values from LFM to Max Turbo. 0 means don't use custom value.
Custom Settings Down		
Config TDP Level1	Ratio:12 TAR:11 PL1:12.0W	
Power Limit 1	[Max-Value, Min-Value, Step-Value] = [0x003E7F83, **0x00000000**, 0x0000007D]	Power Limit 1 in Milli Watts. BIOS will round to the nearest 1/8W when programming. 0 = no custom override. For 12.50W, enter 12500. Overclocking SKU: Value must be between Max and Min Power Limits (specified by PACKAGE_POWER_SKU_MSR). Other SKUs: This value must be between Min Power Limit and TDP
Power Limit 2	[Max-Value, Min-Value, Step-Value] = [0x003E7F83, **0x00000000**, 0x0000007D]	Power Limit 2 value in Milli Watts. BIOS will round to the nearest 1/8W when programming. 0 = no custom override. For 12.50W, enter 12500. Processor applies control policies such that the package power does not exceed this limit.
Power Limit 1 Time Window	**0**, 1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 14, 16, 20, 24, 28, 32, 40, 48, 56, 64, 80, 96, 112, 128	Power Limit 1 Time Window value in seconds. The value may vary from 0 to 128. 0 = default value (28 sec for Mobile and 8 sec for Desktop). Defines the time window in which the TDP value should be maintained.
Config TDP Turbo Activation Ratio	[Max-Value, Min-Value, Step-Value] = [0xFF, **0x00**, 0x01]	Custom value for Turbo Activation Ratio. Needs to be configured with valid values from LFM to Max Turbo. 0 means don't use custom value.
Custom Settings Up		
Config TDP Level2	Ratio:19 TAR:18 PL1:35.0W	
Power Limit 1	[Max-Value, Min-Value, Step-Value] =	Power Limit 1 in Milli Watts. BIOS will round to the nearest 1/8W when programming. 0 = no custom override. For 12.50W, enter 12500. Overclocking SKU: Value must be between Max and Min Power Limits (specified by

Feature	Options	Description
	[0x003E7F83, **0x00000000**, 0x0000007D]	PACKAGE_POWER_SKU_MSR). Other SKUs: This value must be between Min Power Limit and TDP
Power Limit 2	[Max-Value, Min-Value, Step-Value] = [0x003E7F83, **0x00000000**, 0x0000007D]	Power Limit 2 value in Milli Watts. BIOS will round to the nearest 1/8W when programming. 0 = no custom override. For 12.50W, enter 12500. Processor applies control policies such that the package power does not exceed this limit.
Power Limit 1 Time Window	**0**, 1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 14, 16, 20, 24, 28, 32, 40, 48, 56, 64, 80, 96, 112, 128	Power Limit 1 Time Window value in seconds. The value may vary from 0 to 128. 0 = default value (28 sec for Mobile and 8 sec for Desktop). Defines the time window in which the TDP value should be maintained.
Config TDP Turbo Activation Ratio	[Max-Value, Min-Value, Step-Value] = [0xFF, **0x00**, 0x01]	Custom value for Turbo Activation Ratio. Needs to be configured with valid values from LFM to Max Turbo. 0 means don't use custom value.
CPU VR Settings	Submenu	
CPU VR Settings		
Current VccIn Aux Icc Max	128	
PSYS Slope	[Max-Value, Min-Value, Step-Value] = [0xC8, **0x00**, 0x01]	PSYS Slope is defined in 1/100 increments. The range is from 0-200. For a 1.25 slope, enter 125. 0 = AUTO. Uses BIOS VR mailbox command 0x9."
PSYS Offset	[Max-Value, Min-Value, Step-Value] = [0xF9FF, **0x0000**, 0x0001]	PSYS Offset is defined in 1/1000 increments. The range is from 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	[Max-Value, Min-Value, Step-Value] = [0x1FFF, **0x0000**,	PSYS PMax power, defined in 1/8 Watt increments. The range is from 0-8192. For a PMax of 125W, enter 1000. 0 = AUTO. Uses BIOS VR mailbox command 0xB.

Feature	Options	Description
	0x0001]	
Min Voltage Override	**Disabled**, Enabled	Min Voltage Override. Enable to override minimum voltage for runtime and for C8.
VccIn Aux Icc Max	[Max-Value, Min-Value, Step-Value] = [0x200, **0x00**, 0x00]	Sets the Max Icc VccIn Aux value defined in 1/4A increments. The range is from 0-512. For an IccMax 32A, enter 128(32*4).
VccIn Aux IMON Slope	[Max-Value, Min-Value, Step-Value] = [0xC8, **0x100**, 0x01]	VccIn Aux IMON Slope defined in 1/100 increments. The range is from 0-200. For a 1.25 slope, enter 125. 0 = AUTO. Uses BIOS VR mailbox command 0x1B.
VccIn Aux IMON Offset	[Max-Value, Min-Value, Step-Value] = [0xF9FF, **0x0000**, 0x0001]	VccIN Aux IMON Offset defined in 1/1000 increments. The range is from 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 Critical	**Disabled**, Enabled	Vsys Critical Enable or disable
VR Power Delivery Design	**AUTO**, ADL P 282 15W, ADL P 482 28W, ADL P 682 28W, ADL P 682 45W, ADL P 142 15W, ADL P 242 15W, ADL P 482 45W, ADL P 442 45W, ADL P 442 28W, ADL P 282 28W, ADL P 242 28W, ADL P 142 28W, ADL P 242 45W, ADL P 182 28W, ADL P 662 28W, ADL P 642 28W, ADL P 642 45W	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.
Acoustic Noise Settings	Submenu	

Feature	Options	Description
Acoustic Noise Mitigation	**Disabled**, Enabled	Enabling this option will help mitigate acoustic noise on certain SKUs when the CPU is in deeper C state
Pre Wake Time	[Max-Value, Min-Value, Step-Value] = [0xFF, **0x00**, 0x01]	Set the maximum Pre Wake randomization time in micro ticks. The range is from 0-255. This is for acoustic noise mitigation Dynamic Periodicity Alteration (DPA) tuning.
Ramp Up Time	[Max-Value, Min-Value, Step-Value] = [0xFF, **0x00**, 0x01]	Set the maximum Ramp Up randomization time in micro ticks. The range is from 0-255. This is for acoustic noise mitigation Dynamic Periodicity Alteration (DPA) tuning.
Ramp Down Time	[Max-Value, Min-Value, Step-Value] = [0xFF, **0x00**, 0x01]	Set the maximum Ramp Down randomization time in micro ticks. The range is from 0-255. This is for acoustic noise mitigation Dynamic Periodicity Alteration (DPA) tuning.
IA VR Domain		
Disable Fast PKG C State Ramp for IA Domain	FALSE	
Slow Slew Rate for IA Domain	Fast/2	
GT VR Domain		
Disable Fast PKG C State Ramp for GT Domain	FALSE	
Slow Slew Rate for GT Domain	Fast/2	
Core/IA VR Settings	Submenu	
Core/IA VR Domain		
VR Config Enable	Disabled, **Enabled**	VR Config Enable
Current AC Loadline	230	
Current DC Loadline	230	

Feature	Options	Description
Current Psi1 Threshold	80	
Current Psi2 Threshold	20	
Current Psi3 Threshold	4	
Current Imon Slope	0	
Current Imon Offset	1	
Current VR Current Limit	340	
Current TDC Current Limit	312	
Current Voltage Limit	1600	
AC Loadline	[Max-Value, Min-Value, Step-Value] = [0x1868, 0x0000, 0x0001], **0x0000**	AC Loadline defined in 1/100 mOhms. A value of 100 = 1.00 mOhm, and 1255 = 12.55 mOhm. The range is from 0-6249 (0-62.49 mOhms). 0 = AUTO/HW default. Uses BIOS mailbox command 0x2.
DC Loadline	[Max-Value, Min-Value, Step-Value] = [0x1868, 0x0000, 0x0001], **0x0000**	DC Loadline defined in 1/100 mOhms. A value of 100 = 1.00 mOhm, and 1255 = 12.55 mOhm. The range is from 0-6249 (0-62.49 mOhms). 0 = AUTO/HW default. Uses BIOS mailbox command 0x2.
PS Current Threshold1	[Max-Value, Min-Value, Step-Value] = [0x0200, 0x0000, 0x0001], **0x0080**	PS Current Threshold1, defined in 1/4 A increments. A value of 400 = 100A. The range is from 0-512, which translates to 0-128A. 0 = AUTO. Uses BIOS VR mailbox command 0x3.
PS Current Threshold2	[Max-Value, Min-Value, Step-Value] = [0x0200, 0x0000, 0x0001], **0x0020**	PS Current Threshold2, defined in 1/4 A increments. A value of 400 = 100A. The range is from 0-512, which translates to 0-128A. 0 = AUTO. Uses BIOS VR mailbox command 0x3.

Feature	Options	Description
PS Current Threshold3	[Max-Value, Min-Value, Step-Value] = [0x0200, 0x0000, 0x0001], **0x0004**	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, **Enabled**	PS3 Enable/Disable. 0 - Disabled, 1 - Enabled. Uses BIOS VR mailbox command 0x3.
PS4 Enable	Disabled, **Enabled**	PS4 Enable/Disable. 0 - Disabled, 1 - Enabled. Uses BIOS VR mailbox command 0x3
IMON Slope	[Max-Value, Min-Value, Step-Value] = [0x00C8, **0x0000**, 0x0001]	IMON Slope defined in 1/100 increments. The range is from 0-200. For a 1.25 slope, enter 125. 0 = AUTO. Uses BIOS VR mailbox command 0x4.
IMON Offset	[Max-Value, Min-Value, Step-Value] = [0xF9FF, **0x0000**, 0x0001]	IMON Offset defined in 1/1000 increments. The range is from 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	[Max-Value, Min-Value, Step-Value] = [0x03FF, **0x0000**, 0x0001]	Voltage Regulator Current Limit (Icc Max). 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	[Max-Value, Min-Value, Step-Value] = [0x1F3F, **0x0000**, 0x0001]	Voltage Limit (VMAX). This value represents the Maximum instantaneous voltage allowed at any given time. The range is from 0 - 7999mV. Uses BIOS VR mailbox command 0x8.
TDC Enable	Disabled, **Enabled**	TDC Enable. 0- Disable, 1 - Enable
TDC Current Limit	[Max-Value, Min-Value, Step-Value] = [0x7FFF, **0x0000**, 0x007D]	TDC Current Limit, defined in 1/8A increments. The range is from 0-32767. For a TDC Current Limit of 125A, enter 1000. 0 = 0 Amps. Uses BIOS VR mailbox command 0x1A.

Feature	Options	Description
TDC Time Window	**1 sec**, 2 sec, 3 sec, 4 sec, 5 sec, 6 sec, 7 sec, 8 sec, 10 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, 80 sec, 96 sec, 112 sec, 128 sec, 160 sec, 192 sec, 224 sec, 256 sec, 320 sec, 384 sec, 448 sec	VR TDC Time Window, value in seconds. 1s is the default, Ranging from 1s to 448s.
TDC Lock	**Disabled**, Enabled	TDC Lock
IRMS	Disabled, **Enabled**	Enable/Disable IRMS - Current root mean square.
GT VR Settings	Submenu	
GT Domain		
VR Config Enable	Disabled, **Enabled**	VR Config Enable
Current AC Loadline	320	
Current DC Loadline	320	
Current Psi1 Threshold	80	
Current Psi2 Threshold	20	
Current Psi3 Threshold	4	
Current Imon Slope	0	
Current Imon Offset	1	

Feature	Options	Description
Current VR Current Limit	220	
Current TDC Limit	240	
Current Voltage Limit	1519	
AC Loadline	[Max-Value, Min-Value, Step-Value] = [0x1868, 0x0000, 0x0001], **0x0000**	AC Loadline is defined in 1/100 mOhms. A value of 100 = 1.00 mOhm, and 1255 = 12.55 mOhm. The range is 0-6249 (0-62.49 mOhms). 0 = AUTO/HW default. Uses BIOS mailbox command 0x2.
DC Loadline	[Max-Value, Min-Value, Step-Value] = [0x1868, 0x0000, 0x0001], **0x0000**	DC Loadline is defined in 1/100 mOhms. A value of 100 = 1.00 mOhm, and 1255 = 12.55 mOhm. The range is from 0-6249 (0-62.49 mOhms). 0 = AUTO/HW default. Uses BIOS mailbox command 0x2.
PS Current Threshold1	[Max-Value, Min-Value, Step-Value] = [0x0200, 0x0000, 0x0001], **0x0080**	PS Current Threshold1, defined in 1/4 A increments. A value of 400 = 100A. The range is 0-512, which translates to 0-128A. 0 = AUTO. Uses BIOS VR mailbox command 0x3.
PS Current Threshold2	[Max-Value, Min-Value, Step-Value] = [0x0200, 0x0000, 0x0001], **0x0020**	PS Current Threshold2, defined in 1/4 A increments. A value of 400 = 100A. The range is from 0-512, which translates to 0-128A. 0 = AUTO. Uses BIOS VR mailbox command 0x3.
PS Current Threshold3	[Max-Value, Min-Value, Step-Value] = [0x0200, 0x0000, 0x0001], **0x0004**	PS Current Threshold3, defined in 1/4 A increments. A value of 400 = 100A. The range is from 0-512, which translates to 0-128A. 0 = AUTO. Uses BIOS VR mailbox command 0x3.
PS3 Enable	Disabled, **Enabled**	PS3 Enable/Disable. 0 - Disabled, 1 - Enabled. Uses BIOS VR mailbox command 0x3.
PS4 Enable	Disabled, **Enabled**	PS4 Enable/Disable. 0 - Disabled, 1 - Enabled. Uses BIOS VR mailbox command 0x3
IMON Slope	[Max-Value, Min-Value, Step-Value] =	IMON Slope defined in 1/100 increments. The range is from 0-200. For a 1.25 slope, enter 125. 0 = AUTO. Uses BIOS VR mailbox command 0x4.

Feature	Options	Description
	[0x00C8, **0x0000**, 0x0001]	
IMON Offset	[Max-Value, Min-Value, Step-Value] = [0xF9FF, **0x0000**, 0x0001]	IMON Offset defined in 1/1000 increments. The range is from 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	[Max-Value, Min-Value, Step-Value] = [0x03FF, **0x0000**, 0x0001]	Voltage Regulator Current Limit (Icc Max). 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	[Max-Value, Min-Value, Step-Value] = [0x1F3F, **0x0000**, 0x0001]	Voltage Limit (VMAX). This value represents the Maximum instantaneous voltage allowed at any given time. The range is from 0 - 7999mV. Uses BIOS VR mailbox command 0x8.
TDC Enable	Disabled, **Enabled**	TDC Enable. 0- Disable, 1 - Enable
TDC Current Limit	[Max-Value, Min-Value, Step-Value] = [0x7FFF, **0x0000**, 0x007D]	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, 10 sec, 12 sec, 14 sec, 16 sec, 20 sec, 24 sec, 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	VR TDC Time Window, value in seconds. 1s is the default, Ranging from 1s to 448s.

Feature	Options	Description
TDC Lock	**Disabled**, Enabled	TDC Lock
RFI Settings	Submenu	
RFI Domain		
RFI Current Frequency	139.200MHz	
RFI Frequency	[Max-Value, Min-Value, Step-Value] = [0x077E, 0x0000, **0x0000**]	Set desired RFI frequency, in increments of 100KHz. (For a frequency of 100.6MHz, enter 1006.)
FIVR Spread Spectrum	Disabled, **Enabled**	Enable or Disable the FIVR Spread Spectrum
RFI Spread Spectrum	0.5%, 1%, **1.5%**, 2%, 3%, 4%, 5%, 6%	Set the Spread Spectrum
Platform PL1 Enable	**Disabled**, Enabled	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 a given time window.
Platform PL1 Power	[Max-Value, Min-Value, Step-Value] = [0x003E7F83, **0x00000000**, 0x0000007D]	Platform Power Limit 1 Power in Milli Watts. BIOS will round to the nearest 1/8W when programming. Any value can be programmed between Max and Min Power Limits (specified by PACKAGE_POWER_SKU_MSR). For 12.50W, enter 12500. This setting will act as the new PL1 value for the Package RAPL algorithm.
Platform PL1 Time Window	**0**, 1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 14, 16, 20, 24, 28, 32, 40, 48, 56, 64, 80, 96, 112, 128	Platform Power Limit 1 Time Window value in seconds. The value may vary from 0 to 128. 0 = default values. Indicates the time window over which Platform TDP value should be maintained.
Platform PL2 Enable	**Disabled**, Enabled	Enable/Disable Platform Power Limit 2 programming. If this option is disabled, BIOS will program the default values for Platform Power Limit 2.
Platform PL2 Power	[Max-Value, Min-Value, Step-Value] = [0x003E7F83,	Platform Power Limit 2 Power in Milli Watts. BIOS will round to the nearest 1/8W when programming. Any value can be programmed between Max and Min Power Limits (specified by PACKAGE_POWER_SKU_MSR). For 12.50W, enter 12500. This setting will act as the new PL2 value for the Package RAPL algorithm.

Feature	Options	Description
	0x00000000, 0x0000007D]	
Power Limit 4 Override	**Disabled**, Enabled	Enable/Disable Power Limit 4 override. If this option is disabled, BIOS will leave the default values for Power Limit 4.
Power Limit 4	[Max-Value, Min-Value, Step-Value] = [0x003E7F83, **0x00000000**, 0x0000007D]	Power Limit 4 in Milli Watts. BIOS will round to the nearest 1/8W when programming. For 12.50W, enter 12500. If the value is 0, BIOS leaves the default value
Power Limit 4 Lock	**Disabled**, Enabled	Power Limit 4 MSR 601h Lock. When enabled PL4 configurations are locked during OS. When disabled PL4 configuration can be changed during OS.
C states	Disabled, **Enabled**	Enable/Disable CPU Power Management. Allows CPU to go to C states when it's not 100% utilized.
Enhanced C-State	Disabled, **Enabled**	Enable/Disable C1E. When enabled, the CPU will switch to minimum speed when all cores enter C-State.
C-State Auto Demotion	Disabled, **C1**	Configure C-State Auto Demotion
C-State Un-Demotion	Disabled, **C1**	Configure C-State Un-demotion
Package C-State Demotion	Disabled, **Enabled**	Package C-State Demotion
Package C-State Un-Demotion	Disabled, **Enabled**	Package C-State Un-demotion
CState Pre-Wake	Disabled, **Enabled**	Disable - Sets bit 30 of POWER_CTL MSR(0x1FC) to 1 to disable the Cstate Pre-Wake
IO MWAIT Redirection	**Disabled**, Enabled	When set, will map IO_read instructions sent to IO registers PMG_IO_BASE_ADDRBASE+offset to MWAIT(offset)
Package C State Limit	C0/C1, C2, C3, C6, C7, C7S, C8, C9, C10, Cpu Default, **Auto**, 0xFF, 0x00, 0x01	Maximum Package C State Limit Setting. Cpu Default: Leaves to Factory default value.Auto: Initializes to deepest available Package C State Limit.
C6/C7 Short Latency Control (MSR 0x60B)		

Feature	Options	Description
Time Unit	1 ns, 32 ns, **1024 ns**, 32768 ns, 1048576 ns, 33554432 ns	Unit of measurement for IRTL value - bits [12:10]
Latency	[Max-Value, Min-Value, Step-Value] = [0x03FF, **0x0000**, 0x0001]	Interrupt Response Time Limit value- bits [9:0], Enter 0-1023
C6/C7 Long Latency Control (MSR 0x60C)		
Time Unit*	1 ns, 32 ns, **1024 ns**, 32768 ns, 1048576 ns, 33554432 ns	Unit of measurement for IRTL value - bits [12:10]
Latency	[Max-Value, Min-Value, Step-Value] = [0x03FF, **0x0000**, 0x0001]	Interrupt Response Time Limit value- bits [9:0], Enter 0-1023
C8 Latency Control(MSR 0x633)		
Time Unit*	1 ns, 32 ns, **1024 ns**, 32768 ns, 1048576 ns, 33554432 ns	Unit of measurement for IRTL value - bits [12:10]
Latency	[Max-Value, Min-Value, Step-Value] = [0x03FF, **0x0000**, 0x0001]	Interrupt Response Time Limit value- bits [9:0], Enter 0-1023
C9 Latency Control(MSR 0x634)		
Time Unit*	1 ns, 32 ns, **1024 ns**, 32768 ns, 1048576 ns, 33554432 ns	Unit of measurement for IRTL value - bits [12:10]
Latency	[Max-Value, Min-Value, Step-Value] =	Interrupt Response Time Limit value- bits [9:0], Enter 0-1023

Feature	Options	Description
	[0x03FF, **0x0000**, 0x0001]	
C10 Latency Control(MSR 0x635)		
Time Unit*	1 ns, 32 ns, **1024 ns**, 32768 ns, 1048576 ns, 33554432 ns	Unit of measurement for IRTL value - bits [12:10]
Latency	[Max-Value, Min-Value, Step-Value] = [0x03FF, **0x0000**, 0x0001]	Interrupt Response Time Limit value- bits [9:0], Enter 0-1023
Thermal Monitor	Disabled, **Enabled**	Enable/Disable Thermal Monitor
Interrupt Redirection Mode Selection	**Fixed Priority**, Round robin, Hash Vector, No Change	Interrupt Redirection Mode Select for Logical Interrupts
Timed MWAIT	**Disabled**, Enabled	Enable/Disable Timed MWAIT Support
Custom P-state Table	Submenu	
Custom P-state Table		
Number of P States	**0**	Sets the number of custom P-states. At least 2 states must be present.
EC Turbo Control Mode	**Disabled**, Enabled	Enable/Disable EC Turbo Control mode
AC Brick Capacity	**90W AC Brick,** 65W AC Brick, 75W AC Brick	Specify the AC Brick capacity
EC Polling Period	[Max-Value, Min-Value, Step-Value] = [0x03FF, **0x0000**, 0x0001]	Count 1 to 255 for a range of 10ms to 2.55 seconds (1 count = 10ms)

Feature	Options	Description
EC Guard Band Value	[Max-Value, Min-Value, Step-Value] = [0x14, **0x01**, 0x0001]	Count 1 to 20 for a range of 1 watt to 20 watts.
EC Algorithm Selection	[Max-Value, Min-Value, Step-Value] = [0x0A, **0x01**, 0x0001]	Count 1 to 10 for Algorithm Selection.
Energy Performance Gain	**Disabled**, Enabled	Enables/disables Energy Performance Gain.
EPG DIMM Idd3N	[Max-Value, Min-Value, Step-Value] = [0x07D0, 0x0000, 0x0001] , **0x001A**	Active standby current (Idd3N) in milliamps from datasheet. Must be calculated on a per DIMM basis.
EPG DIMM Idd3P	[Max-Value, Min-Value, Step-Value] = [0x07D0, 0x0000, 0x0001], **0x000B**	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 Override	**Disabled**, Enabled	Enables/Disables 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.
Power Limit 3	[Max-Value, Min-Value, Step-Value] = [0x003E7F83, **0x00000000**, 0x0000007D]	Power Limit 3 in Milli Watts. BIOS will round to the nearest 1/8W when programming. For 12.50W, enter 12500. XE SKU: Any value can be programmed. Overclocking SKU: Value must be between Max and Min Power Limits (specified by PACKAGE_POWER_SKU_MSR). Other SKUs: This value must be between Min Power L.
Power Limit 3 Time Window	**0**, 3, 4, 5, 6, 7, 8, 10, 12, 14, 16, 20, 24, 28, 32, 40, 48, 56, 64	Power Limit 3 Time Window value in Milli seconds. The value may vary from 3 to 64(max). Indicates the time window over which Power Limit 3 value should be maintained. If the value is 0, BIOS leaves the hardware default value.
Power Limit 3 Duty Cycle	[Max-Value, Min-Value, Step-Value] = [0x64, 0x00, **0x00**]	Specifies the duty cycle in percentage that the CPU is required to maintain over the configured time window. The range is from 0-100.

Feature	Options	Description
Power Limit 3 Lock	**Disabled**, Enabled	Power Limit 3 MSR 615h Lock. When enabled, PL3 configurations are locked during OS. When disabled, PL3 configuration can be changed during OS boot.
CPU Lock Configuration	Submenu	Enables/Disables 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.
CFG Lock	Disabled, **Enabled**	Configures MSR 0xE2[15], CFG Lock bit
Overclocking Lock	Disabled, **Enabled**	Enables/Disables Overclocking Lock (Bit 20) in FLEX_RATION(194) MSR

7.3.2.2. GT Power Management Control

Feature	Options	Description
RC6(Render Standby)*	**Disabled**, Enabled	Check to enable render standby support.
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	Maximum GT frequency is limited by the user. Choose between 100MHz (RPN) and 1350MHz (RP0). Value beyond the range will be clipped to min/max supported by SKU
Disable Turbo GT Frequency	Enabled, **Disabled**	Enabled: Disables Turbo GT frequency. Disabled: GT frequency is not limited.

7.3.3 Graphic Configuration

Feature	Options	Description
Nxp configuration	Info Only	

Data format and Color Depth	VESA 24 bpp JEIDA 24 bpp **JEIDA/vesa 18 bpp**	Data format and Color Depth select
LVDS Output Mode	Dual LVDS bus **Single LVDS bus**	Single/Dual mode select
DE Polarity	**Active High** Active Low	DE Polarity select
Vsync Polarity	**Active High** Active Low	Vsync Polarity select
Spreading depth	**No Spreading** 0.5% 1.0% 1.5% 2.0% 2.5%	Clock frequency center spreading depth.
Integrated Display Configuration	Info only	
eDP/LVDS	**Disabled** Enabled	Enables/Disables eDP/LVDS
LFP Panel Type	**VBIOS Default** 640x480 800x600 1024x768 1280x1024 1400x1050 LVDS1 1400x1050 LVDS2 1600x1200 1366x768 1680x1050 1920x1200 1440x900	Select LFP panel used by Internal Graphics Device by selecting the appropriate setup item.

	1600x900 1024x768 1280x800 1920x1080 2048x1536	
LVDS Backlight Mode	**EC Mode** GTT Mode	Selects LVDS Backlight control function.
LVDS Backlight	Submenu	
LVDS Backlight Brightness	Value Range (0-255)	The change takes effect immediately. The value range starts from 0 and ends at 255.
DDI port 1	No Device Display Port HDMI **DisplayPort with HDMI/DVI Compatibility**	DDI port 1 function choose to Display Port or HDMI
DDI port 2	No Device Display Port HDMI **DisplayPort with HDMI/DVI Compatibiity**	DDI port 2 function choose to Display Port or HDMI
DDI port 3	No Device Display Port HDMI **DisplayPort with HDMI/DVI Compatibility**	DDI port 3 function choose to Display Port or HDMI

7.3.4 Power Management

Feature	Options	Description
Enable ACPI Auto Configuration	**Disabled**, Enabled	Enables or Disables BIOS ACPI Auto Configuration.

Enable Hibernation	Disabled, **Enabled**	Enables or Disables the system's ability to Hibernate (OS/S4 Sleep State). This option may not be effective with some operating systems.
ACPI Sleep State*	Suspend Disabled, **S3 (Suspend to RAM)**	Select the highest ACPI sleep state the system will enter when the SUSPEND button is pressed.
LID Function	**Disabled**, Enabled	Enables/Disables LID Function
Sleep Function	Disabled, **Enabled**	Enables/Disables Sleep Button Function
ECO Mode*	**Disabled**, Enabled	Reduces the power consumption of the system, but after a shut down, you have to wait at least 5 seconds before you can restart the system.
Power-Up Mode*	**Turn On,** Remain Off, Last State	Turn On:
ATTENTION: The Power-Up Mode only has effect, If the module is in ATX-Mode.		
Power Consumption	Submenu	

7.3.4.1. Power Management > Power Consumption

Feature	Options	Description
Power Consumption	Info only	
Main Current	Read only	Display input current.
Current Input Power	Read only	Display input power.
RTC	Read only	Display the sensed voltage based on hardware design.
5VSB	Read only	Display the sensed voltage based on hardware design.
VIN	Read only	Display the sensed voltage based on hardware design
3.3V	Read only	Display the sensed voltage based on hardware design
VMEM	Read only	Display the sensed voltage based on hardware design
3.3VSB	Read only	Display the sensed voltage based on hardware design

Feature	Options	Description
VCORE	Read only	Display the sensed voltage based on hardware design

7.3.5 System Management

Feature	Options	Description
System Management	Info Only	
Version	Info Only	Display SEMA Module Version.
SEMA Firmware	Info Only	Display SEMA Firmware Version.
SEMA Flags	Submenu	Display SEMA Flags
SEMA Features	Info	Display SEMA Supported Features

7.3.5.1. System Management > SEMA Flags

Feature	Options	Description
SEMA Flags	Info Only	
BIOS Select	Info Only	
ATX/AT-Mode	Info Only	

7.3.6 Thermal Management

Feature	Options	Description
Thermal Management	Info Only	

Feature	Options	Description
Critical Trip Point	**Disabled** 80 C 90 C 95 C	The value is the temperature threshold of the Critical Trip Point.
Passive Cooling Trip Point	**Disabled** 70 C 80 C 90 C 100 C	The value is the temperature threshold of the Passive Cooling Trip Point.
Active Cooling Trip Point	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
Temperature and Fan Speed	Submenu	

7.3.6.1. Thermal Management-> Temperature and Fan Speed

Feature	Options	Description
Temperatures and Fan Speed	Info Only	
CPU Temperature	Info Only	
Current	Info Only	Display Current CPU Temperature
Startup	Info Only	Display Startup Board Temperature
Min	Info Only	Display Min Board Temperature
Max	Info Only	Display Max Board Temperature

Feature	Options	Description
CPU Fan Speed	Info Only	Display CPU Fan Speed
Smart Fan	Submenu	

7.3.6.2. Submenu: 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 (Smart Fan)** Fan Off Fan On	Select CPU Fan control mode.
Trigger Point 1	Info-only	
Trigger Temperature	45	Set the temperature value for trigger point 1 to control CPU fan.
PWM Level	25	When configured sensor reaches the trigger temperature value, set PWM level for this condition.
Trigger Point 2	Info-only	
Trigger Temperature	60	Set the temperature value for trigger point 2 to control CPU fan.
PWM Level	50	When configured sensor reaches the trigger temperature value, set PWM level for this condition.
Trigger Point 3	Info-only	
Trigger Temperature	75	Set the temperature value for trigger point 3 to control CPU fan.
PWM Level	75	When configured sensor reaches the trigger temperature value, set PWM level for this condition.
Trigger Point 4	Info-only	
Trigger Temperature	90	Set the temperature value for trigger point 4 to control CPU fan.
PWM Level	100	When configured sensor reaches the trigger temperature value, set PWM level for this condition.

Feature	Options	Description
Trigger Point 1	Info-only	

7.3.7 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. Pressing F12 during start up disables the Power Up Watchdog
Timeout	**65535**	Here you can enter the time the Power Up Watchdog should wait until it resets the system. The value range starts by 24 and ends at 65535
RunTime Watchdog	**Disabled** Enabled	The RunTime Watchdog resets the system after a certain period following a power-up.
Timeout	**24**	Here you can specify the duration of the Runtime Watchdog and wait until it resets the system. The value range starts by 30 and ends by 65535.

7.3.8 Super IO Configuration

Feature	Options	Description
Super IO Configuration	Info only	
IT5121E Super IO Configuration	Submenu	System Super IO Chip Parameters.
W83627DHGSEC Super IO Configuration	Submenu	System Super IO Chip Parameters.

7.3.8.1. Super IO Configuration > IT5121E Super IO Configuration

Feature	Options	Description

IT5121E Super IO Configuration		
Serial Port 1 Configuration	Submenu	
Serial Port 2 Configuration	Submenu	

Submenu: Super IO Configuration → Serial Port x Configuration

Feature	Options	Description
Serial Port 1 Configuration		
Serial Port 1 Configuration	Disabled, **Enabled**	Set Parameters of Serial Port 1
Device Settings	4;	
Change Settings	**Auto**, IO=3F8h; IRQ=4;, IO=3F8h; IRQ=3,4,5,6,7,9,10,11,12;, IO=2F8h; IRQ=3,4,5,6,7,9,10,11,12;, IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12;, IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12;	Select an optimal setting for Super IO Device
Change Settings	**Normal**, High Speed	Select an optimal setting for Super IO Device
Serial Port 2 Configuration		
Serial Port 2 Configuration	Disabled, **Enabled**	Set Parameters of Serial Port 2
Device Settings	3;	
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;, Normal, High Speed	Select an optimal setting for Super IO Device
Change Settings	**Normal**, High Speed	Select an optimal setting for Super IO Device

7.3.8.2. Super IO Configuration > W83627DHGSEC Super IO Configuration

Feature	Options	Description
W83627DHGSEC Super IO Configuration		
Serial Port 1 Configuration	Submenu	
Serial Port 2 Configuration	Submenu	

Submenu: Super IO Configuration → Serial Port x Configuration

Feature	Options	Description
Serial Port 1 Configuration		
Serial Port 1 Configuration	Disabled, **Enabled**	Set Parameters of Serial Port 1
Device Settings	5	
Change Settings	Auto, IO=240h; IRQ=10;, IO=240h; IRQ=3,4,5,6,7,10,11,12;, IO=248h; IRQ=3,4,5,6,7,10,11,12;, IO=250h; IRQ=3,4,5,6,7,10,11,12;, IO=258h; IRQ=3,4,5,6,7,10,11,12;, IO=260h; IRQ=3,4,5,6,7,10,11,12;, IO=268h; IRQ=3,4,5,6,7,10,11,12;	Select an optimal setting for Super IO Device
Serial Port 2 Configuration		
Serial Port 2 Configuration	Disabled, **Enabled**	Set Parameters of Serial Port 2
Device Settings	7;	
Change Settings	Auto, IO=248h; IRQ=10;, IO=240h; IRQ=3,4,5,6,7,10,11,12;, IO=248h; IRQ=3,4,5,6,7,10,11,12;, IO=250h; IRQ=3,4,5,6,7,10,11,12;, IO=258h; IRQ=3,4,5,6,7,10,11,12;, IO=260h; IRQ=3,4,5,6,7,10,11,12;, IO=268h; IRQ=3,4,5,6,7,10,11,12;	Select an optimal setting for Super IO Device
Device Mode	Standard Serial Port Mode, IrDA Active	Change the Serial Port mode.

	pulse 1.6 uS, IrDA Active pulse 3/16 bit time, ASKIR Mode	

7.3.9 Miscellaneous

Feature	Options	Description
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
WOL From S5	OFF **ON**	This Config to control power on/off LAN in S5 State by SEMA(EC).
Smart Battery Function	**Disabled** Enabled Auto	Enable/Disable Smart Battery function. Auto: disable Smart Battery function if charger IC not be detected.
SMBUS Select Configuration	From EC**, From PCH**	SMBUS Select Configuration from PCH or EC.

7.3.10 USB Configuration

Feature	Options	Description
USB Configuration	Info Only	
USB Module Version	Info Only	Display USB Module Version.

Feature	Options	Description
USB Controllers:	Info Only	Display USB Controllers is XHCI or EHCI.
USB Devices:	Info Only	Display attachment USB devices.
Legacy USB Support	**Enabled** Disabled Auto	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	**Enabled** Disabled	This is a workaround for OSs without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.
USB Mass Storage Driver Support	Disabled **Enabled**	Enable / Disable USB Mass Storge Driver Support.
USB hardware delays and time-outs:	Info Only	
USB transfer rime-out	1 sec 5sec 10sec **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 Hot Controller. 'Auto' uses default value: for a Root po\rt it is 100 ms, for a hub port the delay is taken form a hub descriptor.

7.3.11 NVMe Configuration

Feature	Options	Description
NVMe device name	Submenu	

Feature	Options	Description
Seg:Bus:Dev:Func	Info Only	Display NVMe Seg:Bus:Dev:Func.
Model Number	Info Only	Display NVMe Model Number.
Total Size	Info Only	Display NVMe Total Size.
Vendor ID	Info Only	Display Vendor ID.
Device ID	Info Only	Display NVMe Total Size.
Namespace :	Info Only	Display NVMe Total Size.
Device Self-Test :		
Self-Test Option	**Short**, Extended	Select either Short or Extended Self-Test. Short option will take couple of minutes and extended option will take several minutes to complete."
Self-Test Action	**Controller Only Test,** Controller and NameSpace Test	Select either to test Contoller alone or Controller and NameSpace. Selecting Controller and Namespace option will take lot longer to complete the test.
Run Device Self-Test		Perform device self-test for the corresponding Option and Action selected by user. Pressing the 'Esc' key will abort the test. Result shown below is the recent result logged in the device.
Short Device Self-Test Result	Info Only	Display Short Device Self-Test Result.
Extended Device Self-Test Result	Info Only	Display Extended Device Self-Test Result.

7.3.12 AMI Graphics Output Protocol Policy

Feature	Options	Description
Intel(R) Graphics Controller		
Intel(R) GOP Driver [21.0.10xx]		

Output Select	HDMI	Auto detect Output Interface
Output Select*	HDMI/DP/eDP	Manual select Output Interface
Brightness Setting	[Max-Value, Min-Value, Step-Value, Step-Value] = [0xFFFFFFFF, 0x00000000, 0x00000001, Brightness Setting]	Item shown when eDP detected Set Gop Brightness value
BIST Enable	**Disabled**, Enabled	Item shown when eDP detected Starts or stops the BIST on the integrated display panel.
Output Select	HDMI	Auto detect Output Interface

7.3.13 Serial Console Redirection

Feature	Options	Description
Console Redirection	**Disabled,** Enabled	To enable or disable console redirection of COMx.
Console Redirection Settings	Submenu	The settings specify how the host computer and the remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings.

7.3.13.1.Serial Console Redirection → Console Redirection Settings

Feature	Options	Description
Terminal Type	VT100 VT100+ VT-UTF8 **ANSI**	Configures the type of console emulation. 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**	Configures the number of data bits in each transmitted or received serial character for both serial ports.
Parity	**None** Even Odd	Configures if parity bit is generated (transmit data) or checked. A parity bit can be sent with the data bits to detect some transmission errors. Even: The parity bit is 0 if the num of 1's in the data bits is even. Odd: The parity bit is 0 if num of 1's in the data bits is odd. Mark: The parity bit is always 1. Space: The parity bit is always 0. Mark and Space parity bits do not allow for error detection. They can be used as an additional data bit.
Stop Bits	**1** 2	Configures the number of stop bits transmitted and received in each serial character for both serial ports. 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 Software	Configures flow control for console redirection. Hardware flow control uses RTC/CTS. Software flow control uses XON/XOFF.
VT-UTF8 Combo Key Support	Disabled **Enabled**	Enables VT-UTF8 combination key support for ANSI/VT100 terminals.
Recorder Mode	**Disabled** Enabled	With this mode enabled only text will be sent. This is to capture terminal data.
Resolution 100x31	**Disabled** Enabled	Enables or disables extended terminal resolution.
Legacy OS Redirection Resolution	**80x24** 80x25	Set console display resolution.
Putty KeyPad	**VT100** LINUX XTERMR6 SCO ESCN VT400	Selects Function Keys and Key Pad on Putty.
Redirection After BIOS POST	**Always Enabled** BootLoader	The setting specifies if BootLoader is selected, then legacy console redirection is disabled before booting to legacy OS.

7.3.14 Network Stack Configuration

Feature	Options	Description
Network Stack	**Disabled**, Enabled	Enables/Disables UEFI Network Stack
IPv4 PXE Support	**Disabled**, Enabled	Enables/Disables IPv4 PXE boot support. If disabled, IPv4 PXE boot support will not be available.
IPv4 HTTP Support	**Disabled**, Enabled	Enables/Disables IPv4 HTTP boot support. If disabled, IPv4 HTTP boot support will not be available.
IPv6 PXE Support	**Disabled**, Enabled	Enables/Disables IPv6 PXE boot support. If disabled, IPv6 PXE boot support will not be available.
IPv6 HTTP Support	**Disabled**, Enabled	Enables/Disables IPv6 HTTP boot support. If disabled, IPv6 HTTP boot support will not be available.
PXE boot wait time	[Max-Value, Min-Value, Step-Value] =[0x05, **0x00**, 0x01]	Wait time in seconds to press the ESC key to abort the PXE boot. Use either +/- or numeric keys to set the value.
Media detect count	[Max-Value, Min-Value, Step-Value] =[0x32, **0x01**, 0x01]	Number of times the presence of media will be checked. Use either +/- or numeric keys to set the value.

7.3.15 Trusted Computing

Feature	Options	Description
Security Device Support	**Disable**, Enable	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.
NO Security Device Found		

7.4. Chipset

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

7.4.1 Chipset > System Agent (SA) Configuration

Feature	Options	Description
Memory Configuration	Submenu	
Graphics Configuration	Submenu	
VMD setup menu	Submenu	
PCI Express Configuration	Submenu	
Stop Grant Configuration	**Auto**, Manual	Automatic/Manual stio grant configuration.
VT-d	Disabled, **Enabled**	VT-d capability
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	Enabled, **Disabled**	Support the word/dword decoding of port 80h behind LPC
DMA Control Guarantee	Disabled, **Enabled**	Enable/Disable DMA_CONTROL_GUARANTEE bit
Above 4GB MMIO BIOS assignment	**Enabled**, Disabled	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 RC Version	**Info-only**	
Memory Frequency	**Info-only**	
Memory Timings (tCL-tRCD-tRP-tRAS)	**Info-only**	

Controller x Channel x Slot x	**Info-only**	
Size	**Info-only**	
Number of Ranks	**Info-only**	
Manufacturer	**Info-only**	
Memory Test on Warm Boot	**Enabled,** Disabled	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 3600 3733 4000 4200 4267 4400 4600 4800 5000	Maximum Memory Frequency Selections in Mhz. Valid values should match the refclk, i.e., divided by 133 or 100

	5200 5400 5600 5800 6000 6200 6400 10000	
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 DIMM Control	**Enabled,** Disabled	Controller 0, Channel 0 DIMM Control Support - Enable or Disable Dimms on Controller 0, Channel 0.
Controller 1, Channel 0 DIMM Control	**Enabled,** Disabled	Controller 1, Channel 0 DIMM Control Support - Enable or Disable Dimms on Controller 1, Channel 0.
In-Band ECC Support (Industrial SKU only)	Enabled**, Disabled**	Enable/Disable In-Band ECC. Either the IBECC or the TME can be enabled.
In-Band ECC Operation Mode	0, 1, **2**	0: Functional Mode protects requests based on the address range, 1: Makes all requests non protected and ignore range checks, 2:Makes all requests protected and ignore range checks
In-Band ECC Error Injection Control	**No Error Injection,** Inject Correctable Error Address match, Inject Correctable Error on insertion counter, Inject Uncorrectable Error Address match,	Enables IBECC Error Injection

	Inject Uncorrectable Error on insertion counter	

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

Feature	Options	Description
Skip Scaning of External Gfx Card	**Disabled**, Enabled	If Enabled, 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	**Auto**, 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
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.
Intel Graphics Pei Display Peim	Enabled, **Disabled**	Enable/Disable Pei (Early) Display

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 > PCIE Configuration

Feature	Options	Description
Connection Type	Built-in, **Slot**	Built-In: a built-in device is connected to this rootport. Slot Implemented 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.
PCI Express Power Gating	Disabled, **Enabled**	PCI Express Power Gating Enable/Disable for each root port.
ASPM	**Disabled**, L0s, L1, L0sL1	Set the ASPM Level: Force L0s - Force all links to L0s State AUTO - BIOS auto configure DISABLE - Disables ASPM
L1 Substates	**Disabled**, L1.1, L1.1 & L1.2	PCI Express L1 Substates settings. L1SS cannot be enabled when CLKREQMSG is disabled
Gen3 Eq Phase3 Method	**Hardware**, Static Coeff.	PCIe Gen3 Equalization Phase 3 Method
Gen4 Eq Phase3 Method	**Hardware**, Static Coeff.	PCIe Gen3 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	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.
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
Enable ClockReg Messaging	**Disabled**, Enabled	Enable or Disable ClockReg Messaging
Transmitter Half Swing	**Disabled**, Enabled	Transmitter Half Swing Enable/Disable.
Detect Timeout	[Max-Value, Min-Value, Step-Value] = [0xFFFF, **0x0000**, 0x0001]	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
CPU PCIE Func0 Link Disable	**Disabled**, Enabled	CPU PCIE Func0 Link Disable while Device attached into Port having Func0 and FuncN
SA PCIe LTR Configuration		
LTR	Disabled, **Enabled**	SA PCIE Latency Reporting Enable/Disable
Snoop Latency Override	Disabled, Manual, **Auto**	Snoop Latency Override for SA PCIE.
Non Snoop Latency Override	Disabled, Manual, **Auto**	Non-Snoop Latency Override for SA PCIE.
Force LTR Override	**Disabled**, Enabled	Force LTR Override for SA PCIE.
LTR Lock	**Disabled**, Enabled	PCIE LTR Configuration Lock
CPU PCIe Gen3 HWEQ Config		
UPTP	[Max-Value, Min-Value, Step-Value] = [0x0A, 0x00, 0x01]	Upstream Port Transmitter Preset
DPTP	[Max-Value, Min-Value, Step-Value] = [0x0A, 0x00, 0x01]	Downstream Port Transmitter Preset
CPU PCIe Gen4 HWEQ Config		
UPTP	[Max-Value, Min-Value, Step-Value] = [0x0A, 0x00, 0x01]	Upstream Port Transmitter Preset
DPTP	[Max-Value, Min-Value, Step-Value] = [0x0A, 0x00,	Downstream Port Transmitter Preset

	0x01]	

7.4.2 Chipset > PCH-IO Configuration

Feature	Options	Description
PCI Express Configuration	Submenu	
SATA Configuration	Submenu	
USB Configuration	Submenu	
Security Configuration	Submenu	
HD Audio Configuration	Submenu	
Seriallo Serial IO Configuration	Submenu	
PCH LAN Controller	Info-Only	No GbE Region
Port 80h Redirection	LPC Bus, **PCIE Bus**	Control where the Port 80h cycles are sent.
Enhance Port 80h LPC Decoding	**Enabled**, Disabled	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%, 1.2%, 1.3%, 1.4%, 1.5%, 1.6%, 1.7%, 1.8%, 1.9%, 2.0%, Disable	Pcie Pll SSC percentage.AUTO - Keep hw default, no BIOS override. The range is from 0.0%-2.0%.
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 > PCI Express Configuration

Feature	Options	Description
DMI Link ASPM Control	**Disabled**, L0s, L1, L0sL1, Auto	The control of Active State Power Management of the DMI Link.
Port8xh Decode	**Disabled**, Enabled	PCI Express Port8xh Decode Enable/Disable.
PCIE Ports 5-8 Configuration	**4x1 Port,** 1x2 2x1 Port, 2x2	Notes:

	Port, 1x4 Port	Please make sure the system boots completed after changing the configuration. Do Not Attempt to Shut Down Your Computer, doing so may lead to system malfunction.
PCI Express Root Port 5 (COMe Lane 0)	Submenu	
PCI Express Root Port 6 (COMe Lane 1)	Submenu	
PCI Express Root Port 7 (COMe Lane 2)	Submenu	
PCI Express Root Port 8 (COMe Lane 3)	Submenu	
PCI Express Root Port 9 (LAN I225)	Submenu	
PCI Express Root Port 10 (COMe Lane 4~7 (option))	Submenu	.

7.4.2.2. Chipset > PCH-IO Configuration > PCI Express Configuration > PCI Express Root Port#

Feature	Options	Description
PCI Express Root Port	Disabled **Enable**	Control the PCI Express Root Port.
Connection Type	Built-in **Slot**	Built-In: a built-in device is connected to this rootport. Slot Implemented bit will be clear. Slot: this rootport connects to user-accessible slot. Slot Implemented bit will be set.
ASPM	**Disabled** L1 Auto	Set the ASPM Level. Force L0s - Force all links to L0s State Auto - BIOS auto configure; Disabled - Disables ASPM
L1 Substates	Disabled L1.1 **L1.1 & L1.2**	PCI Express L1 Substates settings.
L1 Low	**Disabled** Enable	PCI Express L1 Low substate Enable/Disable.
ACS	Disabled **Enable**	Enable/Disable Access Control Services Extended Capability

Feature	Options	Description
PTM	Disabled **Enable**	Enable/Disable Precision Time Measurement
DPC	**Disabled** Enable	Enable/Disable Downstream Port Containment
EDPC	Disabled **Enable**	Enable/Disable Rootport extensions for Downstream Port Containment
URR	**Disabled** Enable	PCI Express Unsupported Request Reporting Enable/Disable.
FER	**Disabled** Enable	PCI Express Device Fatal Error Reporting Enable/Disable.
NFER	**Disabled** Enable	PCI Express Device Non-Fatal Error Reporting Enable/Disable.
CER	**Disabled** Enable	PCI Express Device Correctable Error Reporting Enable/Disable.
SEFE	**Disabled** Enable	Root PCI Express System Error on Fatal Error Enable/Disable.
SENFE	**Disabled** Enable	Root PCI Express System Error on Non-Fatal Error Enable/Disable.
SECE	**Disabled** Enable	Root PCI Express System Error on Correctable Error Enable/Disable.
PME SCI	Disabled **Enable**	PCI Express PME SCI Enable/Disable.
Hot Plug	**Disabled** Enable	PCI Express Hot Plug Enable/Disable.
Advanced Error Reporting	Disabled **Enable**	Advanced Error Reporting Enable/Disable.

Feature	Options	Description
PCIe Speed	**Auto** Gen1 Gen2 Gen3	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 **Enable**	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.
Force LTR Override	**Disabled** Enable	Force LTR Override for PCH PCIE.
LTR Lock	**Disabled** Enable	PCIE LTR Configuration Lock
Peer Memory Write Enable	**Disabled**	Peer Memory Write Enable/Disable

Feature	Options	Description
	Enable	

7.4.2.3. 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 X	Info-Only	
Software Preserve	Info-Only	
Port X	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, Staggered 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,**	Identify the SATA Topology if it is Default, ISATA, Flex, Direct Connect, or M2

	ISATA, Direct Connect, Flex, M2	
SATA Port X DevSlp	**Disabled**, Enabled	Enable/Disable SATA Port X 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

7.4.2.4. Chipset > PCH-IO Configuration >USB Configuration

Feature	Options	Description
xDCI Support	**Disabled**, Enabled	Enable/Disable xDCI (USB OTG Device).
USB2 PHY Sus Well Power Gating	Disabled, **Enabled**	Select 'Enabled' to enable SUS Well PG for USB2 PHY. This option has no effect on PCH-H
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 Speed Selection	**Gen2**, Gen1	USB3.1 Speed selection; Gen1 or Gen2
USB Port Disable Override	**Disabled**, Select Per-Pin	Selectively Enable/Disable the corresponding USB port from reporting a Device Connection to the controller.

7.4.2.5. 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

7.4.2.6. Chipset > PCH-IO Configuration > HD Audio Configuration

Feature	Options	Description
HD Audio	Disabled **Enabled**	Control Detection of the HD-Audio device.

7.4.2.7. Chipset > PCH-I/O Configuration > Serial IO Configuration

Feature	Options	Description
I2C0 Controller	Disabled**, Enabled**	**Enables/Disables Serial I/O Controller**
I2C1 Controller	Disabled**, Enabled**	**Enables/Disables Serial I/O Controller**
UART0 Controller	**Disabled,** Enabled, Communication port (COM)	**Enables/Disables Serial I/O Controller**
UART1 Controller	**Disabled,** Enabled, Communication port (COM)	**Enables/Disables Serial I/O Controller**
GPIO IRQ Route	**IRQ14,** IRQ15	**Route all GPIOs to one of the IRQ.**

7.5. Security

Feature	Options	Description
Password Description	Info only	
Administrator Password	Enter password	
User Password	Enter password	

Feature	Options	Description
Password Description	Info only	
Secure Boot menu	submenu	

7.5.1 Secure Boot menu

Feature	Options	Description
Secure Boot	Info only	
Secure Boot Control	**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.

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 option.

Feature	Options	Description
Boot Configuration	Info only	
UEFI Application Boot Priorities	Info only	

7.7. Save & Exit

Feature	Options	Description
Save Options	Info only	
Save Changes and Exit		Exit system setup after saving the changes.
Discard Changes and Exit		Exit system setup without saving any changes.

Feature	Options	Description
Save Change and Reset		Reset the system after saving the changes.
Discard Changes and Reset		Reset system setup without saving any changes.
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.
Default Options	Info only	
Restore Defaults		Restore/Load Default values for all the setup options.
Save as User Defaults		Save the changes done so far as User Defaults.
Restore User Defaults		Restore the User Defaults to all the setup options.
Boot Override	Info only	

8. BIOS Checkpoints, Beep Codes

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

Checkpoints and Beep Codes Definition

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

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

Aptio Boot Flow

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

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

Viewing BIOS Checkpoints

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

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

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

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

8.1. Status Code Ranges

Status Code Range	Description
0x01 – 0x0B	SEC execution
0x0C – 0x0F	SEC errors
0x10 – 0x2F	PEI execution up to and including memory detection
0x30 – 0x4F	PEI execution after memory detection
0x50 – 0x5F	PEI errors
0x60 – 0x8F	DXE execution up to BDS
0x90 – 0xCF	BDS 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).
0x02	AP initialization before microcode loading
0x03	North Bridge initialization before microcode loading
0x04	South Bridge initialization before microcode loading
0x05	OEM initialization before microcode loading
0x06	Microcode loading
0x07	AP initialization after microcode loading
0x08	North Bridge initialization after microcode loading
0x09	South Bridge initialization after microcode loading
0x0A	OEM initialization after microcode loading
0x0B	Cache initialization

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

8.2.2 SEC Beep Codes

None

8.2.3 PEI Phase

Status Code	Description
Progress Codes	
0x10	PEI Core is started
0x11	Pre-memory CPU initialization is started
0x12	Pre-memory CPU initialization (CPU module specific)
0x13	Pre-memory CPU initialization (CPU module specific)
0x14	Pre-memory CPU initialization (CPU module specific)
0x15	Pre-memory North Bridge initialization is started
0x16	Pre-Memory North Bridge initialization (North Bridge module specific)
0x17	Pre-Memory North Bridge initialization (North Bridge module specific)
0x18	Pre-Memory North Bridge initialization (North Bridge module specific)
0x19	Pre-memory South Bridge initialization is started
0x1A	Pre-memory South Bridge initialization (South Bridge module specific)
0x1B	Pre-memory South Bridge initialization (South Bridge module specific)
0x1C	Pre-memory South Bridge initialization (South Bridge module specific)
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

Status Code	Description
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	Post-Memory North Bridge initialization (North Bridge module specific)
0x39	Post-Memory North Bridge initialization (North Bridge module specific)
0x3A	Post-Memory North Bridge initialization (North Bridge module specific)
0x3B	Post-Memory South Bridge initialization is started
0x3C	Post-Memory South Bridge initialization (South Bridge module specific)
0x3D	Post-Memory South Bridge initialization (South Bridge module specific)
0x3E	Post-Memory South Bridge initialization (South Bridge module specific)
0x3F-0x4E	OEM post memory initialization codes
0x4F	DXE IPL is started
PEI Error Codes	
0x50	Memory initialization error. Invalid memory type or incompatible memory speed

Status Code	Description
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

8.2.4 PEI Beep Codes

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

8.2.5 DXE Status Codes

Status Code	Description
0x60	DXE Core is started
0x61	NVRAM initialization
0x62	Installation of the South Bridge Runtime Services
0x63	CPU DXE initialization is started
0x64	CPU DXE initialization (CPU module specific)
0x65	CPU DXE initialization (CPU module specific)
0x66	CPU DXE initialization (CPU module specific)
0x67	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	North Bridge DXE initialization (North Bridge module specific)
0x6C	North Bridge DXE initialization (North Bridge module specific)
0x6D	North Bridge DXE initialization (North Bridge module specific)
0x6E	North Bridge DXE initialization (North Bridge module specific)
0x6F	North Bridge DXE initialization (North Bridge module specific)
0x70	South Bridge DXE initialization is started
0x71	South Bridge DXE SMM initialization is started
0x72	South Bridge devices initialization
0x73	South Bridge DXE Initialization (South Bridge module specific)
0x74	South Bridge DXE Initialization (South Bridge module specific)

Status Code	Description
0x75	South Bridge DXE Initialization (South Bridge module specific)
0x76	South Bridge DXE Initialization (South Bridge module specific)
0x77	South Bridge DXE Initialization (South Bridge module specific)
0x78	ACPI module initialization
0x79	CSM initialization
0x7A – 0x7F	Reserved for future AMI DXE codes
0x80 – 0x8F	OEM DXE initialization codes
0x90	Boot Device Selection (BDS) phase is started
0x91	Driver connecting is started
0x92	PCI Bus initialization is started
0x93	PCI Bus Hot Plug Controller Initialization
0x94	PCI Bus Enumeration
0x95	PCI Bus Request Resources
0x96	PCI Bus Assign Resources
0x97	Console Output devices connect
0x98	Console input devices connect
0x99	Super IO Initialization
0x9A	USB initialization is started
0x9B	USB Reset
0x9C	USB Detect
0x9D	USB Enable
0x9E – 0x9F	Reserved for future AMI codes

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

Status Code	Description
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

8.2.6 DXE Beep Codes

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

8.2.7 ACPI/ASL Checkpoint

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

Status Code	Description
	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

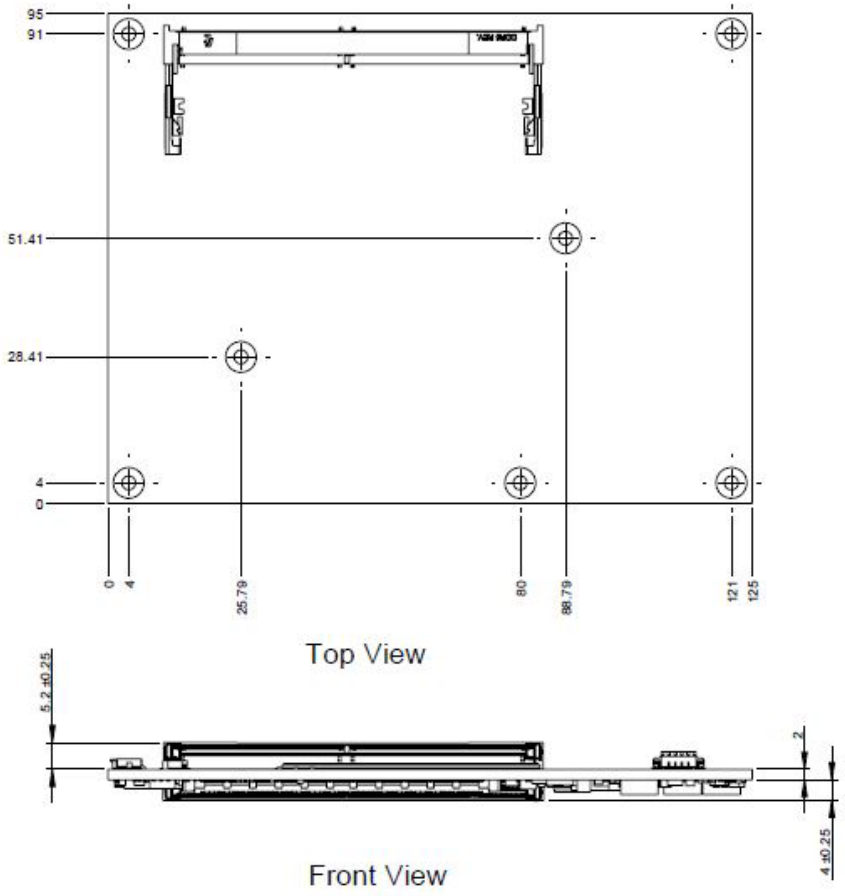
9.1. Windows 10 IoT Enterprise 64-bit

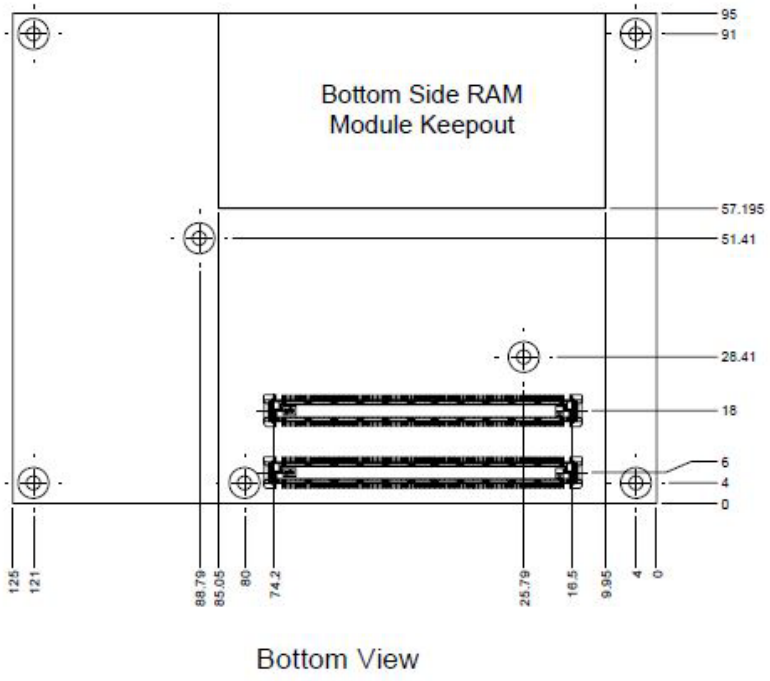
9.2. Yocto Linux 64-bit

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

10. Mechanical and Thermal

10.1. Module Dimensions





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

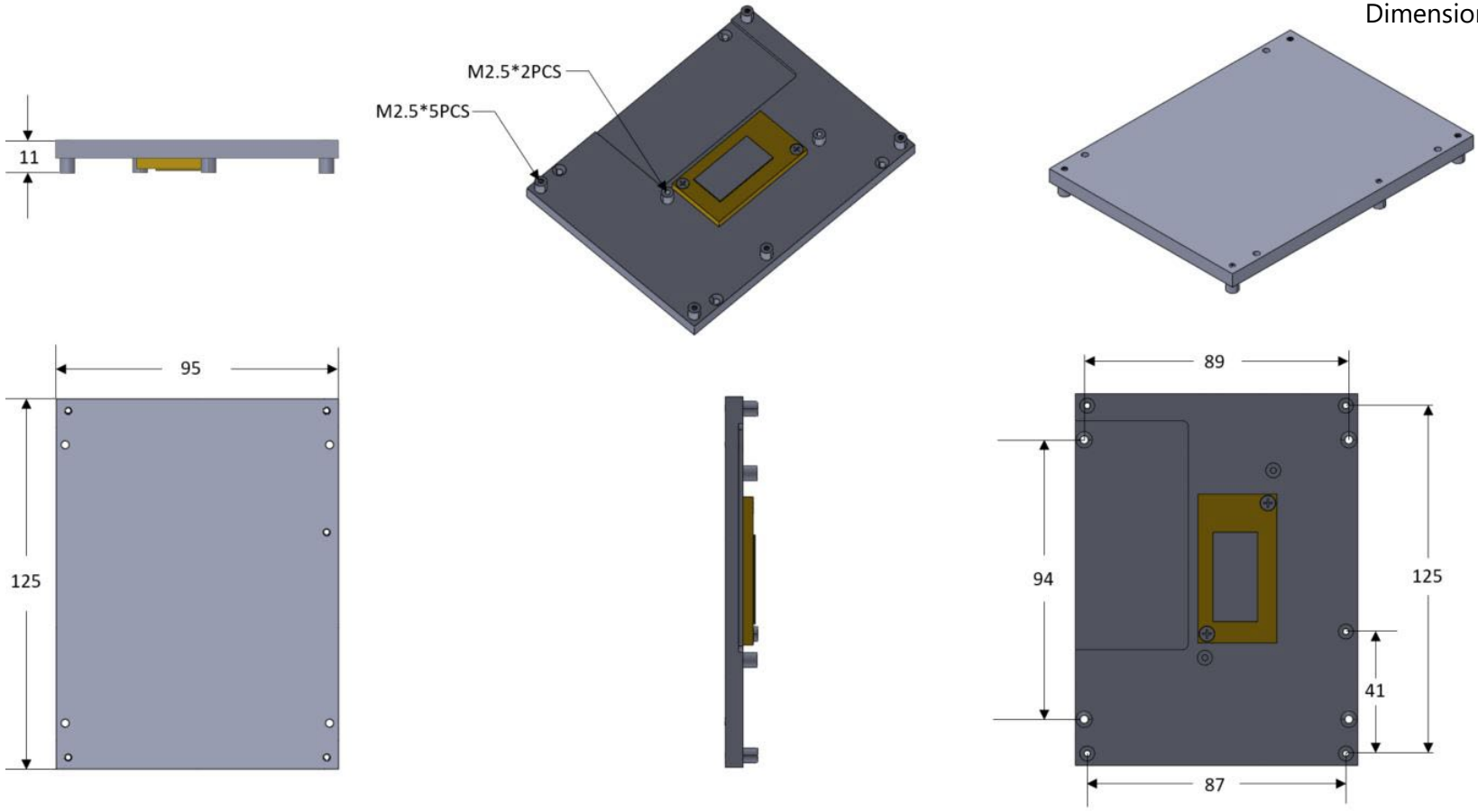
Dimensions: mm

Figure 5 – Module mechanical dimensions

10.2. Thermal Solutions

10.2.1 Heatspreader: HTS

Dimensions: mm



Heatspreader: HTS

Figure 6 – Heatspreader: HTS

10.2.2 Heatsink: THS

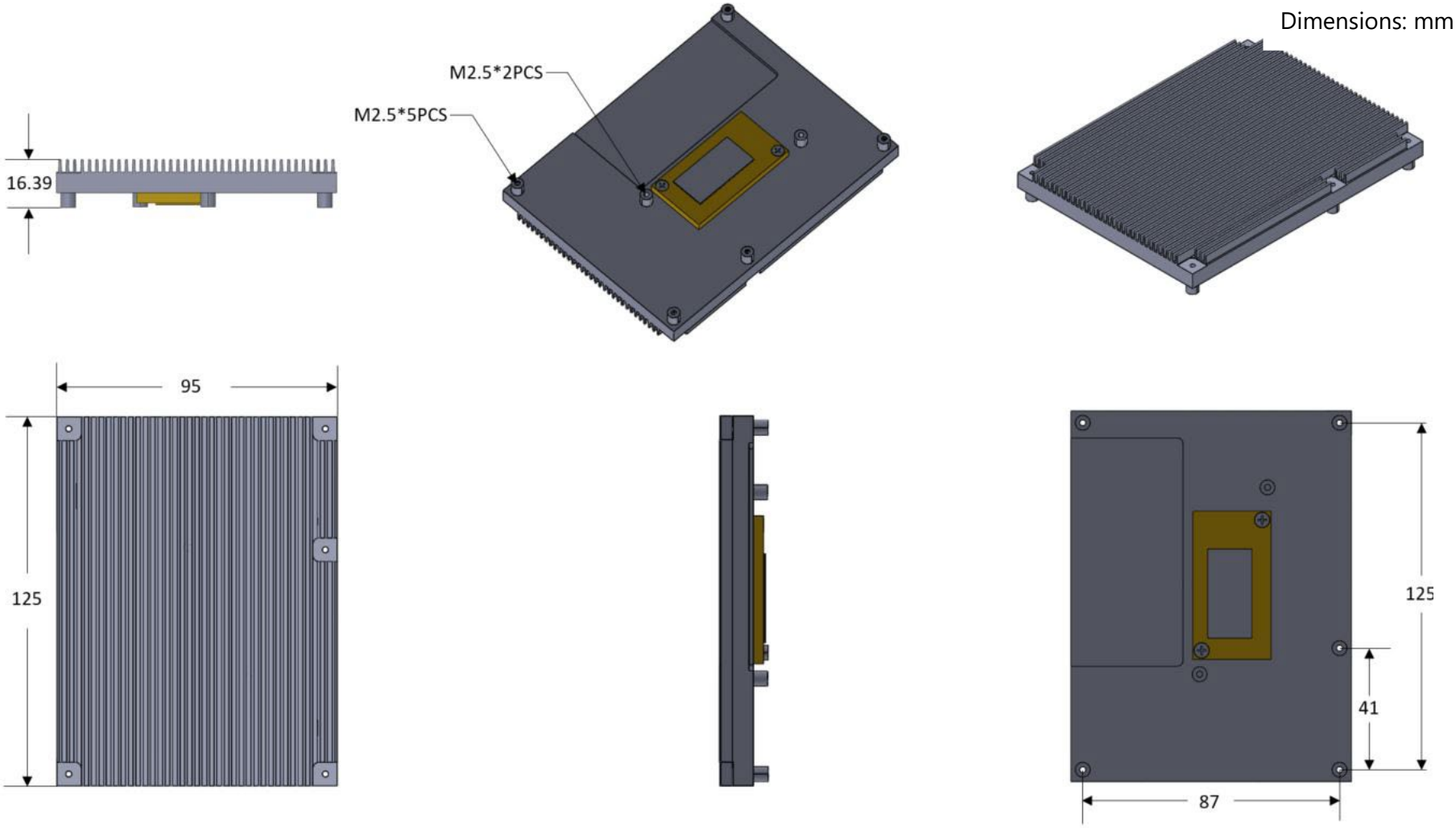


Figure 7 – Heatsink: THS

10.2.3 Heatsink High Profile: THSH

Dimensions: mm

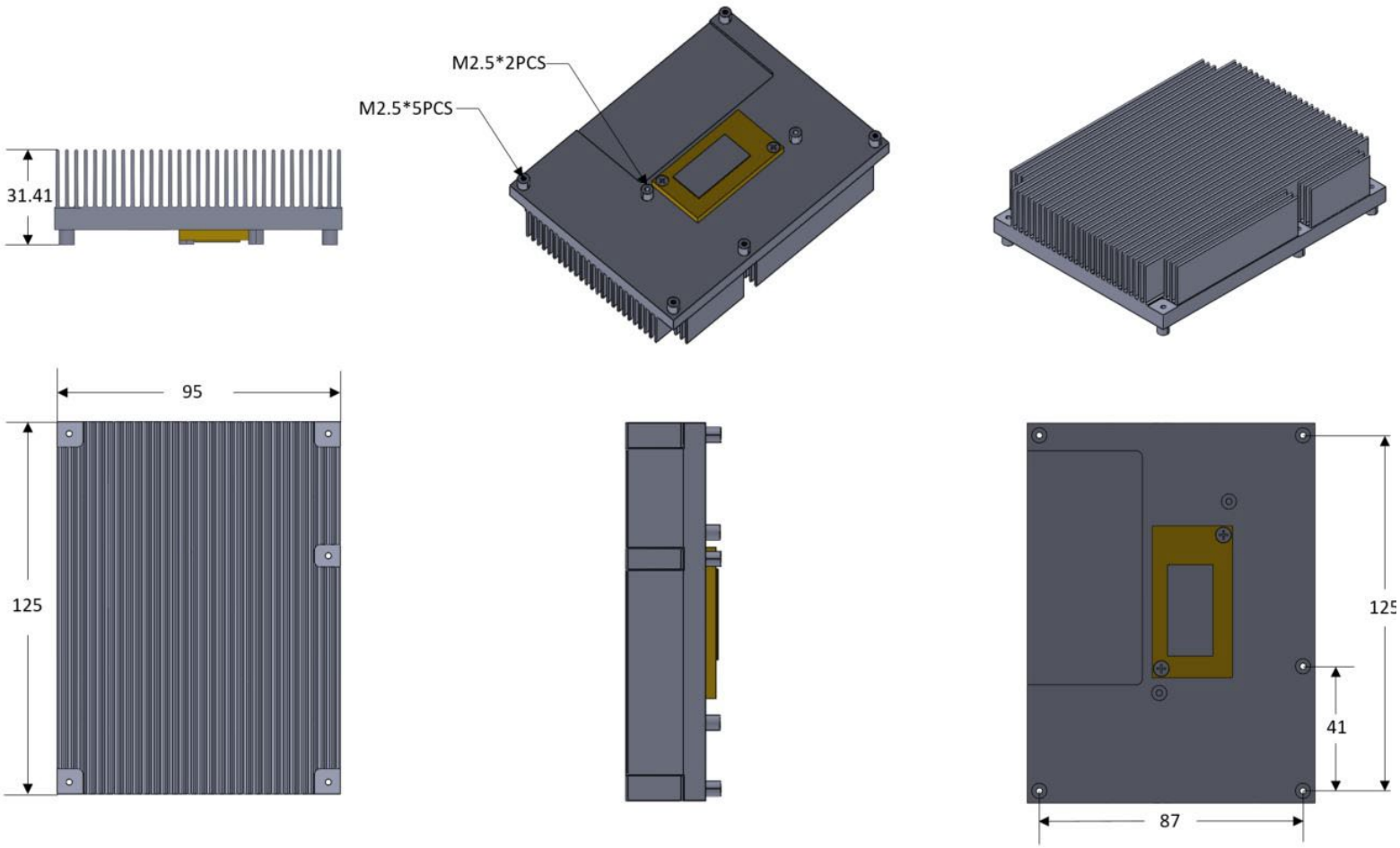


Figure 8 – Heatsink High Profile: THSH

10.2.4 Heatsink with Fan: THSF

Dimensions: mm

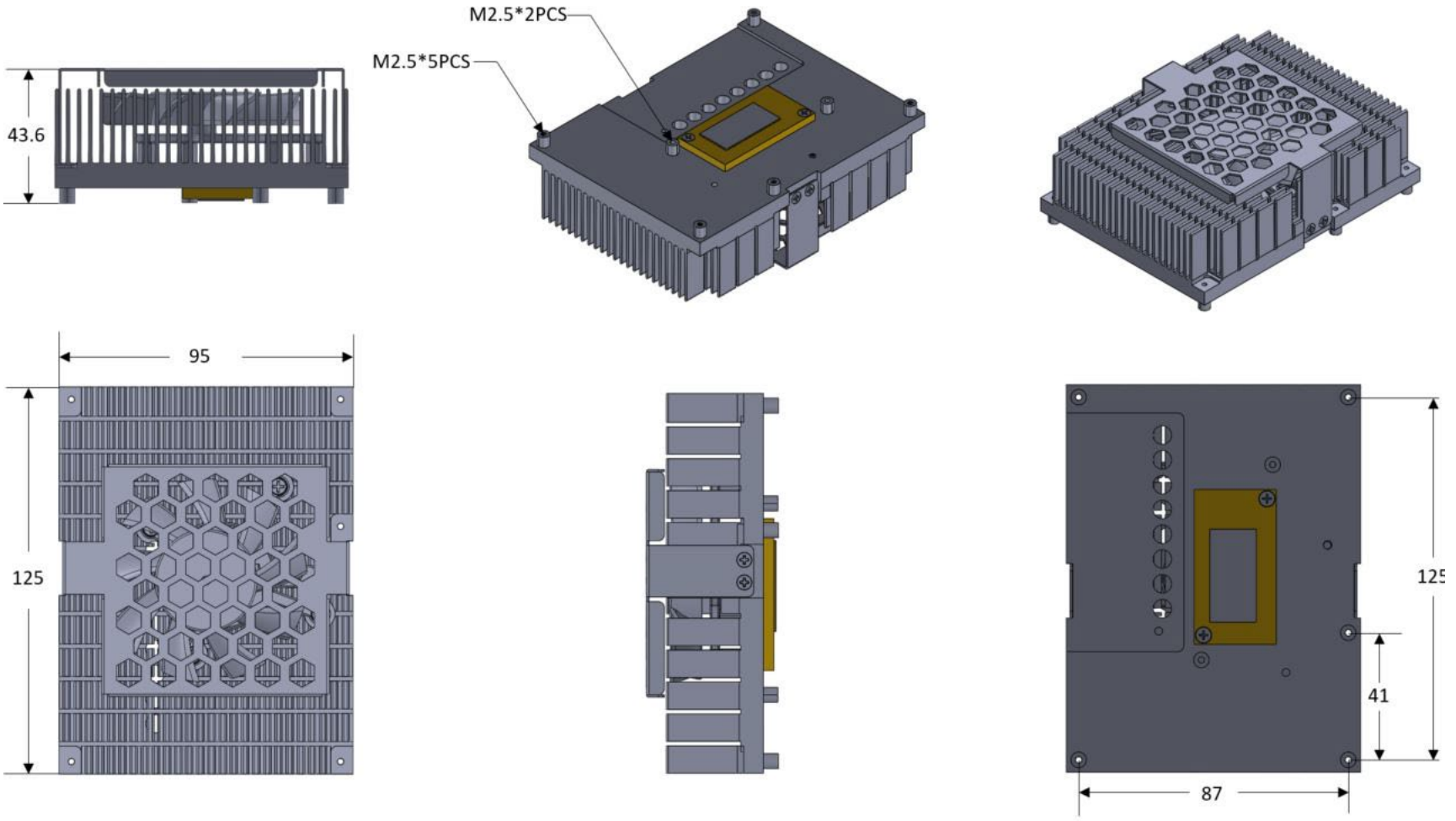


Figure 9 – Heatsink with Fan: THSF