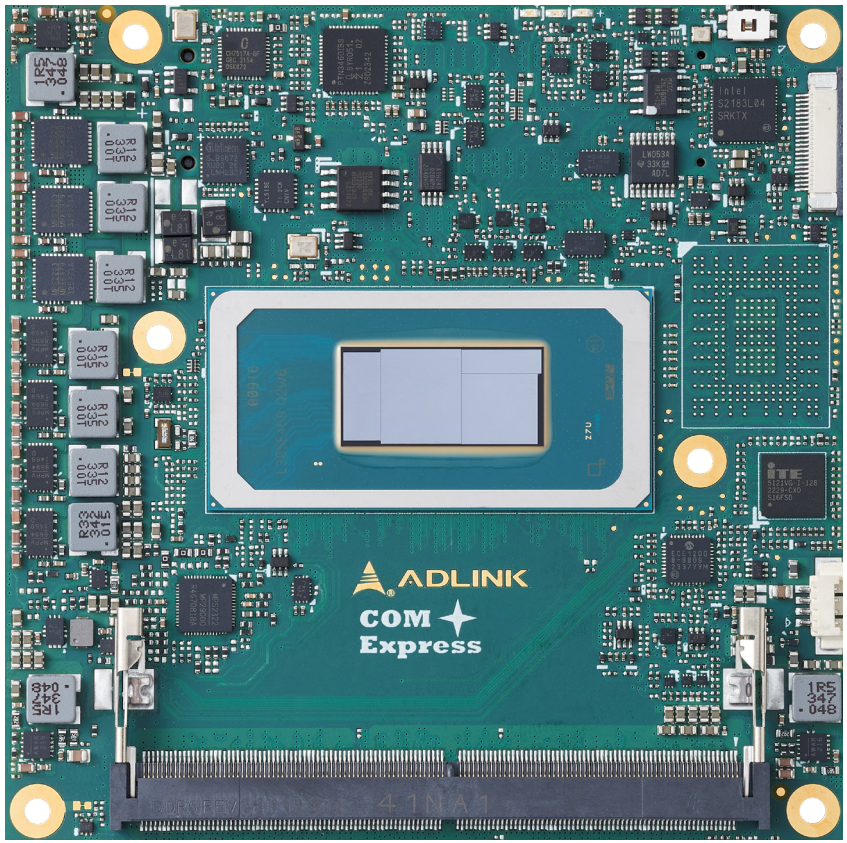
cExpress-MTL

User's Guide



COM Express®

Revision: Rev. 1.1
Date: 2025-05-29
Part Number: 50M-72221-1010

ADLINK
LEADING EDGE COMPUTING

Revision History

Revision	Description	Date	Author
1.0	Initial release	2025-03-11	AL
1.1	Pinout and signal descriptions updated	2025-05-29	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 © 2025 ADLINK Technology Incorporated

Safety Instructions

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

Read these safety instructions carefully.

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

Conventions

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

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

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

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

Getting Service

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

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

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

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

ADLINK Technology GmbH
Hans-Thoma-Strasse 8-10, 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 cExpress-MTL is a COM Express® COM.0 R3.1 Compact Size Type 6 module based on the intel® new generation edge/IoT platform on new Intel 4 process provides industry leading performance/watt. The new-generation Core™ Ultra processors (formerly "Meter Lake H/U") supporting up to 14 cores (Ultra 7) at maximum 28W TDP. Performance core and efficiency core improve multi-tasking ability include of two low power island E-core to reduce CPU power consumption. Up to 2x DDR5 SO-DIMMs supporting a maximum of 96GB memory capacity at up to 5600 MT/s. New integrated ARC graphics up to 128 EU that enhance close to two-time performance than previous generation platform. All CPU SKU build-in NPU to strengthen AI accelerator. Following PICMG R3.1 specifications all-around PCIe Gen4 support and integrated 2.5G Ethernet connectivity makes it suit for high-performance, low-power-consumption, powerful image processing capability and fast-response-required applications, including, but not limited to, video storage analytics, medical image presentation and analysis, intelligent surveillance, and industrial automation and control.

Meteor Lake has two kinds of cTDP CPU SKU (15W and 28W) can be choose. Low CPU power consumption means more suitable for use on handheld devices, such as handheld ultrasound devices. The module builds in PCIe gen 4 NVMe SSD in compact size dimension and new Integrated NPU for dedicated AI acceleration that reduces the system cost but improve the system AI processing ability. This design provides a better option for customer who have a strong need to reduce the size and cost of their product.

Input/output features include up to 24 PCIe Gen4 lanes, a single onboard 2.5-Gigabit Ethernet port, 4x USB 3.2/2.0 ports up to 10Gb/s, 2x SATA 6 Gb/s ports, independent four displays that resolution up to 8K. Additional General Purpose SPI (GP_SPI), two MIPI-CSI connectors to support cameras and onboard storage up to 1T capacity etc. option function. Support for SMBus and I2C is also provided. The module is equipped with SPI AMI EFI BIOS with CMOS backup, supporting embedded features such as a remote console, hardware monitor, and watchdog timer.

2. Specifications

2.1. Core System

CPU

Intel® Core™ Ultra Processors (formerly "Meteor Lake H/U")

- Intel® Core™ Ultra 7 155H 4.8/1.4GHz, 28W with 20-65W cTDP (16C/22T include 2 NPU)
- Intel® Core™ Ultra 5 135H 4.6/1.7GHz, 28W with 20-65W cTDP (14C/18T include 2 NPU)
- Intel® Core™ Ultra 5 125H 4.5/1.2GHz, 28W with 20-65W cTDP (14C/18T include 2 NPU)
- Intel® Core™ Ultra 5 135U 4.4/1.6GHz, 15W with 12-28W cTDP (12C/14T include 2 NPU)
- Intel® Core™ Ultra 5 125U 4.3/1.3GHz, 15W with 12-28W cTDP (12C/14T include 2 NPU)

Memory

Up to 96GB DDR5, dual memory channel in 2x SODIMM sockets, maximum 48GB per socket, non-ECC

Up to 5600 MT/s memory speed

1x SODIMM sockets on top side and 1x SODIMM sockets on bottom side

Cache (L3)

24MB: 155H

18MB: 135H, 125H

12MB: 135U, 125U

Embedded BIOS

AMI Aptio V UEFI with CMOS backup in 32 MB SPI BIOS

2.2. Video

GPU

Intel® X^e Graphics architecture with up to 128 execution units

Feature Support

Display Interface

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)

Graphics acceleration

DirectX 12 Video Acceleration (DXVA)/Open GL 4.6/Vulkan 1.2 and one VPL support for accelerated video processing

Video Decode

8K60 12b 4:2:0 HEVC/VP9/SCC

8K30 10b 4:2:0 AV1

5K60 10b 4:4:4 HEVC/VP9/SCC

4K60 8b 4:2:0 AVC

Video Encode

8K30 or 5K60 8b/10b 4:2:0 HEVC/VP9/SCC

4K60 10b 4:4:4 HEVC/VP9/SCC

4K60 8b 4:2:0 AVC

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

2.2.1. Display interface Support

DDI x3: Digital Display Ports (DDI) support DisplayPort 1.4a (via TBT4 w/Hayden Bridge can upgrade to DP 2.1), HDMI 2.1 or DVI.

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.

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

2.3. Audio

Intel® HD Audio integrated
Located on carrier Express-BASE6 or Express-BASE6 R3.1 (ALC886 standard support)

2.4. Expansion Buses

8 PEG Express Gen4: PEG Lane 0-7 (based on CPU SKU, 28W CPU SKU support)

PCIe reference clock uses PCIE_CK_REF6.

4 PEG Express Gen4: Two PEG Express Gen 4 at PEG Lane 8-11 and PEG Lane 12-15

4 PCI Express Gen4: Lanes 0-3 (configurable to 1 x4, 2 x2 and 4 x1)

2 PCI Express Gen4: Lane 4-5 (configurable to 1 x2 and 2 x1)

Note: 1. PCIe Gen4 support also depends on carrier board design.

2. PCIe lane 6-7 can be adjust at bios setup manual and combines PCIe Lane 4-5 can be configured 1 x4, 2 x2 and 4 x1 (sacrifice SATA 0-1)

3. PEG 0-7, 8-11, and 12-15 are recommended to be used for discrete graphics and storage purposes only.

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

I^2C from CPU is supported by BOM option and project basis

SMBus from EC (embedded controller) is supported by BOM option and project basis

Additional GP_SPI (general purpose SPI by project basis)

2.5. GbE Ethernet

Intel® Ethernet Controller I226 Series (V, IT or LM version)

Up to 2.5GbE, 1000/100/10 Mbit/s connections

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

2.6. Multi I/O and Storage

USB

- **USB4 x2**: 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 3.2 Gen2 x4**: USB port 0, 1, 2, 3 support
- **USB 2.0 x4**: USB port 4, 5, 6, 7 support

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

Up to 10Gb/s and also depends on carrier board design

USB_OC pins share the same source, from SoC.

Note: 1. Carrier board must be designed for Gen2 operation.

2. USB 0,1,2,3 are backward compatible with USB 2.0/1.1.

SATA

SATA x2: Speed up to 6Gb/s (SATA 0,1)

Note: 1. SATA [0:1] can be changed to PCIe[6:7] by bios setup menu.

UART

2x UART interfaces SER0 and SER1 RX/TX on module

Console Redirection COM 1 or COM 2 selectable in BIOS

SER0, SER1 from CPU UART are supported by BOM option and project basis

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

GPIO ~~or SD~~

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

GPI and GPO from CPU GPIO are supported by BOM option and project basis

MIPI-CSI

MIPI-CSI x1: 4 Lanes MIPI-CSI interface and supports camera video capture up to 750MP/s

2.7. Trusted Platform Module (TPM)

Chipset: Infineon solution

Type: TPM 2.0 (SPI bus-based)

2.8. NVMe SSD

NVMe SSD x1: Support PCIe Gen 4 x4 and the max capacity up to 1TB

2.9. SEMA Board Controller

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

2.10. 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

2.11. Power

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

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

Wide Voltage Input: AT: 8.5-20V or ATX: 8.5-20V / 5Vsb ±5% (only for standard operating temperature)

Power Management: ACPI 5.0 compliant

Power States: C0-C6, S0, S5, S5 ECO mode (Wake-on-USB S3/S4, WoL S3/S4/S5). ECO Mode support for deep S5 for 5Vsb power saving

Note: 1. S3 support by AMI workaround. Intel will official release the S3 POR at 2025 Q1

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

2.12. Mechanical and Environmental

Form Factor and specification

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

Operating Temperature

Standard	0°C to 60°C	Storage: -20°C to 80°C
Extreme Rugged	-40°C to 85°C	Storage: -40°C to 85°C

Humidity

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

Shock and Vibration

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

HALT tested

Thermal Stress, Vibration Stress, Thermal Shock and Combined Test

3. Block Diagram

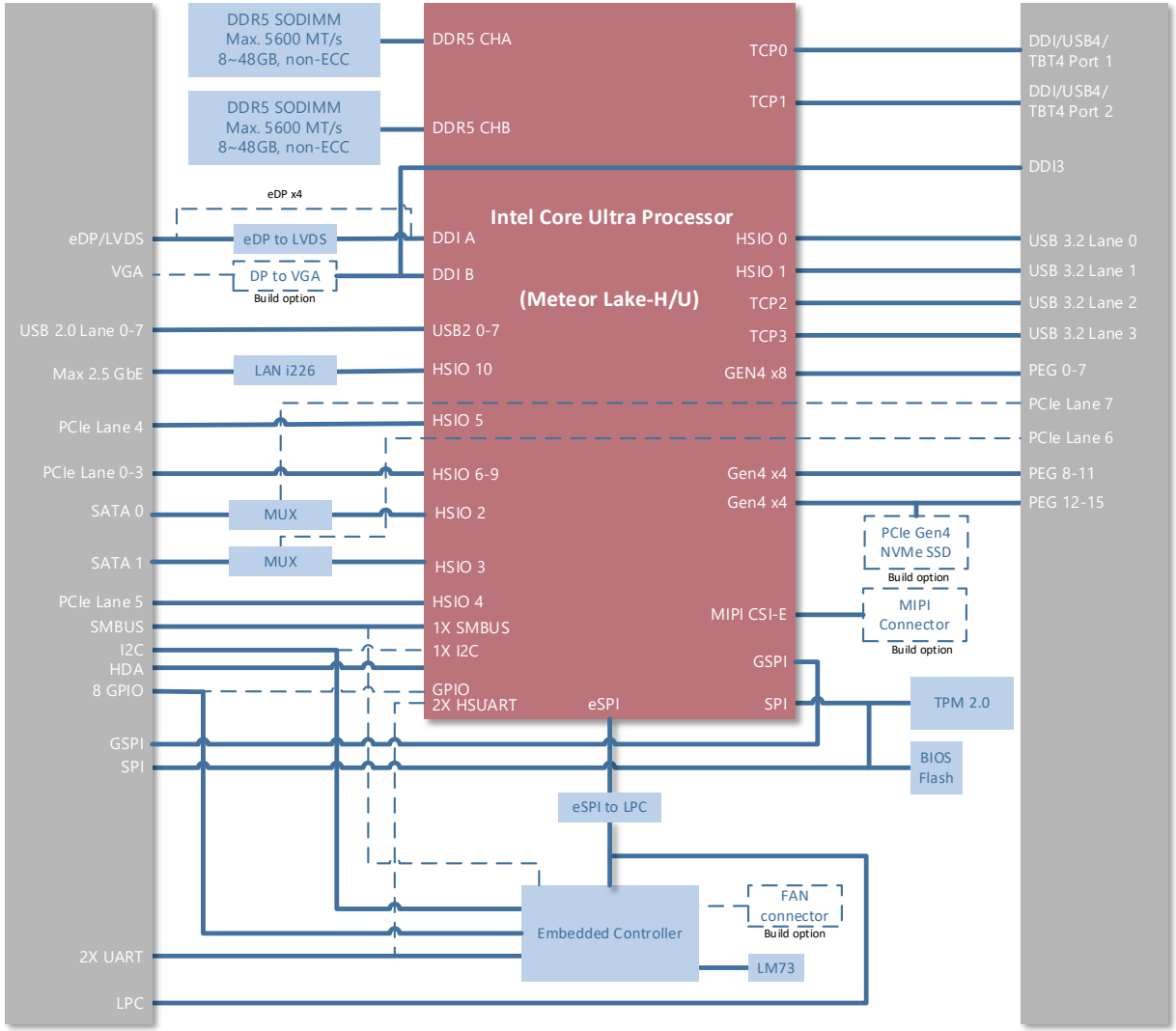


Figure 1 – Module functional block diagram

4. Pinout and Signal Descriptions

4.1. Pin Summary

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

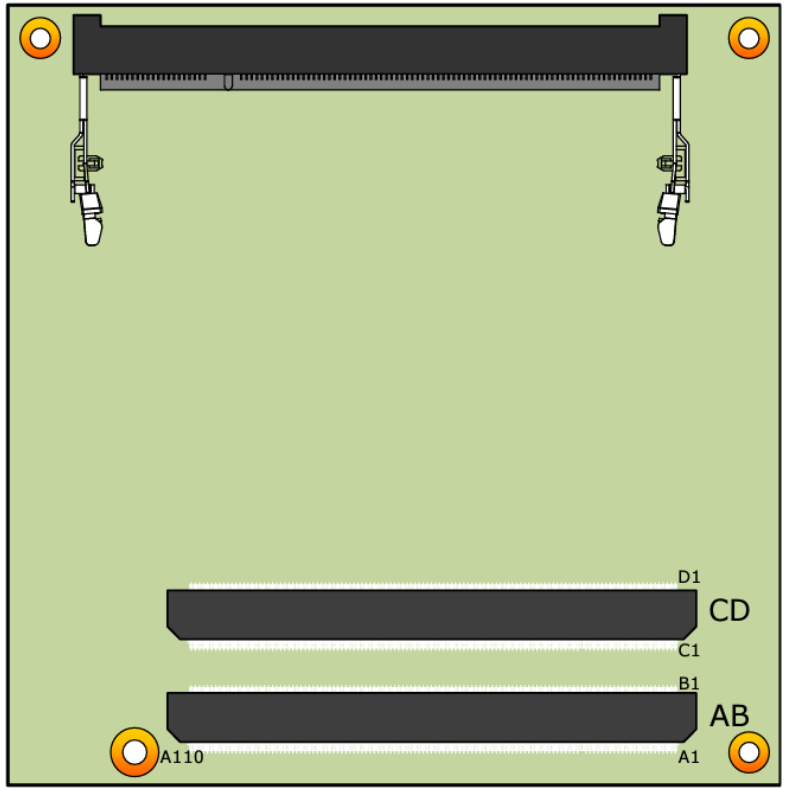


Figure 2 – Module rear side row and pin numbering

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 28W 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 on a project basis.
2. GP_SPI and SNDW0 support TBC.

4.2 Signal Terminology Descriptions

Definitions of terms used in signal description tables

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

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 (I²C 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 supported as a BOM option (in place of DDI 3) on a 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 is available that removes the eDP to LVDS bridge IC and outputs the eDP signals directly. 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 the carrier board SPI BIOS Flash.	O 3.3VSB	PU 10K 3.3VSB	
SPI_MISO	A92	Data in to module from the carrier board SPI BIOS flash.	I 3.3VSB		
SPI_MOSI	A95	Data out from module to the carrier board SPI BIOS flash.	O 3.3VSB		
SPI_CLK	A94	Clock from module to the carrier board SPI BIOS flash.	O 3.3VSB		
SPI_POWER	A91	Power supply for the carrier board SPI – sourced from the 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 2.2K 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 2.2K 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 4.7K 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 the module to reset and reboot. It may be falling edge sensitive. In situations where SYS_RESET# is unable 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 the module to the carrier board. Active low. Issued by the 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 it may be initiated by the module software.	O 3.3V		
PWR_OK	B24	Power OK from the main power supply. A high value indicates that the power is good. This signal can be used to hold off module startup, allowing 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 an imminent suspend operation; used to notify LPC devices.	O 3.3VSB		
SUS_S3#	A15	Indicates that the system is in the 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 that the system is in suspend to Disk state. Active low output.	O 3.3VSB	PD 100K	
SUS_S5#	A24	Indicates that the 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 of 5— 20V input. All available VCC_12V pins on the connector(s) should 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) should 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 36.

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, while 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 a floating pin on the carrier enable 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 a pull high on the carrier enable HDMI 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, while 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 a floating pin on the carrier enable 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 coupling on the module
HDMI2_CTRLDATA	C33	I2C_DAT Line for HDMI	I/O PCIE	PU 2.2K	AC coupling on the module
DDI2_DDC_AUX_SEL	C34	Strapping Signal to select HDMI or DP output 1M pull-down on the module and a pull high on the carrier enable HDMI 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, while 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 a floating pin on the carrier enable 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 a pull high on the carrier enable HDMI 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
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+	D71 D72	PCI Express Graphics transmit differential pairs.	O PCIE		AC coupled on Module

Name	Pin #	Description	I/O	PU / PD	Comment
PEG_TX6-		These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6			
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
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

Name	Pin #	Description	I/O	PU / PD	Comment
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		

4.4.7 Module Type Definition

<table>
<tr><th>Name</th><th>Pin #</th><th>Description</th><th>I/O</th><th>PU / PD</th><th>Comment</th></tr>
<tr><td>TYPE0#
TYPE1#
TYPE2#</td><td>C54
C57
D57</td><td>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)

<table>
<tr><th>TYPE2#</th><th>TYPE1#</th><th>TYPE0#</th><th></th></tr>
<tr><td>X</td><td>X</td><td>X</td><td>Pinout Type 1</td></tr>
<tr><td>X</td><td>X</td><td>X</td><td>Pinout Type 10</td></tr>
<tr><td>NC</td><td>NC</td><td>NC</td><td>Pinout Type 2</td></tr>
<tr><td>NC</td><td>NC</td><td>GND</td><td>Pinout Type 3</td></tr>
<tr><td>NC</td><td>GND</td><td>NC</td><td>Pinout Type 4</td></tr>
<tr><td>NC</td><td>GND</td><td>GND</td><td>Pinout Type 5</td></tr>
<tr><td>GND</td><td>NC</td><td>NC</td><td>Pinout Type 6</td></tr>
<tr><td>GND</td><td>NC</td><td>GND</td><td>Pinout Type 7</td></tr>
</table>

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.</td><td></td><td></td><td>Type 6</td></tr>
<tr><td>TYPE10#</td><td>A97</td><td>In case of a type 10 module this pin signal is tied to GND through a 47K resistor on the module.</td><td></td><td></td><td>No PD</td></tr>
</table>

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 to 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 follows:

5.1 Module Feature Locations

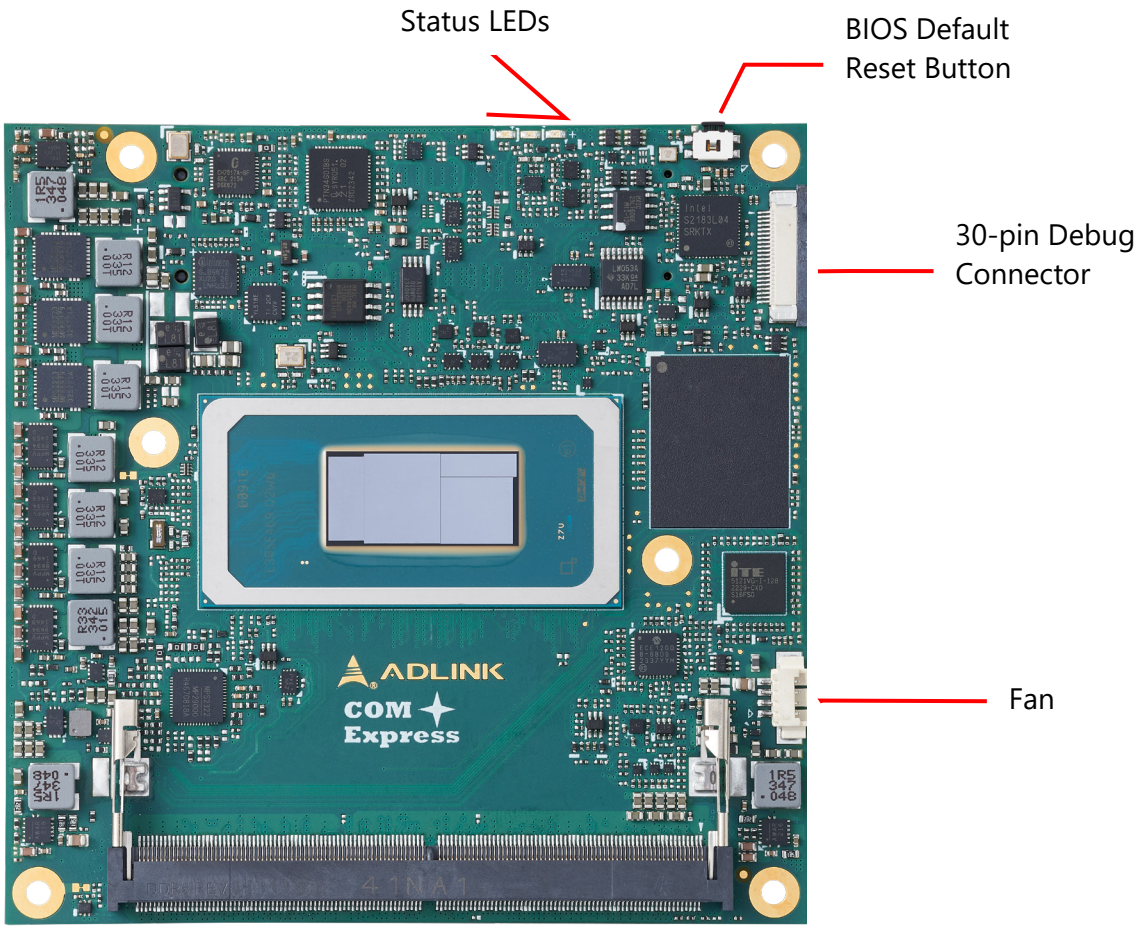


Figure 3 – Module feature locations (top side)

5.2 Debug Connector

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

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

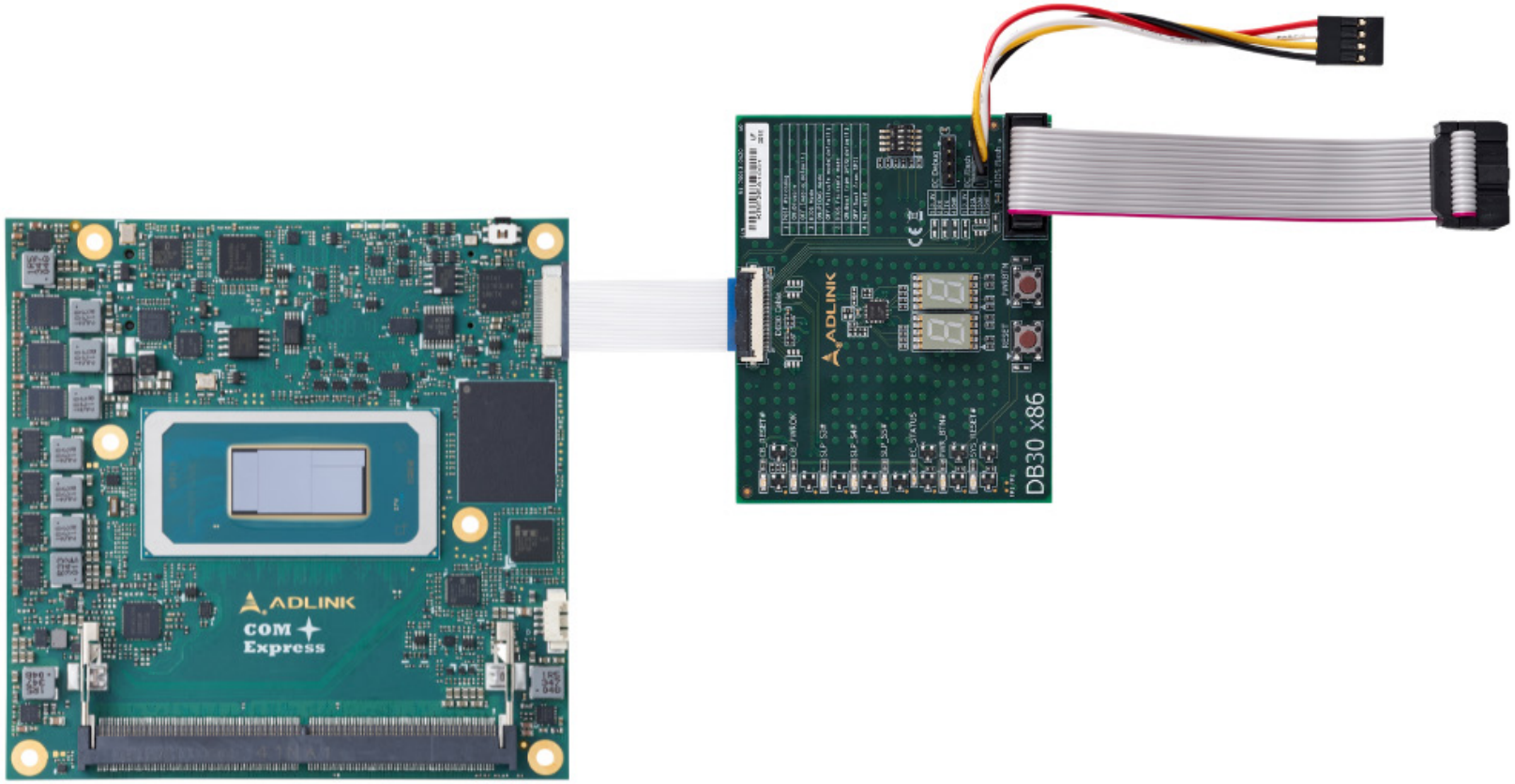
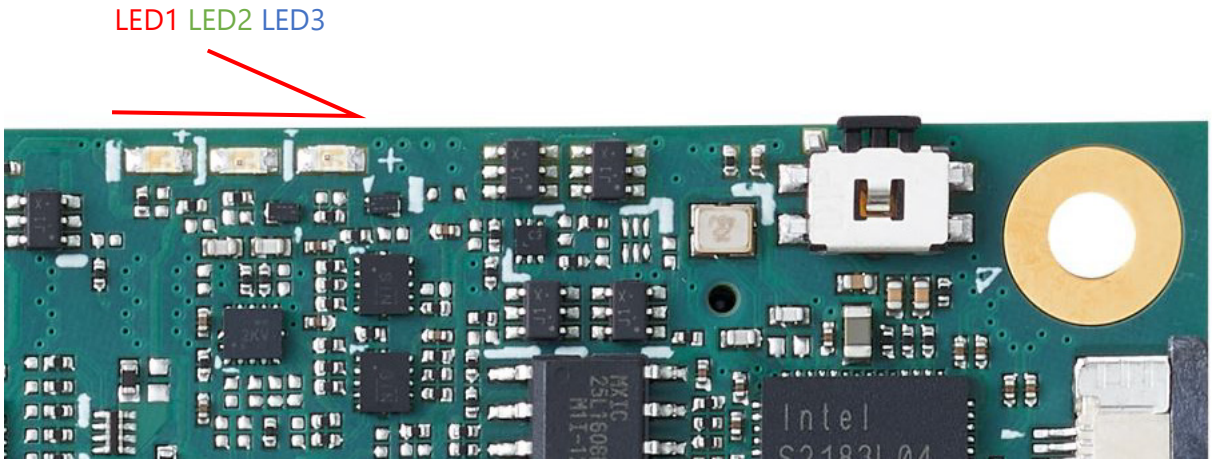


Figure 4 – cExpress-MTL and debug module

5.3 Status LEDs

Status LEDs are mounted on the module to facilitate easier maintenance.



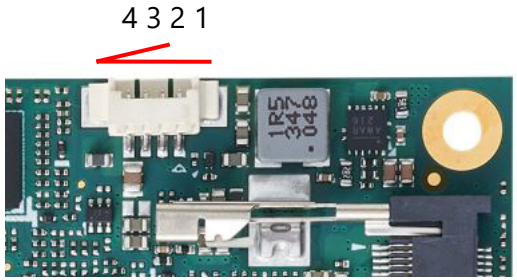
Name	Color	Connection	Function
LED1	Blue	EC output	Power Sequence Status Code (EC) Power Changes, RESET (see Exception Codes below)
LED2	Green	Power Source 3Vcc	S0 LED ON S3/S4/S5 LED OFF ECO mode LED OFF
LED3	Red	EC output and same signal as WDT (B27) on BtB connector	Module power up WD LED = LED OFF 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

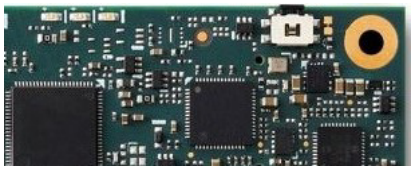
5.5 Fan Connector

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. Press and hold the BIOS Setup Defaults Reset button, then 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 the BIOS defaults have been reset and will request that you reboot the system.

6. System Resources

6.1. System Memory Map

Address Range (hex)	Description
00000000000A0000-000000008BFFFFFF	PCI Express Root Complex
000000008C000000 -000000008CFFFFFF	Intel RST VMD Controller 7D0B
000000008D000000-000000008D2FFFFF	PCI Express Root Port
000000008D300000-000000008D303FFF	Standard NVM Express Controller
000000008D400000-000000008D4030FF	Standard SATA AHCI Controller
00000000BFFFF000-00000000BFFFFFFF	Intel Active Management Technology-SOL
00000000C0000000-00000000CFFFFFFF	Motherboard resource
00000000E0D10000-00000000E0D5FFFF	Intel Serial IO GPIO Host Controller-INTC1083
00000000FC800000-00000000FC81FFFF	Motherboard resource
00000000FE010000-00000000FE010FFF	Intel SPI-7E23
00000000FED00000-00000000FED003FF	High precision event timer
00000000FED20000-00000000FED7FFFF	Motherboard resource
00000000FED40000-00000000FED44FFF	Trusted Platform Module 2.0
00000000FED45000-00000000FEEFFFFF	Motherboard resource
0000004000000000-0000005010FFFFFF	Intel Graphics
0000005012000000-0000005014FFFFFF-	Intel RST VMD Controller 7D0B
0000005016200000-000000501623FFFF	Thunderbolt Controller -7EC2
00000050162A0000-00000050162BFFFF	Intel USB 3.20 eXtensible Host Controller -1.20

Address Range (hex)	Description
00000050162C8000-00000050162C80FF	Intel SMBus -7E22
00000050162CA000-00000050162CAFFF	Intel Serial IO Host Controller -7E51
00000050162CB000-00000050162CBFFF	Intel Serial IO Host Controller -7E50
00000050162CC000-00000050162CCFFF	Intel Management Engine Interface #1
00000050162CD000-00000050162CDFFF	Intel Serial IO Host Controller -7E7B
00000050162CE000-00000050162CEFFF	Intel Serial IO Host Controller -7E79
00000050162CF000-00000050162CFFFF	Intel Serial IO Host Controller -7E78
00000050162D1000-00000050162D1FFF	Thunderbolt Controller -7EC2
0000006010000000-0000006010FFFFFF	Intel Graphics
0000006016200000-0000006016312FFF	Thunderbolt Controller -7EC3
000003FFBEC00000-000003FFBEFFFFFF	Intel Imaging Signal Processor
000003FFBFC00000-000003FFBFDFFFFF	High-Definition Audio Controller
000003FFBFF80000-000003FFBFF9FFFF	Intel Innovation Platform Framework Processor Participant
000003FFBFFBA000-000003FFBFFBAFFF	Intel Serial IO UART Host Controller -7E25
000003FFBFFBB000-000003FFBFFBBFFF	Intel GNA Scoring Accelerator module
000003FFBFFBC000-000003FFBFFBFFFF	High-Definition Audio Controller
000003FFBFFFC000-000003FFBFFFFFFF	Intel Platform Monotoring (PMT) Driver

6.2. I/O Map

Hex Range	Device
00h - 07h	Communications Port (COM1)
20h – 2Dh	Programmable Interrupt controller
2Eh - 2Fh 4Eh - 4Fh	LPC SIO (W83627DHGSEC / NCT6126D) configuration index/data registers
30h – 3Dh	Programmable Interrupt controller
40h - 43h	System Timer
60h & 64h	PS2 Keyboard Mouse
61h	Motherboard resources
62h/66h, 68h/6Ch	IT5121E
67h - 92h	Real Time Clock Controller
A0h - B1h	Programmable Interrupt controller
B2h – B3h	Motherboard resources
B4h – BDh	Programmable Interrupt controller
200h - 201h	IT5121E
240h - 247h	Serial port 3 (COM3)
248h - 24Fh	Serial port 4 (COM4)
2F8h – 2FFh	Serial port 2 (COM2)
3F8h - 3FFh	Serial port 1 (COM1)
4D0h – 4D1h	Programmable Interrupt controller
680h – A6Fh	Motherboard resources
D00h – FFFFh	PCI Express Root Complex

Hex Range	Device
164Eh – 20FEh	Motherboard resources
3020h – 3057h	Standard SATA AHCI Controller
EFA0h – EFBFh	Intel SMBus – 7E22

6.3. Interrupt Request (IRQ) Lines

APIC Mode

IRQ#	Typical Interrupt Resource	Connected to Pin	Available
0	System timer	N/A	No
1	Standard PS/2 Keyboard	IRQ1 via SERIRQ	No
3	Serial Port 2	IRQ3 via SERIRQ	COM2
4	Serial Port 1	IRQ4 via SERIRQ	COM1
5	Serial Port 3	IRQ5 via SERIRQ	COM3
7	Serial Port 4	IRQ7 via SERIRQ	COM4
12	Standard PS/2 Mouse	IRQ12 via SERIRQ	No
14	Intel Serial IO Host GPIO Controller	N/A	No
16	High-Definition Audio Controller	N/A	No
16	Intel Serial IO UART Host Controller	N/A	No
19	Intel Active Management Technology	N/A	No
29	Intel Serial IO I2C Host Controller 7E50	N/A	No
30	Intel Serial IO I2C Host Controller 7E51	N/A	No
32	Intel Serial IO I2C Host Controller 7E78	N/A	No
33	Intel Serial IO I2C Host Controller 7E79	N/A	No

IRQ#	Typical Interrupt Resource	Connected to Pin	Available
35	Intel Serial IO I2C Host Controller 7E7B	N/A	No
55 to 511	Microsoft ACPI Compliant System	N/A	No
-76	Intel GNA Scoring Accelerator module	N/A	No
-75 to -63	Intel Ethernet Controller I226-IT	N/A	No
-62	Intel Management Engine Interface	N/A	No
-61	Intel USB 3.20 eXtensible Host Controller -1.20	N/A	No
-60 to -45	Thunderbolt Controller -7EC2	N/A	No
-44	Intel USB 3.20 eXtensible Host Controller -1.20	N/A	No
-43	Intel Graphics	N/A	No
-42 to -24	Intel RST VMD Controller 7D0B	N/A	No
-23 to -7	Standard NVM Express Controller	N/A	No
-6	Standard SATA AHCI Controller	N/A	No
-5 to -2	PCI Express Root Port	N/A	No

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

6.4. PCI Configuration Space Map

Bus Number	Device Number	Function Number	Routing	Description
00h	00h	00h	Internal	Intel Corporation Host Bridge
00h	02h	00h	Internal	Intel Corporation VGA Controller
00h	04h	00h	Internal	Intel Corporation Data Acquisition
00h	05h	00h	Internal	Intel Corporation Multimedia Device
00h	06h	00h	Internal	Intel Corporation PCI To PCI Bridge
00h	06h	02h	Internal	Intel Corporation PCI To PCI Bridge
00h	07h	00h	Internal	Intel Corporation PCI To PCI Bridge
00h	07h	01h	Internal	Intel Corporation PCI To PCI Bridge
00h	08h	00h	Internal	Intel Corporation System Device
00h	0Ah	00h	Internal	Intel Corporation Data Acquisition
00h	0Dh	00h	Internal	Intel Corporation XHCI USB Controller
00h	0Dh	02h	Internal	Intel Corporation USB Controller
00h	0Eh	00h	Internal	Intel Corporation RAID Controller
00h	14h	00h	Internal	Intel Corporation XHCI USB Controller
00h	14h	02h	Internal	Intel Corporation RAM Controller
00h	15h	00h	Internal	Intel Corporation Controller
00h	15h	01h	Internal	Intel Corporation Controller
00h	15h	03h	Internal	Intel Corporation Controller
00h	16h	00h	Internal	Intel Corporation Communication Device
00h	16h	03h	Internal	Intel Corporation Serial Device
00h	17h	00h	Internal	Intel Corporation AHCI Controller

Bus Number	Device Number	Function Number	Routing	Description
00h	19h	00h	Internal	Intel Corporation Controller
00h	19h	01h	Internal	Intel Corporation Controller
00h	1Eh	00h	Internal	Intel Corporation Communication Device
00h	1Fh	00h	Internal	Intel Corporation ISA Bridge
00h	1Fh	03h	Internal	Intel Corporation HD Audio Device
00h	1Fh	04h	Internal	Intel Corporation SMBus Controller
00h	1Fh	05h	Internal	Intel Corporation Controller
01h	00h	00h	Internal	Intel Corporation Elthernet Controller
02h	00h	00h	Internal	Mass Storage Controller

6.5. PCI Interrupt Routing Map

INT Line	IOE PCIE Port 1	IOE PCIE Port 2	Lpc Bridge	HD Audio Controller	SMBus	SATA Controller
Int0	INTA:16	INTA:16	INTA:16	INTC:34	none	INTA:16
Int1	INTB:17	INTB:17	INTB:17	INTD:35	none	none
Int2	INTC:18	INTC:18	INTC:18	INTA:32	INTC:18	none
Int3	INTD:19	INTD:19	INTD:19	INTB:33	none	none

INT Line	XHCI Controller	TypeC Subsystem XHCI	ITBT PCIE Port 0	ITBT PCIE Port 1	ITBT PCIE Port 2	ITBT PCIE Port 3
Int0	INTA:16	INTA:16	INTA:16	INTA:16	INTA:16	INTA:16
Int1	INTB:17	INTA:17	INTB:17	INTB:17	INTB:17	INTB:17
Int2	none	none	INTC:18	INTC:18	INTC:18	INTC:18
Int3	none	none	INTD:19	INTD:19	INTD:19	INTD:19

INT Line	PCIE Port1	PCIE Port 2	PCIE Port 3	PCIE Port 4	PCIE Port 5	PCIE Port 6	PCIE Port 7	PCIE Port 8
Int0	INTA:16	INTB:17	INTC:18	INTD:19	INTA:16	INTB:17	INTC:18	INTD:19
Int1	INTB:17	INTC:18	INTD:19	INTA:16	INTB:17	INTC:18	INTD:19	INTA:16
Int2	INTC:18	INTD:19	INTA:16	INTB:17	INTC:18	INTD:19	INTA:16	INTB 17
Int3	INTD:19	INTA:16	INTB:17	INTC:18	INTD:19	INTA:16	INTB:17	INTC:18

6.6. SMBus Address Table

Device	Address
DDR5 Channel A(SO-DIMM1)	A0h
DDR5 Channel B(SO-DIMM2)	A2h

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 System Date System Time	CPU Configuration ► Power & Performance ► Graphics Configuration ► Platform Settings ► Power Management ► System Management ► Thermal Management ► Watchdog Timer ► USB Configuration ► AMI Graphic Output Protocol Policy ► Super IO Configuration ► Serial Port Console Redirection ► Miscellaneous ► Network Stack Configuration ► NVME Configuration ► Trusted Computing ► Intel Ethernet Controller ►	System Agent (SA) Configuration ► PCH-IO Configuration ►	Password Description Secure Boot Menu ►	Boot Configuration	Save Options Default Options Boot Override

Note: ► indicates a submenu
Gray text indicates info only

7.2. Main

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

7.2.1. BIOS Information

Feature	Options	Description
BIOS Vender	Info only	American Megatrends
BIOS Version	Info only	Displays Core version
Build Date	Info only	Displays compliancy information
MRC Version	Info only	Displays compliancy information
GOP Driver Version	Info only	Displays Intel Graphic Version
ME FW Version	Info only	Displays Intel CSME Version

7.2.2. System Information

Board Information	Info only	Description
Project Name	Info only	Displays Project Name
CPU Board Version	Info only	Displays CPU Signature
CPU Brand String	Info only	Displays CPU Brand Name
Stepping	Info only	Displays CPU Stepping
CPU Frequency	Info only	Displays CPU Frequency
Total Memory	Info only	Displays installed memory size
Memory Frequency	Info only	Displays memory frequency

PCH SKU	Info only	Displays PCH Information.
Board Information	Submenu	

7.2.3. Board Information

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

7.2.4. System Date and Time

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

Feature	Options	Description
Access Level	Info only	

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 information.
VMX	Info only	Display Intel Virtualization Technology support or not.
SMX/TXT	Info only	Display Intel SMX Technology support or not.
Intel (VMX) Virtualization Technology	Disabled, **Enabled**	When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.
Active Performance-cores	**All**, 5, 4, 3, 2, 1	Number of P-cores to enable in each processor package. Note: Number of Cores and E-cores are looked at together. When both are {0,0}, Pcode will enable all cores.
Active Efficient-cores	**All**,7,6,5,4,3,2,1,0	Number of E-cores to enable in each processor package. Note: Number of Cores and E-cores are looked at together. When both are {0,0}, Pcode will enable all cores.
Hyper-Threading	Disabled, **Enabled**	Enable or Disable Hyper-Threading Technology.
Intel Trusted Execution Technology	**Disabled**, Enabled	Enables utilization of additional hardware capabilities provided by Intel (R) Trusted Execution Technology. Changes require a full power cycle to take effect.
Total Memory Encryption	**Disabled** Enabled	Configure Total 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**	Select the performance state that the BIOS will set starting from reset vector.
Intel(R) SpeedStep(tm)	Disabled, **Enabled**	Allows more than two frequency ranges to be supported.
Race To Halt (RTH)	Disabled, **Enabled**	Enable/Disable Race To Halt feature. RTH will dynamically increase CPU frequency in order to enter pkg C-State faster to reduce overall power. (RTH is controlled through MSR 1FC bit 20)
Intel(R) Speed Shift Technology	Disabled, **Enabled**	Enable/Disable Intel(R) Speed Shift Technology support. Enabling will expose the CPPC v2 interface to allow for hardware-controlled P-states.
Per Core P State OS control P State	Disabled, **Enabled**	Enable/Disable Per Core P state OS control mode. Disabling will set Bit 31 = 1 command 0x06. When set, the highest core request is used for all other core requests.
HwP Autonomous Per Core P State	Disabled, **Enabled**	Disable Autonomous PCPS (Bit 30 = 1, command 0x11) Autonomous will request the same value for all cores all the time. Enable PCPS (default Bit 30 = 0, command 0x11)
HwP Autonomous EPP Grouping	Disabled, **Enabled**	Enable EPP grouping (default Bit 29 =0, command 0x11) Autonomous will request the same values for all cores with same EPP. Disable EPP grouping (Bit 29 =1 , command 0x11) autonomous will not necessarily request same values for all cores with same EPP.
EPB override over PECI	**Disabled**, Enabled	Enable/Disable EPB override over PECI. Enable by sending pcode command 0x2b , subcommand 0x3 to 1. This will allow OOB EPB PECI override control
HwP Lock	Disabled, **Enabled**	Enable/Disable HWP Lock support in Misc Power Management MSR.
HDC Control	Disabled, **Enabled**	This option allows HDC configuration.
Turbo Mode	Disabled, **Enabled**	Enable/Disable processor Turbo Mode (requires EMTTM enabled too). AUTO means enabled.
View/Configure Turbo Options	Submenu	

Feature	Options	Description
Current Turbo Settings		
Max Turbo Power Limit	Info only	
Min Turbo Power Limit	Info only	
Power Limit 1	Info only	
Power Limit 2	Info only	
Energy Efficient P-state	Disabled, **Enabled**	Enable/Disable Energy Efficient P-state feature. When set to 0, will disable access to ENERGY_PERFORMANCE_BIAS MSR and CPUID Function 6 ECX[3] will read 0 indicating no support for Energy Efficient policy setting. When set to 1 will enable access to ENERGY_PERFORMANCE_BIAS MSR 1B0h and CPUID Fun
Package Power Limit MSR Lock	**Disabled**, Enabled	Enable/Disable locking of Package Power Limit settings. When enabled, PACKAGE_POWER_LIMIT MSR will be locked and a reset will be required to unlock the register.
Energy Efficient Turbo	Disabled, **Enabled**	Enable/Disable Energy Efficient Turbo Feature. This feature will opportunistically lower the turbo frequency to increase efficiency. Recommended only to disable in overclocking situations where turbo frequency must remain constant. Otherwise, leave enabled.
Config TDP Configurations	Submenu	
Config TDP Configurations		
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 TDP 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 ConfigTDP Count will be forced to 1 and Custom ConfigTDP Boot Index will be forced to 0.

Feature	Options	Description
ConfigTDP Levels	3	
ConfigTDP Turbo Activation Ratio	24 (Unlocked)	
Power Limit 1	45.0W (MSR:45.0)	
Power Limit 2	115.0W (MSR:115.0)	
Custom Settings Nominal		
ConfigTDP Nominal	Ratio:25 TAR:24 PL1:13.0W	
Power Limit 1	0	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	0	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 time window which TDP value should be maintained.
ConfigTDP 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 Level1		
ConfigTDP Level1	Ratio:18 TAR:17 PL1:3.0W	
Power Limit 1	0	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	0	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

Feature	Options	Description
		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 time window which TDP value should be maintained.
ConfigTDP Turbo Activation Ratio	0	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 Level2		
ConfigTDP Level2	Ratio:28 TAR:27 PL1:1.0W	
Power Limit 1	0	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	0	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 time window which TDP value should be maintained.
ConfigTDP Turbo Activation Ratio	0	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	136	
PSYS Slope	0	PSYS Slope defined in 1/100 increments. Range is 0-200. For a 1.25 slope, enter 125. 0 = AUTO. Uses BIOS VR mailbox command 0x9."
PSYS Offset	0	PSYS Offset defined in 1/1000 increments. Range is 0-63999. For an offset of 25.348, enter 25348. PSYS Uses BIOS

Feature	Options	Description
		VR mailbox command 0x4.
PSYS Prefix	**+**, -	Sets the offset value as positive or negative.
PSYS PMax Power	0	PSYS PMax power, defined in 1/8 Watt increments. Range 0-8192. For a PMax of 125W, enter 1000. 0 = AUTO. Uses BIOS VR mailbox command 0xB.
Min Voltage Override	**Disabled**, Enabled	Min Voltage Override. Enable to override minimum voltage for runtime and for C8.
VccIn Aux Icc Max	0	Sets the Max Icc VccIn Aux value defined in 1/4A increments. Range is 0-512. For an IccMax 32A, enter 128(32*4).
VccIn Aux IMON Slope	100	VccIN Aux IMON Slope defined in 1/100 increments. Range is 0-200. For a 1.25 slope, enter 125. 0 = AUTO. Uses BIOS VR mailbox command 0x18.
VccIn Aux IMON Offset	0	VccIN Aux IMON Offset defined in 1/1000 increments. Range is 0-63999. For an offset of 25.348, enter 25348. IMON Uses BIOS VR mailbox command 0x18.
VccIn Aux IMON Prefix	**+.-**	Sets the offset value as positive or negative.
Vsys/Psys Critical	**Disabled**,Psys Critical,Vsys Critical	Vsys/Psys Critical Enable or disable
Assertion Deglitch Mantissa	**1**	Assertion Deglitch Mantissa 0x4F[7-3]. Assertion Deglitch = 2µs * Mantissa * 2^(Exponent)
Assertion Deglitch Exponent	**0**	Assertion Deglitch Exponent 0x4F[3-0]. Assertion Deglitch = 2µs * Mantissa * 2^(Exponent)
De assertion Deglitch Mantissa	**13**	De Assertion Deglitch Mantissa 0x49[7-3]. Assertion Deglitch = 2µs * Mantissa * 2^(Exponent)
De assertion Deglitch Exponent	**2**	De Assertion Deglitch Exponent 0x49[3-0]. Assertion Deglitch = 2µs * Mantissa * 2^(Exponent)
VR Power Delivery Design	**Auto**	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	0	Set the maximum Pre Wake randomization time in micro ticks. Range is 0-255. This is for acoustic noise mitigation Dynamic Periodicity Alteration (DPA) tuning.
Ramp Up Time	0	Set the maximum Ramp Up randomization time in micro ticks. Range is 0-255. This is for acoustic noise mitigation Dynamic Periodicity Alteration (DPA) tuning.
Ramp Down Time	0	Set the maximum Ramp Down randomization time in micro ticks. Range is 0-255. This is for acoustic noise mitigation Dynamic Periodicity Alteration (DPA) tuning.
IA VR Domain		
Disable Fast PKG C State Ramp for IA Domain	**FALSE**, TRUE	This option needs to be configured to reduce acoustic noise during deeper C states. False: Don't disable Fast ramp during deeper C states; True: Disable Fast ramp during deeper C state.
Slow Slew Rate for IA Domain	**Fast/2,** Fast/4, Fast/8, Fast/16	Set VR IA Slow Slew Rate for Deep Package C State ramp time; Slow slew rate equals to Fast divided by number, the number is 2, 4, 8, 16 to slow down the slew rate to help minimize acoustic noise
GT VR Domain		
Disable Fast PKG C State Ramp for GT Domain	**FALSE**, TRUE	This option needs to be configured to reduce acoustic noise during deeper C states. False: Don't disable Fast ramp during deeper C states; True: Disable Fast ramp during deeper C state
Slow Slew Rate for GT Domain	**Fast/2,** Fast/4, Fast/8	Set VR GT Slow Slew Rate for Deep Package C State ramp time; Slow slew rate equals to Fast divided by number, the number is 2, 4, 8 to slow down the slew rate to help minimize acoustic noise; divide by 16 is disabled
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	640	
Current Tdc Current Limit	640	
Current Voltage Limit	1600	
AC Loadline	0	AC Loadline defined in 1/100 mOhms. A value of 100 = 1.00 mOhm, and 1255 = 12.55 mOhm. Range is 0-6249 (0-62.49 mOhms). 0 = AUTO/HW default. Uses BIOS mailbox command 0x2.
DC Loadline	0	DC Loadline defined in 1/100 mOhms. A value of 100 = 1.00 mOhm, and 1255 = 12.55 mOhm. Range is 0-6249 (0-62.49 mOhms). 0 = AUTO/HW default. Uses BIOS mailbox command 0x2.
PS Current Threshold1	80	PS Current Threshold1, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO. Uses BIOS VR mailbox command 0x3.
PS Current Threshold2	20	PS Current Threshold2, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO. Uses BIOS VR mailbox command 0x3.
PS Current Threshold3	4	PS Current Threshold3, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO. Uses BIOS VR mailbox command 0x3.
PS3 Enable	Disabled, **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	0	IMON Slope defined in 1/100 increments. Range is 0-200. For a 1.25 slope, enter 125. 0 = AUTO. Uses BIOS VR mailbox command 0x4.

Feature	Options	Description
IMON Offset	0	IMON Offset defined in 1/1000 increments. Range is 0-63999. For an offset of 25.348, enter 25348. IMON Uses BIOS VR mailbox command 0x4.
IMON Prefix	+,-	Sets the offset value as positive or negative.
VR Current Limit	0	Voltage Regulator Current Limit (IccMax). This value represents the Maximum instantaneous current allowed at any given time. The value is represented in 1/4 A increments. A value of 400 = 100A. 0 means AUTO. Uses BIOS VR mailbox command 0x6.
Core VR Fast Vmode	Disabled, **Enabled**	Core VR Fast Vmode. Use to control Core Fast Vmode Enable/Disable. The value will only be effective by enabling the corresponding CEP.
Fast Vmode Itrip ICC Limit	548	Voltage Regulator Fast Vmode Itrip ICC Limit. A value of 400 = 100A. A value of 0 corresponds to feature disabled (no reactive protection). This value represents the current threshold where the VR would initiate reactive protection if Fast Vmode is enabled. The value is represented in 1/4 A increments. Uses BIOS VR mailbox command 0x25.
VR Voltage Limit	0	Voltage Limit (VMAX). This value represents the Maximum instantaneous voltage allowed at any given time. Range is 0 - 7999mV. Uses BIOS VR mailbox command 0x8.
TDC Enable	Disabled, **Enabled**	TDC Enable. 0- Disable, 1 - Enable
TDC Current Limit	0	TDC Current Limit, defined in 1/8A increments. Range 0-32767. For a TDC Current Limit of 125A, enter 1000. 0 = 0 Amps. Uses BIOS VR mailbox command 0x1A.
TDC Time Window	1 sec	VR TDC Time Window, value in seconds. 1s is default. Range from 1s to 448s.
TDC Lock	**Disabled**, Enabled	TDC Lock
IRMS	Disabled, **Enabled**	Enable/Disable IRMS – Current root mean square
GT VR Settings	Submenu	
RFI Settings	Submenu	
RFI Domain		

Feature	Options	Description
RFI Current Frequency	139.200MHz	
RFI Frequency	0	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 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 given time window.
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.
ATX Telemetry Unit	**Watts**, Percentage	ATX Telemetry Unit in Watts or Percentage.
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.
C states	**Disabled**, Enabled	Enable/Disable CPU Power Management. Allows CPU to go to C states when it's not 100% utilized.
Thermal Monitor	Disabled, **Enabled**	Enable/Disable Thermal Monitor
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

Feature	Options	Description
Energy Performance Gain	**Disabled**, Enabled	Enable/Disable Energy Performance Gain.
EPG DIMM Idd3N	**26**	
EPG DIMM Idd3P	**11**	
Power Limit 3 Settings	Submenu	
Power Limit 3 Override	**Disabled**, Enabled	Enable/Disable Power Limit 3 override. If this option is disabled, BIOS will leave the hardware default values for Power Limit 3 and Power Limit 3 Time Window.
CPU Lock Configuration	Submenu	Enable/Disable Power Limit 3 override. If this option is disabled, BIOS will leave the hardware default values for Power Limit 3 and Power Limit 3 Time Window.
CFG Lock	Disabled, **Enabled**	Configure MSR 0Xe2[15], CFG Lock bit
Overclocking Lock	Disabled, **Enabled**	Enable/Disable Overclocking Lock (BIT 20) in FLEX_RATIO (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 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 Polaity 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	Enable/Disable eDP/LVDS
LFP Panel Type	**VBIOS Default** 640x480 800x600 1024x768	Select LFP panel used by Internal Graphics Device by selecting the appropriate setup item.

	1280x1024 1400x1050 LVDS1 1400x1050 LVDS2 1600x1200 1366x768 1680x1050 1920x1200 1440x900 1600x900 1024x768 1280x800 1920x1080 2048x1536	
LVDS Backlight Mode	**EC Mode** GTT Mode	Select LVDS Backlight control function.
LVDS Backlight	Submenu	
LVDS Backlight Brightness	Value Range (0-255)	A change takes effect immediately. The value range starts by 0 and ends of 255.
DDI port 3	No Device Display Port HDMI **DisplayPort with HDMI/DVI Compatibility**	DDI port 3 function choose to DisplayPort or HDMI

7.3.4. Platform Settings

7.3.4.1. TSCC Platform Setting

Feature	Options	Description
Disable TBT PCIE Tree BME	Disabled, **Enabled**	Recommend enabling 'VT-d', 'DMA Control Guarantee' and 'Control Iommu Pre-boot Behavior' options along with this.
USBC connector manager selection	Disable **Enable UCSI 1.**2 Enable UCSI 2.0	Select UCSI or UCMC device in ACPI support based on configuration
Type C retimer TX Compliance Mode	**Disable** Enable	Default is disable Compliance Mode. Change to enabled for Type C retimer Tx Compliance Mode testing.
BIOS-TCSS handshake	Disabled **Enable**	Enable/Disable BIOS TCSS handshake messages.\nDisabled: TCSS handshake disabled \nEnabled: TCSS handshake with either EC or PMC is enabled based on the board ID
Timeout for EC USB enumeration message	Range 50 to 1000 **Default 500**	BIOS-EC handshake message USBC_GetUSBConnStatus timeout value in milli seconds
USBC and USBA Wake Capability	S3 **S4**	USBC and USBA Wake Capability
PD PS_ON mode selection	**Disable** Enable PD/PD-less PS_ON	Select TCSS PD Policy on Low Power Entry
Type C Port 1 Conv to Type	**Disable** Enable	Enable / Disable Type C Port 1 Convert to TypeA
Type C Port 2 Conv to Type	**Disable** Enable	Enable / Disable Type C Port 2 Convert to TypeA
Type C Port 3 Conv to Type	Disable **Enable**	Enable / Disable Type C Port 3 Convert to TypeA
Type C Port 4 Conv to Type	Disable **Enable**	Enable / Disable Type C Port 4 Convert to TypeA
Thunder (TM) Configuration		
USBC DataRole Swap Platform Disable Option	**TRUE** FALSE	Enable/Disable setting USBC DataRole Swap Platform Disable Option

7.3.4.1.1 Thunder (TM) Configuration

Feature	Options	Description
PCIE Tunneling over USB4	Disabled, **Enabled**	Enable or disable PCIE Tunneling over USB4
USB4 CM Mode	**Firmware CM** Software CM OS Dependent CM Debug	FW CM - The system boots with FW CM in both BIOS and OS phase.\nSW CM - The system boots with SW CM in BIOS phase all the time, then boot to OS based on OS preference for backward and forward compatible.\nOS dependent - The system will boot with SW CM in BIOS phase after saving this setting, then boot to OS based on OS preference the reflect to CM setting to next BIOS boot.\nCM debug - The system with boot without any CM in BIOS phase, then boot to OS with the CM based on OS' preference by every boot.
Integrated Thunderbolt (TM) Enable	Disable **Enable**	Enable or Disable Integrated Thunderbolt (TM).
OS Native Resource Balance	**Disabled** Enable	OS Native Resource Balance
Connect Topology Timeout value for ITBT	Range 1 to 65535 **Default 5000**	Connect Topology Timeout value for Integrated Thunderbolt (TM) Controller
Force Power on Timeout value for ITBT	Range 1 to 65535 **Default 500**	Force Power On Timeout value for Integrated Thunderbolt (TM)
ITBT RTD3	Disable **Enable**	ITBT RTD3 Enable/Disable. Note: ITBT RTD3 Disabled is not supported when SW CM is applied for OS
ITBT RTD3 EXIT DELAY	Range 0 to 20000 **Default 0**	ITBT RTD3 EXIT DELAY
PCIE RTD3 POLLING LINK ACTIVE TIMEOUT	Range 0 to 20000 **Default 0**	ADJUST LINK ACTIVE POLLING TIME DURING D3C EXIT AND DELAY IN PS0 BEFORE RETURN TO OS (milli seconds)

7.3.4.2. ACPI D3Cold settings

Feature	Options	Description
ACPI D3Cold Support	Disabled, **Enabled**	Enable/Disable ACPI D3Cold support to be executed on D3 entry and exit\n\nNote: Disable it would affect the Storage D3 setting
VR Ramp up delay	Range 0 to 100 **Default 16**	Delay between subsequent VR ramp ups if they are all Turn ON at the same time

PCIE Slot 5 Device Power-on delay in ms	Range 0 to 200 **Default 100**	Delay between applying core power and Deasserting PERST#
Audio Delay	Range 0 to 1000 **Default 200**	Delay after applying power to HD Audio (Realtek) codec device.
SensorHub	Range 0 to 1000 **Default 68**	Delay after applying power to SensorHub device.
TouchPad	Range 0 to 1000 **Default 68**	Delay after applying power to TouchPad device.
TouchPanel	Range 0 to 1000 **Default 68**	Delay in PR _ON after applying power to TouchPanel device.
P-state Capping	Disable **ENABLE**	Set _PPC and send ACPI notification
USB Port 1	High Speed Super Speed **Disable**	USB RTD3 support. Super Speed : USB3.0 devices will be exposed as RTD3 capable. High Speed: USB2.0 devices will be exposed as RTD3 capable. Disabled : USB RTD3 support disabled.\n\n For SawtoothPeak USB Port1(Below) is Superspeed and Port2(Top) is HighSpeed. Check respective board configuration to know about USB port position.
USB Port 2	High Speed Super Speed Super Speed WWAN **Disable**	USB RTD3 support. Super Speed : USB3.0 devices will be exposed as RTD3 capable. High Speed: USB2.0 devices will be exposed as RTD3 capable. Disabled : USB RTD3 support disabled.\n\n For SawtoothPeak USB Port1(Below) is Superspeed and Port2(Top) is HighSpeed. Check respective board configuration to know about USB port position.
ZPODD	**Disable** Enable	Zero Power ODD option is applicable only for the board with ZPODD support.
Sata Port 0	**Disable** Enable	Setup option to control the SATA port RTD3 functionality
Sata Port 1	**Disable** Enable	Setup option to control the SATA port RTD3 functionality
PCIe Remapped CR1	**Disable** Enable	PCIe RTD3 setup conflicts with SATA RTD3. Platform specific.
PCIe Remapped CR2	**Disable** Enable	PCIe RTD3 setup conflicts with SATA RTD3. Platform specific.
PCIe Remapped CR3	**Disable** Enable	PCIe RTD3 setup conflicts with SATA RTD3. Platform specific.

RTD3 Support for PCIE Rootports	Disable **Enable**	**Disable** Enable

7.3.5. 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 System 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	Enable/Disable LID Function
Sleep Function	Disabled, **Enabled**	Enable/Disable Sleep Button Function
ECO Mode*	**Disabled**, Enabled	Reduces the power consumption of the system, but after a shut down, you have to wait at least 5 seconds before you can restart the system.
Power-Up Mode*	**Turn On,** Remain Off, Last State	Turn On:
ATTENTION: The Power-Up Mode only has effect when the module is in ATX-Mode.		
Power Consumption	Submenu	

7.3.5.1. Power Management > Power Consumption

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

7.3.6. System Management

Feature	Options	Description
System Management	Info only	
SEMA Firmware Version	Info only	
SEMA Flags	Submenu	
SEMA Features	Info only	
Uptime & Power Cycles Counter	Read only	
System Restart Event	Read only	

Feature	Options	Description
4096 Bytes User-Flash	Read only	
Runtime Watchdog	Read only	
Temperatures	Read only	
Voltage Monitor	Read only	
Display Backlight Control	Read only	
Power-up Watchdog	Read only	
Power Monitor (Current Sense)	Read only	
Boot Counter	Read only	
Dual-BIOS	Read only	
I2C Bus 1	Read only	
I2C Bus 2	Read only	
CPU Fan	Read only	
System Fan 1	Read only	
AT/ATX Mode	Read only	
ACPI Thermal Trigger	Read only	
Power-up to Last State	Read only	
Backlight Restore	Read only	
Ext - GPIO	Read only	
I2C Bus 3	Read only	
Other BMC	Read only	
Error Log	Read only	
Wake-by-BMC	Read only	

Feature	Options	Description
Soft Fan	Read only	
Parameter Memory	Read only	
Ext-GPIO Input Interrupt Support	Read only	

7.3.6.1. System Management > SEMA Flags

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

7.3.7. Thermal Management

Feature	Options	Description
Thermal Management	Info Only	
Critical Trip Point	**Disabled** 95 C 98 C 100 C	The value is the temperature threshold of the Critical Trip Point.
Passive Cooling Trip Point	**Disabled** 100C 105C 110C	The value is the temperature threshold of the Passive Cooling Trip Point.
Active Cooling Trip Point	40 C 50 C	This value is the temperature threshold of the active cooling trip point.

Feature	Options	Description
	60 C 70 C **Refer to BMC**	
Watchdog ACPI Event Shutdown	**Disabled** Enabled	Watchdog ACPI Event Shutdown Enabled/Disabled
Temperature and Fan Speed	Submenu	

7.3.7.1. 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
CPU Fan Speed	Info Only	Display CPU Fan Speed
Smart Fan	Submenu	

7.3.7.2. Submenu: Thermal Management > Smart Fan

Feature	Options	Description
Smart Fan	Info Only	
CPU Smart FanTemperature Source	**CPU Sensor**	CPU Smart FanTemperature Source

Feature	Options	Description
	Board Sensor	
CPU Fan Mode	**AUTO (Smart Fan)** Fan Off Fan On	Select CPU Fan control mode.
Trigger Point 1	Info-only	
Trigger Temperature	40	Set the temperature value for trigger point 1 to control CPU fan.
PWM Level	30	When configured sensor reaches the trigger temperature value, set PWM level for this condition.
Trigger Point 2	Info-only	
Trigger Temperature	50	Set the temperature value for trigger point 2 to control CPU fan.
PWM Level	40	When configured sensor reaches the trigger temperature value, set PWM level for this condition.
Trigger Point 3	Info-only	
Trigger Temperature	60	Set the temperature value for trigger point 3 to control CPU fan.
PWM Level	63	When configured sensor reaches the trigger temperature value, set PWM level for this condition.
Trigger Point 4	Info-only	
Trigger Temperature	70	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.

7.3.8. Watchdog Timer

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

Feature	Options	Description
up disables the Power Up Watchdog.		
RunTime Watchdog	**Disabled** Enabled	The RunTime Watchdog resets the system after a certain amount of time after power up.

7.3.9. USB Configuration

Feature	Options	Description
USB Configuration	Info Only	
USB Module Version	Info Only	Display USB Module Version
USB Controllers:	Info Only	Display USB Controllers is XHCI or EHCI.
USB Devices:	Info Only	Display attachment USB devices.
XHCI Hand-off	**Enabled** Disabled	This is a workaround for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.
USB Mass Storage Driver Support	Disabled **Enabled**	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 100ms, for a Hub port the delay is taken form Hub descriptor.

7.3.10. AMI Graphics Output Protocol Policy

Feature	Options	Description
Intel(R) Graphics Controller		
Intel(R) GOP Driver [17.0.10xx]		
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.

7.3.11. Super IO Configuration

Feature	Options	Description
Super IO Configuration	Info only	
ITE5121 Super IO Configuration	submenu	
Nct6126dSec Super IO Configuration	submenu	

7.3.11.1. Super IO Configuration> ITE5121 Super IO Configuration

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

7.3.11.2. Super IO Configuration> Nct6126dSec Super IO Configuration

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

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

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

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

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

7.3.11.5. Super IO Configuration > Nct6126dSec Super IO Configuration > Serial Port 1 Configuration

Feature	Options	Description
Serial Port 1 Configuration	Info only	
Serial Port	Disabled **Enabled**	Enable or Disable Serial Port (COM).
Device Settings	IO=240h; IRQ=5	Fixed configuration of serial port.
Change Settings	**Auto**	Select an optimal setting for Super IO device.

Feature	Options	Description
	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	
UART Mode	**RS232** RS485 RS422	Change UART mode.

7.3.11.6. Super IO Configuration > Nct6126dSec Super IO Configuration > Serial Port 2 Configuration

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

Feature	Options	Description
	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	
UART Mode	**RS232** RS485 RS422	Change UART mode.

7.3.12. 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.

7.3.12.1. Serial Port Console > Console Redirection Settings

Feature	Options	Description
COM0	Info only	
Console Redirection Settings	Info only	
Terminal Type	VT100 VT100+ VT-UTF8	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.

Feature	Options	Description
	ANSI	
Bits per second	9600 19200 38400 57600 **115200**	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Data Bits	7 **8**	Data Bits.
Parity	**None** Even Odd Mark Space	A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the num of 1's in the data bits is even. Odd: parity bit is 0 if num of 1's in the data bits is odd. Mark: parity bit is always 1. Space: Parity bit is always 0. Mark and Space Parity do not allow for error detection..
Stop Bits	**1** 2	Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit.

7.3.13. Miscellaneous

Feature	Options	Description
Miscellaneous	Info only	
Power Supply Unit	Emulate AT Mode **ATX Mode**	Select Emulation AT or ATX function. If this option set to [Emulation AT], BIOS will report no suspend functions (S3 & S4 & S5) to ACPI OS. In windows XP, it will make OS show shutdown message during system shutdown. ATX: OS will turn off system power when shutdown.
I2C Speed Control	**100 Kbps** 400 Kbps	I2C Speed Control
SMBUS Select Configuration	From EC **FrOM PCH**	SMBUS select configuration from PCH or EC.

WOL From S5	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.
EC SATA PCIE Select Configuration	**SATA** PCIE	EC SATA PCIE Select Configuration. 0: SATA / 1: PCIE.

7.3.14. Network Stack Configuration

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

7.3.15. NVMe Configuration

Feature	Options	Description
Seg:Bus:Dev:Func	Info only	
Model Number	Info only	
Total Size	Info only	
Vendor ID	Info only	
Device ID	Info only	
Namespace	Info only	
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 Controller 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.

7.3.16. 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	Memory Configuration Parameters
Graphics Configuration	submenu	Graphics Configuration
TCSS setup menu	submenu	TCSS Configuration settings
VMD setup menu	submenu	VMD Configuration settings
VT-d setup menu	submenu	VT-d Configuration settings
Intel TXT Information	**Info-only**	Display Intel TXT information
GNA Device (B0:D8:F0)	**Enabled,** Disabled	Enable/Disable SA GNA Device.
CRID Support	Enabled**, Disabled**	Enable/Disable SA CRID and TCSS CRID control for Intel SIPP
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.
IPU Device (B0:D5:F0)	**Enabled,** Disabled	Enable/Disable SA IPU Device \nThis option will be grayed out when IPU is fused off from silicon.
NPU Device (B0:D11:F0)	Enabled**, Disabled**	Enable/Disable NPU (Neural Processing Unit) Device.
MIPI Camera Enable	Enabled**, Disabled**	MIPI Camera Configuration

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	Maximum Memory Frequency Selections in Mhz. Valid values should match the refclk, i.e. divide by 133 or 100
Max TOLUD	**Dynamic** 1 GB 1.25 GB	Maximum Value of TOLUD. Dynamic assignment would adjust TOLUD automatically based on largest MMIO length of installed graphic controller

	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	
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 Error Injection	**Disabled,** Enabled	By enabling this Error Injection feature, the user acknowledges the security risks
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

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

Feature	Options	Description
Skip Scanning 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.
Select PCIE Card	**Auto**, Elk Creek 4, PEG Eval	Select the card used on the platform
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,	Select DVMT 5.0 Pre-Allocated (Fixed) Graphics Memory size used by the Internal Graphics Device.

	20M, 24M, 28M, 32M/F7, 36M, 40M, 44M, 48M, 52M, 56M, **60M**	
DVMT Total Gfx Mem	128M, **256M**, MAX	Select DVMT5.0 Total Graphic Memory size used by the Internal Graphics Device.
Intel Graphics Pei Display Peim	**Enabled**, Disabled	Enable/Disable Pei (Early) Display

7.4.1.3. Chipset > System Agent (SA) Configuration > TCSS setup menu

Feature	Options	Description
IOM FW version	**Info-only**	
PHY FW version	**Info-only**	
TBT FW IMR Status	**Info-only**	
TBT FW version	**Info-only**	
Deepest TC state	**Info-only**	
TCSS xHCI Support	**Enabled,** Disabled	Enable/Disable TCSS xHCI
TSCC USB Configuration	submenu	SA TCSS USB Configuration settings
ITBT PCIE0 Root Port	**Enabled,** Disabled	Enable/Disable ITBT PCIE ROOT
ITBT PCIE1 Root Port	**Enabled,** Disabled	Enable/Disable ITBT PCIE ROOT
ITBT PCIE2 Root Port	Enabled**, Disabled**	Enable/Disable ITBT PCIE ROOT
ITBT PCIE3 Root Port	Enabled**, Disabled**	Enable/Disable ITBT PCIE ROOT
ITBT DMA0	Disabled**, Enabled**	Enable/Disable ITBT DMA0
ITBT DMA1	**Disabled,** Enabled	Enable/Disable ITBT DMA1
VCCST status of IOM	Disabled**, Enabled**	Enables/Disables VCCST. \nEnable: Sends VCCST ON message to EC or PMC \nDisable: Sends VCCST OFF message to EC or PMC
D3 Cold Enable/Disable	Disabled**, Enabled**	Enables/Disables D3 Cold. \nEnable: D3 cold support for IOM is enabled \nDisable: D3 cold support for IOM is Disabled
D3 Hot	Disabled**, Enabled**	Enables/Disables D3 Hot. \nEnable: D3 Hot support for IOM is enabled \nDisable: D3 Hot support for IOM is Disabled
Tc C-State Limit	Disabled**,** 1,	BIOS mailbox to limit deepest TCx state

	2, 4, 5, 6, 7, **10**,	
PCI Express Root Port 0	submenu	
PCI Express Root Port 1	submenu	PCI Express Root Port Settings.

7.4.1.3.1 Chipset > System Agent (SA) Configuration > TCSS setup menu >TCSS USB Configuration

Feature	Options	Description
USB CONNECT OVERRIDE	**Disabled** Enabled	Option will allow VCCSTTPC to turn off even when there is a connection for a USB3 port.
TCSS xDCI Support	**Disabled** Enabled	Enable/Disable TCSS xDCI
TCSS CPU USB PDO Programming	Disabled**, Enabled**	Select 'Enabled' if Port Disable Override functionality is used.
TCSS CPU USB Port Disable Override	**Disabled** Enabled	Selectively Enable/Disable the corresponding USB port from reporting a Device Connection to the controller.

7.4.1.3.2 Chipset > System Agent (SA) Configuration > TCSS setup menu > PCI Express Root Port 0

Feature	Options	Description
PTM	Disabled **Enabled**	Enable/Disable Precision Time Measurement
LTR	Disabled **Enabled**	PCIE Latency Reporting Enable/Disable
Snoop Latency Override	Disabled**, Enabled**	Snoop Latency Override for SA PCIE.\nDisabled: Disable override.\nManual: Manually enter override values.\nAuto (default): Maintain default BIOS flow.

Feature	Options	Description
Snoop Latency Valu	0 to 1023 **200**	LTR Snoop Latency value of SA PCIE
Snoop Latency Multiplier	1 ns 32 ns **1024 ns** 32678 ns 1048576 ns 33554432 ns	LTR Non Snoop Latency Multiplier of SA PCIE
Non Snoop Latency Override	Disabled**, Enabled**	Non Snoop Latency Override for SA PCIE.\nDisabled: Disable override.\nManual: Manually enter override values.\nAuto (default): Maintain default BIOS flow.
Non Snoop Latency Value	0 to 1023 **200**	LTR Non Snoop Latency value of PCH PCIE
Non Snoop Latency Multiplier	1 ns 32 ns **1024 ns** 32678 ns 1048576 ns 33554432 ns	LTR Non Snoop Latency Multiplier of SA PCIE
Force LTR Override	**Disabled,** Enabled	Force LTR Override for ITBT PCIE.\nDisabled: LTR override values will not be forced.\nEnable: LTR override values will be forced and LTR messages from the device will be ignored.
LTR Lock	**Disabled,** Enabled	PCIE LTR Configuration Lock

7.4.1.3.3 Chipset > System Agent (SA) Configuration > TCSS setup menu > PCI Express Root Port 1

Feature	Options	Description
PTM	Disabled **Enabled**	Enable/Disable Precision Time Measurement
LTR	Disabled **Enabled**	PCIE Latency Reporting Enable/Disable

Feature	Options	Description
Snoop Latency Override	Disabled**, Enabled**	Snoop Latency Override for SA PCIE.\nDisabled: Disable override.\nManual: Manually enter override values.\nAuto (default): Maintain default BIOS flow.
Snoop Latency Valu	0 to 1023 **200**	LTR Snoop Latency value of SA PCIE
Snoop Latency Multiplier	1 ns 32 ns **1024 ns** 32678 ns 1048576 ns 33554432 ns	LTR Non Snoop Latency Multiplier of SA PCIE
Non Snoop Latency Override	Disabled**, Enabled**	Non Snoop Latency Override for SA PCIE.\nDisabled: Disable override.\nManual: Manually enter override values.\nAuto (default): Maintain default BIOS flow.
Non Snoop Latency Value	0 to 1023 **200**	LTR Non Snoop Latency value of PCH PCIE
Non Snoop Latency Multiplier	1 ns 32 ns **1024 ns** 32678 ns 1048576 ns 33554432 ns	LTR Non Snoop Latency Multiplier of SA PCIE
Force LTR Override	**Disabled,** Enabled	Force LTR Override for ITBT PCIE.\nDisabled: LTR override values will not be forced.\nEnable: LTR override values will be forced and LTR messages from the device will be ignored.
LTR Lock	**Disabled,** Enabled	PCIE LTR Configuration Lock

7.4.1.4. Chipset > System Agent (SA) Configuration > VMD Setup Menu

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

7.4.1.5. Chipset > System Agent (SA) Configuration > VT-d setup menu

Feature	Options	Description
Pre-boot DMA Protection	**Disabled**, Enabled	Enable DMA Protection in Pre-boot environment (If DMAR table is installed in DXE and If VTD_INFO_PPI is installed in PEI.)
DMA Control Guarantee	Disabled, **Enabled**	Enable/Disable DMA_CONTROL_GUARANTEE bit

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	
Serial I/O Configuration	Submenu	
Thermal Throttling Control	Submenu	
PCH LAN Controller	Info-Only	No GbE Region
State After G3	S0 State **S5 State**	Specify what state to go to when power is re-applied after a power failure (G3 state)
Port 80h Redirection	**LPC Bus** PCIE Bus	Control where the Port 80h cycles are sent.
Enhance Port 80h LPC Decoding	Disabled, **Enabled**	Support the word/dword decoding of port 80h behind LPC
IOAPIC 24-119 Entries	Disabled, **Enabled**	Enables/Disables IOAPIC 24-119 Entries. IRQ24-119 may be used by PCH devices. Disabling those interrupts may cause certain devices failure.
Enable 8254 Clock Gate	Disabled, **Enabled**	Enables/Disables 8254 clock gate in early phase. Set 8254CGE is necessary for SLP_S0 support. Platform is albe to disable this policy and set 8254CGE in late phase.
Lock PCH Sideband Access	Disabled, **Enabled**	Lock PCH Sideband access, include SideBand interface lock and SideBand PortID mask for certain end point (e.g. PSFx). The option is invalid if POSTBOOT SAI is set.
Flash Protection Range Registers (FPRR)	**Disabled**, Enabled	Enable Flash Protection Range Registers

SPD Write Disable	**TRUE**, FALSE	Enable/Disable setting SPD Write Disable. For security recommendations, SPD write disable bit must be set.
LGMR	**Disabled**, Enabled	64KB memory block for LGMR (LPC Memory Range Decode)
HOST_C10 reporting to Target	**Disabled**, Enabled	This option enables HOST_C10 reporting to Target via eSPI Virtual Wire
OS IDLE Mode	Disabled, **Enabled**	Enable/Disable OS Idle Mode Feature
S0ix Auto Demotion	Disabled, **Enabled**	Enable/Disable Host Low Power Mode S0ix Auto-Demotion

7.4.2.1. Chipset > PCH-IO Configuration > PCI Express Configuration

Feature	Options	Description
Port8xh Decode	**Disabled**, Enabled	PCI Express Port8xh Decode Enable/Disable.
Compliance Test Mode	**Disabled**, Enabled	Enable when using Compliance Load Board
PCIE clocks	All port aet to **Platform-POR**	Platform-POR = clock is assigned to PCIe port or LAN according to board layout. Enabled = keep clock enabled even if unused. Disabled = Disable clock.
PCIE Ports 1-4 Configuration	**4x1 Port**, 1x2 2x1 Port, 1x2 2x1 Port Reversed, 2x2 Port, 2x2 Port Reversed, 1x4 Port, 1x4 Port Reversed	Please make sure the system boots completed after changing the configuration. Do not attempt to Shut Down Your Computer, doing that may lead to system malfunction.
PCIE Ports 5-8 Configuration	4x1 Port, 1x2 2x1 Port, 1x2 2x1 Port Reversed, 2x2 Port, 2x2 Port Reversed, **1x4 Port**, 1x4 Port Reversed	Please make sure the system boots completed after changing the configuration. Do Not Attempt to Shut Down Your Computer, doing that may lead to system malfunction.

PCI Express Root Port PXPA3	Submenu	Control the PCI Express Root Port.
PCI Express Root Port PXPA4	Submenu	Control the PCI Express Root Port.
PCI Express Root Port PXPB1	Submenu	Control the PCI Express Root Port.
PCI Express Root Port PXPC	Submenu	Control the PCI Express Root Port.
PCI Express Root Port PXPD	Submenu	Control the PCI Express Root Port.
PCI Express Root Port PXPE	Submenu	Control the PCI Express Root Port.
PCI Express Root Port PXPF	Submenu	Control the PCI Express Root Port.

7.4.2.1.1 Chipset > PCH-IO Configuration > PCI Express Configuration > PCI Express Root Port PXPA3

Feature	Options	Description
PCI Express Root Port PXPA3	Disabled, **Enabled**	Control the PCI Express Root Port.
Connection Type	Built-in, **Slot**	Built-In: a built-in device is connected to this rootport. SlotImplemented bit will be clear. Slot: this rootport connects to user-accessible slot. SlotImplemented bit will be set.
ASPM	**Disabled**, L0s, L1, L0sL1, Auto	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.
ACS	Disabled, **Enabled**	Enable/Disable Access Control Services Extended Capability
PTM	Disabled, **Enabled**	Enable/Disable Precision Time Measurement
FOM Scoreboard Control Policy	**Auto**, Gen3, Gen4, Gen3/Gen4, Gen5	Select the FOM Scoreboard Control Policy, when set to Auto, speed is based on TLS
URR	Disabled,	PCI Express Unsupported Request Reporting Enable/Disable.

	Enabled	
FER	Disabled, **Enabled**	PCI Express Device Fatal Error Reporting Enable/Disable.
NFER	Disabled, **Enabled**	PCI Express Device Non-Fatal Error Reporting Enable/Disable.
CER	Disabled, **Enabled**	PCI Express Device Correctable Error Reporting Enable/Disable.
SEFE	**Disabled**, Enabled	Root PCI Express System Error on Fatal Error Enable/Disable.
SENFE	**Disabled**, Enabled	Root PCI Express System Error on Non-Fatal Error Enable/Disable.
SECE	**Disabled**, Enabled	Root PCI Express System Error on Correctable Error Enable/Disable.
PME SCI	**Disabled**, Enabled	PCI Express PME SCI Enable/Disable.
Hot Plug	**Disabled**, Enabled	PCI Express Hot Plug Enable/Disable.
PCIe Speed	**Auto**, Gen1, Gen2, Gen3, Gen4	Configure PCIe Speed
Detect Timeout	0 to 65535 **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.
Assertion on Link Down GPIOs	Disabled, **Enabled**	GPIO Assertion on Link Down
LTR	Disabled, **Enabled**	PCH PCIE Latency Reporting Enable/Disable
Snoop Latency Override	Disabled, Manual, **Auto**	Snoop Latency Override for PCH PCIE. Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.
Non Snoop Latency Override	Disabled, Manual,	Non Snoop Latency Override for PCH PCIE. Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.

	Auto	
P2P Support	Disabled, **Enabled**	Program P2P Support Registers according to setup option
PCIe EQ override	**Disabled**, Enabled	Choose your own PCIe EQ settings, only for users who have a thorough understanding of equalization process

7.4.2.1.2 Chipset > PCH-IO Configuration > PCI Express Configuration > PCI Express Root Port PXPA4

Feature	Options	Description
PCI Express Root Port PXPA4	Disabled, **Enabled**	Control the PCI Express Root Port.
Connection Type	Built-in, **Slot**	Built-In: a built-in device is connected to this rootport. SlotImplemented bit will be clear. Slot: this rootport connects to user-accessible slot. SlotImplemented bit will be set.
ASPM	**Disabled**, L0s, L1, L0sL1, Auto	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.
ACS	Disabled, **Enabled**	Enable/Disable Access Control Services Extended Capability
PTM	Disabled, **Enabled**	Enable/Disable Precision Time Measurement
FOM Scoreboard Control Policy	**Auto**, Gen3, Gen4, Gen3/Gen4, Gen5	Select the FOM Scoreboard Control Policy, when set to Auto, speed is based on TLS
URR	Disabled, **Enabled**	PCI Express Unsupported Request Reporting Enable/Disable.
FER	Disabled, **Enabled**	PCI Express Device Fatal Error Reporting Enable/Disable.

NFER	Disabled, **Enabled**	PCI Express Device Non-Fatal Error Reporting Enable/Disable.
CER	Disabled, **Enabled**	PCI Express Device Correctable Error Reporting Enable/Disable.
SEFE	**Disabled**, Enabled	Root PCI Express System Error on Fatal Error Enable/Disable.
SENFE	**Disabled**, Enabled	Root PCI Express System Error on Non-Fatal Error Enable/Disable.
SECE	**Disabled**, Enabled	Root PCI Express System Error on Correctable Error Enable/Disable.
PME SCI	**Disabled**, Enabled	PCI Express PME SCI Enable/Disable.
Hot Plug	**Disabled**, Enabled	PCI Express Hot Plug Enable/Disable.
PCIe Speed	**Auto**, Gen1, Gen2, Gen3, Gen4	Configure PCIe Speed
Detect Timeout	0 to 65535 **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.
Assertion on Link Down GPIOs	Disabled, **Enabled**	GPIO Assertion on Link Down
LTR	Disabled, **Enabled**	PCH PCIE Latency Reporting Enable/Disable
Snoop Latency Override	Disabled, Manual, **Auto**	Snoop Latency Override for PCH PCIE. Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.
Non Snoop Latency Override	Disabled, Manual, **Auto**	Non Snoop Latency Override for PCH PCIE. Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.
P2P Support	Disabled, **Enabled**	Program P2P Support Registers according to setup option

PCIe EQ override	**Disabled**, Enabled	Choose your own PCIe EQ settings, only for users who have a thorough understanding of equalization process

7.4.2.1.3 Chipset > PCH-IO Configuration > PCI Express Configuration > PCI Express Root Port PXPB1

Feature	Options	Description
PCI Express Root Port PXPB1	Disabled, **Enabled**	Control the PCI Express Root Port.
Connection Type	Built-in, **Slot**	Built-In: a built-in device is connected to this rootport. SlotImplemented bit will be clear. Slot: this rootport connects to user-accessible slot. SlotImplemented bit will be set.
ASPM	**Disabled**, L0s, L1, L0sL1, Auto	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.
ACS	Disabled, **Enabled**	Enable/Disable Access Control Services Extended Capability
PTM	Disabled, **Enabled**	Enable/Disable Precision Time Measurement
FOM Scoreboard Control Policy	**Auto**, Gen3, Gen4, Gen3/Gen4, Gen5	Select the FOM Scoreboard Control Policy, when set to Auto, speed is based on TLS
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,	PCI Express Device Correctable Error Reporting Enable/Disable.

	Enabled	
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.
PCIe Speed	**Auto**, Gen1, Gen2, Gen3, Gen4	Configure PCIe Speed
Detect Timeout	0 to 65535 **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.
Assertion on Link Down GPIOs	Disabled, **Enabled**	GPIO Assertion on Link Down
LTR	Disabled, **Enabled**	PCH PCIE Latency Reporting Enable/Disable
Snoop Latency Override	Disabled, Manual, **Auto**	Snoop Latency Override for PCH PCIE. Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.
Non Snoop Latency Override	Disabled, Manual, **Auto**	Non Snoop Latency Override for PCH PCIE. Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.
P2P Support	Disabled, **Enabled**	Program P2P Support Registers according to setup option
PCIe EQ override	**Disabled**, Enabled	Choose your own PCIe EQ settings, only for users who have a thorough understanding of equalization process

7.4.2.1.4 Chipset > PCH-IO Configuration > PCI Express Configuration > PCI Express Root Port PXPC

Feature	Options	Description
PCI Express Root Port PXPC	Disabled, **Enabled**	Control the PCI Express Root Port.
Connection Type	Built-in, **Slot**	Built-In: a built-in device is connected to this rootport. SlotImplemented bit will be clear. Slot: this rootport connects to user-accessible slot. SlotImplemented bit will be set.
ASPM	**Disabled**, L0s, L1, L0sL1, Auto	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.
ACS	Disabled, **Enabled**	Enable/Disable Access Control Services Extended Capability
PTM	Disabled, **Enabled**	Enable/Disable Precision Time Measurement
FOM Scoreboard Control Policy	**Auto**, Gen3, Gen4, Gen3/Gen4, Gen5	Select the FOM Scoreboard Control Policy, when set to Auto, speed is based on TLS
URR	Disabled, **Enabled**	PCI Express Unsupported Request Reporting Enable/Disable.
FER	Disabled, **Enabled**	PCI Express Device Fatal Error Reporting Enable/Disable.
NFER	Disabled, **Enabled**	PCI Express Device Non-Fatal Error Reporting Enable/Disable.
CER	Disabled, **Enabled**	PCI Express Device Correctable Error Reporting Enable/Disable.
SEFE	**Disabled**, Enabled	Root PCI Express System Error on Fatal Error Enable/Disable.
SENFE	**Disabled**,	Root PCI Express System Error on Non-Fatal Error Enable/Disable.

	Enabled	
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.
PCIe Speed	**Auto**, Gen1, Gen2, Gen3, Gen4	Configure PCIe Speed
Detect Timeout	0 to 65535 **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.
Assertion on Link Down GPIOs	Disabled, **Enabled**	GPIO Assertion on Link Down
LTR	Disabled, **Enabled**	PCH PCIE Latency Reporting Enable/Disable
Snoop Latency Override	Disabled, Manual, **Auto**	Snoop Latency Override for PCH PCIE. Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.
Non Snoop Latency Override	Disabled, Manual, **Auto**	Non Snoop Latency Override for PCH PCIE. Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.
P2P Support	Disabled, **Enabled**	Program P2P Support Registers according to setup option
PCIe EQ override	**Disabled**, Enabled	Choose your own PCIe EQ settings, only for users who have a thorough understanding of equalization process

7.4.2.1.5 Chipset > PCH-IO Configuration > PCI Express Configuration > PCI Express Root Port PXPD

Feature	Options	Description
PCI Express Root Port PXPD	Disabled, **Enabled**	Control the PCI Express Root Port.
Connection Type	Built-in, **Slot**	Built-In: a built-in device is connected to this rootport. SlotImplemented bit will be clear. Slot: this rootport connects to user-accessible slot. SlotImplemented bit will be set.
ASPM	**Disabled**, L0s, L1, L0sL1, Auto	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.
ACS	Disabled, **Enabled**	Enable/Disable Access Control Services Extended Capability
PTM	Disabled, **Enabled**	Enable/Disable Precision Time Measurement
FOM Scoreboard Control Policy	**Auto**, Gen3, Gen4, Gen3/Gen4, Gen5	Select the FOM Scoreboard Control Policy, when set to Auto, speed is based on TLS
URR	Disabled, **Enabled**	PCI Express Unsupported Request Reporting Enable/Disable.
FER	Disabled, **Enabled**	PCI Express Device Fatal Error Reporting Enable/Disable.
NFER	Disabled, **Enabled**	PCI Express Device Non-Fatal Error Reporting Enable/Disable.
CER	Disabled, **Enabled**	PCI Express Device Correctable Error Reporting Enable/Disable.
SEFE	**Disabled**, Enabled	Root PCI Express System Error on Fatal Error Enable/Disable.
SENFE	**Disabled**,	Root PCI Express System Error on Non-Fatal Error Enable/Disable.

	Enabled	
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.
PCIe Speed	**Auto**, Gen1, Gen2, Gen3, Gen4	Configure PCIe Speed
Detect Timeout	0 to 65535 **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.
Assertion on Link Down GPIOs	Disabled, **Enabled**	GPIO Assertion on Link Down
LTR	Disabled, **Enabled**	PCH PCIE Latency Reporting Enable/Disable
Snoop Latency Override	Disabled, Manual, **Auto**	Snoop Latency Override for PCH PCIE. Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.
Non Snoop Latency Override	Disabled, Manual, **Auto**	Non Snoop Latency Override for PCH PCIE. Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.
P2P Support	Disabled, **Enabled**	Program P2P Support Registers according to setup option
PCIe EQ override	**Disabled**, Enabled	Choose your own PCIe EQ settings, only for users who have a thorough understanding of equalization process

7.4.2.1.6 Chipset > PCH-IO Configuration > PCI Express Configuration > PCI Express Root Port PXPE

Feature	Options	Description
PCI Express Root Port PXPA4	Disabled, **Enabled**	Control the PCI Express Root Port.
Connection Type	**Built-in**, Slot	Built-In: a built-in device is connected to this rootport. SlotImplemented bit will be clear. Slot: this rootport connects to user-accessible slot. SlotImplemented bit will be set.
ASPM	**Disabled**, L0s, L1, L0sL1, Auto	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.
ACS	Disabled, **Enabled**	Enable/Disable Access Control Services Extended Capability
PTM	Disabled, **Enabled**	Enable/Disable Precision Time Measurement
FOM Scoreboard Control Policy	**Auto**, Gen3, Gen4, Gen3/Gen4, Gen5	Select the FOM Scoreboard Control Policy, when set to Auto, speed is based on TLS
URR	Disabled, **Enabled**	PCI Express Unsupported Request Reporting Enable/Disable.
FER	Disabled, **Enabled**	PCI Express Device Fatal Error Reporting Enable/Disable.
NFER	Disabled, **Enabled**	PCI Express Device Non-Fatal Error Reporting Enable/Disable.
CER	Disabled, **Enabled**	PCI Express Device Correctable Error Reporting Enable/Disable.
SEFE	**Disabled**, Enabled	Root PCI Express System Error on Fatal Error Enable/Disable.
SENFE	**Disabled**,	Root PCI Express System Error on Non-Fatal Error Enable/Disable.

	Enabled	
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.
PCIe Speed	**Auto**, Gen1, Gen2, Gen3, Gen4	Configure PCIe Speed
Detect Timeout	0 to 65535 **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.
Assertion on Link Down GPIOs	Disabled, **Enabled**	GPIO Assertion on Link Down
LTR	Disabled, **Enabled**	PCH PCIE Latency Reporting Enable/Disable
Snoop Latency Override	Disabled, Manual, **Auto**	Snoop Latency Override for PCH PCIE. Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.
Non Snoop Latency Override	Disabled, Manual, **Auto**	Non Snoop Latency Override for PCH PCIE. Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.
P2P Support	Disabled, **Enabled**	Program P2P Support Registers according to setup option
PCIe EQ override	**Disabled**, Enabled	Choose your own PCIe EQ settings, only for users who have a thorough understanding of equalization process

7.4.2.1.7 Chipset > PCH-IO Configuration > PCI Express Configuration > PCI Express Root Port PXPF

Feature	Options	Description
PCI Express Root Port PXPF	Disabled, **Enabled**	Control the PCI Express Root Port.
Connection Type	Built-in, **Slot**	Built-In: a built-in device is connected to this rootport. SlotImplemented bit will be clear. Slot: this rootport connects to user-accessible slot. SlotImplemented bit will be set.
ASPM	**Disabled**, L0s, L1, L0sL1, Auto	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.
ACS	Disabled, **Enabled**	Enable/Disable Access Control Services Extended Capability
PTM	Disabled, **Enabled**	Enable/Disable Precision Time Measurement
FOM Scoreboard Control Policy	**Auto**, Gen3, Gen4, Gen3/Gen4, Gen5	Select the FOM Scoreboard Control Policy, when set to Auto, speed is based on TLS
URR	Disabled, **Enabled**	PCI Express Unsupported Request Reporting Enable/Disable.
FER	Disabled, **Enabled**	PCI Express Device Fatal Error Reporting Enable/Disable.
NFER	Disabled, **Enabled**	PCI Express Device Non-Fatal Error Reporting Enable/Disable.
CER	Disabled, **Enabled**	PCI Express Device Correctable Error Reporting Enable/Disable.
SEFE	**Disabled**, Enabled	Root PCI Express System Error on Fatal Error Enable/Disable.
SENFE	**Disabled**,	Root PCI Express System Error on Non-Fatal Error Enable/Disable.

	Enabled	
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.
PCIe Speed	**Auto**, Gen1, Gen2, Gen3, Gen4	Configure PCIe Speed
Detect Timeout	0 to 65535 **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.
Assertion on Link Down GPIOs	Disabled, **Enabled**	GPIO Assertion on Link Down
LTR	Disabled, **Enabled**	PCH PCIE Latency Reporting Enable/Disable
Snoop Latency Override	Disabled, Manual, **Auto**	Snoop Latency Override for PCH PCIE. Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.
Non Snoop Latency Override	Disabled, Manual, **Auto**	Non Snoop Latency Override for PCH PCIE. Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.
P2P Support	Disabled, **Enabled**	Program P2P Support Registers according to setup option
PCIe EQ override	**Disabled**, Enabled	Choose your own PCIe EQ settings, only for users who have a thorough understanding of equalization process

7.4.2.2. Chipset > PCH-IO Configuration > SATA Configuration

Feature	Options	Description
SATA Controller(s)	Disabled, **Enabled**	Enable/Disable SATA Device.
SATA Mode Selection	**AHCI**	Determines how SATA controller(s) operate.
SATA Controller Speed	Default, Gen1, **Gen2**, Gen3	Indicates the maximum speed the SATA controller can support.
SATA Test Mode	**Disabled**, Enabled	Test Mode Enable/Disable (Loop Back).
Aggressive LPM Support	Disabled, **Enabled**	Enable PCH to aggressively enter link power state.
Port 0	Disabled, **Enabled**	Enable or Disable SATA Port
Hot Plug	**Disabled**, Enabled	Designates this port as Hot Pluggable.
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**, ISATA, Direct Connect, Flex, M2	Identify the SATA Topology if it is Default or ISATA or Flex or DirectConnect or M2
SATA Port 0 DevSlp	**Disabled**, Enabled	Enable/Disable SATA Port 0 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

Port 1	Disabled, **Enabled**	Enable or Disable SATA Port
Hot Plug	**Disabled**, Enabled	Designates this port as Hot Pluggable.
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**, ISATA, Direct Connect, Flex, M2	Identify the SATA Topology if it is Default or ISATA or Flex or DirectConnect or M2
SATA Port 0 DevSlp	**Disabled**, Enabled	Enable/Disable SATA Port 0 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

7.4.2.3. Chipset > PCH-IO Configuration > USB Configuration

Feature	Options	Description
xDCI Support	**Disabled**, Enabled	Enable/Disable xDCI (USB OTG Device)
USB PDO Programming	Disabled, **Enabled**	Select 'Enabled' if Port Disable Override functionality is used.
USB Overcurrent	Disabled, **Enabled**	Select 'Disabled' for pin-based debug. If pin-based debug is enabled but USB overcurrent is not disabled, USB DbC does not work.
USB Overcurrent Lock	Disabled, **Enabled**	Select 'Enabled' if Overcurrent functionality is used. Enabling this will make xHCI controller consume the Overcurrent mapping data
USB Audio Offload	Disabled,	Enable/Disable USB Audio Offload functionality

	Enabled	
Enable HSII on xHCI	Disabled, **Enabled**	Enable/Disable HSII feature. It may lead to increased power consumption.
USB3.1 Port 0 Speed Selection	**Gen2,** Gen1	USB3.1 Speed selection; Gen1 or Gen2
USB3.1 Port 1 Speed Selection	**Gen2,** Gen1	USB3.1 Speed selection; Gen1 or Gen2
USB Port Disable Override	**Disabled**, Enabled	Selectively Enable/Disable the corresponding USB port from reporting a Device Connection to the controller.
USB SW Device Mode Port #0	**Disabled**, Enabled	Enable Connector Event for device subscription.
USB SW Device Mode Port #1	**Disabled**, Enabled	Enable Connector Event for device subscription.
USB SW Device Mode Port #2	**Disabled**, Enabled	Enable Connector Event for device subscription.
USB SW Device Mode Port #3	**Disabled**, Enabled	Enable Connector Event for device subscription.
USB SW Device Mode Port #4	**Disabled**, Enabled	Enable Connector Event for device subscription.
USB SW Device Mode Port #5	**Disabled**, Enabled	Enable Connector Event for device subscription.
USB SW Device Mode Port #6	**Disabled**, Enabled	Enable Connector Event for device subscription.
USB SW Device Mode Port #7	**Disabled**, Enabled	Enable Connector Event for device subscription.
USB SW Device Mode Port #8	**Disabled**, Enabled	Enable Connector Event for device subscription.
USB SW Device Mode Port #9	**Disabled**, Enabled	Enable Connector Event for device subscription.

7.4.2.4. Chipset > PCH-IO Configuration > Security Configuration

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

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

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

7.4.2.6. Chipset > PCH-IO Configuration > Serial IO Configuration

Feature	Options	Description
I2C0 Controller	Disabled, **Enabled**	Enables/Disables Serial I/O Controller If given device is Function 0 PSF disabling is skipped. PSF default will remain and device PCI CFG Space will still be visible. This is needed to allow PCI enumerator access functions above 0 in a multifunction device. The following devices depend on each other:I2C0 and I2C1,2,3UART0 and UART1,SPI0,1UART2 and I2C4,5 UART 0 (00:30:00) cannot be disabled when:1. Child device is enabled like CNVi Bluetooth (_SB.PC00.UA00.BTH0) UART 0 (00:30:00) cannot be enabled when:1. I2S Audio codec is enabled (_SB.PC00.I2C0.HDAC)
I2C1 Controller	Disabled, **Enabled**	Enables/Disables Serial I/O Controller If given device is Function 0 PSF disabling is skipped. PSF default will remain and device PCI CFG Space will still be visible. This is needed to allow PCI enumerator access functions above 0 in a multifunction device. The following devices depend on each other:I2C0 and I2C1,2,3UART0 and UART1,SPI0,1UART2 and I2C4,5 UART 0 (00:30:00) cannot be disabled when:1. Child device is enabled like CNVi Bluetooth (_SB.PC00.UA00.BTH0) UART 0 (00:30:00) cannot be enabled when:1. I2S Audio codec is enabled (_SB.PC00.I2C0.HDAC)
I2C3 Controller	Disabled, **Enabled**	I3C cannot be enabled if I2C#3 is enabled due to an ITSS requirement that there are at most 4 unique IRQs per Device, whereas D21 has 5 functions
I2C4 Controller	**Disabled**,	Enables/Disables Serial I/O Controller For I2C5 and UART2 to work this device has to be enabled

	Enabled	
I2C5 Controller	Disabled, **Enabled**	Enables/Disables Serial I/O Controller For this device to work I2C4 has to be enabled
SPI0 Controller	**Disabled**, Enabled	Enables/Disables Serial I/O Controller If given device is Function 0 PSF disabling is skipped. PSF default will remain and device PCI CFG Space will still be visible. This is needed to allow PCI enumerator access functions above 0 in a multifunction device. The following devices depend on each other: I2C0 and I2C1,2,3UART0 and UART1, SPI0,1UART2 and I2C4,5 UART 0 (00:30:00) cannot be disabled when:1. Child device is enabled like CNVi Bluetooth (_SB.PC00.UA00.BTH0) UART 0 (00:30:00) cannot be enabled when:1. I2S Audio codec is enabled (_SB.PC00.I2C0.HDAC)
SPI1 Controller	**Disabled**, Enabled	Enables/Disables Serial I/O Controller If given device is Function 0 PSF disabling is skipped. PSF default will remain and device PCI CFG Space will still be visible. This is needed to allow PCI enumerator access functions above 0 in a multifunction device. The following devices depend on each other: I2C0 and I2C1,2,3UART0 and UART1, SPI0,1UART2 and I2C4,5 UART 0 (00:30:00) cannot be disabled when:1. Child device is enabled like CNVi Bluetooth (_SB.PC00.UA00.BTH0) UART 0 (00:30:00) cannot be enabled when:1. I2S Audio codec is enabled (_SB.PC00.I2C0.HDAC)
SPI2 Controller	**Disabled**, Enabled	Enables/Disables Serial I/O Controller If given device is Function 0 PSF disabling is skipped. PSF default will remain and device PCI CFG Space will still be visible. This is needed to allow PCI enumerator access functions above 0 in a multifunction device. The following devices depend on each other: I2C0 and I2C1,2,3UART0 and UART1, SPI0,1UART2 and I2C4,5 UART 0 (00:30:00) cannot be disabled when:1. Child device is enabled like CNVi Bluetooth (_SB.PC00.UA00.BTH0) UART 0 (00:30:00) cannot be enabled when:1. I2S Audio codec is enabled (_SB.PC00.I2C0.HDAC)
UART0 Controller	Disabled, **Enabled**	Set UART0 mode - DBG used for BIOS log print and/or Kernel OS Debug - COM - 16550 compatible serial port with Power Gating support
UART1 Controller	Disabled, **Enabled**	Enables/Disables Serial I/O Controller If given device is Function 0 PSF disabling is skipped. PSF default will remain and device PCI CFG Space will still be visible. This is needed to allow PCI enumerator access functions above 0 in a multifunction device. The following devices depend on each other: I2C0 and I2C1,2,3UART0 and UART1, SPI0,1UART2 and I2C4,5 UART 0 (00:30:00) cannot be disabled when:1. Child device is enabled like CNVi Bluetooth (_SB.PC00.UA00.BTH0) UART 0 (00:30:00) cannot be enabled when:1. I2S Audio codec is enabled (_SB.PC00.I2C0.HDAC)
UART2 Controller	Disabled, **Enabled**	Enables/Disables Serial I/O Controller If given device is Function 0 PSF disabling is skipped. PSF default will remain and device PCI CFG Space will still be visible. This is needed to allow PCI enumerator access functions above 0 in a multifunction device. The following devices depend on each other: I2C0 and I2C1,2,3UART0 and UART1, SPI0,1UART2 and I2C4,5 UART 0 (00:30:00) cannot be disabled when:1. Child device is enabled like CNVi Bluetooth (_SB.PC00.UA00.BTH0) UART 0 (00:30:00) cannot be enabled when:1. I2S Audio codec is enabled (_SB.PC00.I2C0.HDAC)
GPIO IRQ Route	**IRQ 14** IRQ 15	Route all GPIOs to one of the IRQ.

WITT/MITT I2C Test Device	**Disabled**, Enabled	Enable/Disable I2C WITT Test Device
WITT/MITT I3C Test Device	**Disabled**, Enabled	Enable/Disable I3C WITT Test Device
WITT/MITT SPI Test Device	**Disabled**, Enabled	Enable/Disable SPI WITT Test Device
UART Test Device	**Disabled**, Enabled	Choose if UART Test Device is used and with which controller
Additional Serial IO devices	**Disabled**, Enabled	When enabled, ACPI will report additional devices connected to Serial IO.
SerialIO timing parameters	**Disabled**, Enabled	Enables additional timing parameters for all Serial IO controllers. Defaults can be changed in each controller setting. Platform restart required to apply changes

7.4.2.7. Chipset > PCH-IO Configuration > Thermal Throttling Control

Feature	Options	Description
SOC Thermal Throttling Level	**Suggested Setting**, Manual	Determine if use Intel suggested setting
IOE Thermal Throttling Level	**Suggested Setting**, Manual	Determine if use Intel suggested setting
SATA Thermal Setting	**Suggested Setting**, Manual	Determine if use Intel suggested setting

7.5. Security

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

7.5.1. Secure Boot Menu

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

7.6. Boot

7.6.1. Boot Configuration

Feature	Options	Description
Boot Configuration	Info only	
Setup Prompt Timeout	**1**	Number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite waiting.
Bootup NumLock State	**On** Off	Select the keyboard NumLock state
Quiet Boot	Disabled **Enabled**	Enables or disables Quiet Boot option
Fast Boot	Disabled **Enabled**	Enables or disables boot with initialization of a minimal set of devices required to launch active boot option. Has no effect for BBS boot option.
SATA Support	**Last Boot SATA Devices Only** All Sata Devices	If Last Boot SATA Devices Only, Only last boot SATA device will be available in Post. If All SATA Devices, all SATA devices will be available in OS and Post.
NVME Support	Disabled **Enabled**	If disabled, NVMe device will be skipped.
VGA Support	Auto **EFI Driver**	If Auto, only install Legacy OpRom with Legacy OS and logo would NOT be shown during post. EFI driver will still be installed with EFI OS.
USB Support	Disabled **Full Initial** Partial Initial	If disabled, all USB devices will NOT be available until after OS boot. If Partial Initial, USB Mass Storage and specific USB port/device will NOT be available before OS boot. If enabled, all USB devices will be available in OS and Post.
PS2 Devices Support	Disabled **Enabled**	If disabled, PS2 devices will be skipped.
NetWork Stack Driver Support	**Disabled** Enabled	If Disabled, NetWork Stack Driver will be skipped.

Feature	Options	Description
Redirection Support	Disabled **Enabled**	If disable, Redirection function will be disabled.

7.7. Save & Exit

7.7.1. Save Options

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

7.7.2. Default Options

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

8. BIOS Checkpoints, Beep Codes

This section of the document 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 bootblock and Power-On Self Test (POST) to indicate the tasks 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 are 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 POST 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 "bootblock" functionality of legacy BIOS
[2]Analogous to "POST" functionality in legacy BIOS

8.1. Status Code Ranges

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

8.2. Standard Status Codes

8.2.1. SEC Phase

Status Code	Description
0x00	Not used
Progress Codes	
0x01	Power on. Reset type detection (soft/hard).
0x02	AP initialization before microcode loading
0x03	North Bridge initialization before microcode loading
0x04	South Bridge initialization before microcode loading
0x05	OEM initialization before microcode loading
0x06	Microcode loading
0x07	AP initialization after microcode loading
0x08	North Bridge initialization after microcode loading
0x09	South Bridge initialization after microcode loading
0x0A	OEM initialization after microcode loading
0x0B	Cache initialization

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

8.2.2. SEC Beep Codes

None

8.2.3. PEI Phase

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

Status Code	Description
0x34	CPU post-memory initialization. Application Processor(s) (AP) initialization
0x35	CPU post-memory initialization. Boot Strap Processor (BSP) selection
0x36	CPU post-memory initialization. System Management Mode (SMM) initialization
0x37	Post-Memory North Bridge initialization is started
0x38 – 0x3A	Reserved for North Bridge initialization
0x3B	Post-Memory South Bridge initialization is started
0x3C -0x3E	Reserved for South Bridge
0x3F-0x4E	OEM post memory initialization codes
0x4F	DXE IPL is started
PEI Error Codes	
0x50	Memory initialization error. Invalid memory type or incompatible memory speed
0x51	Memory initialization error. SPD reading has failed
0x52	Memory initialization error. Invalid memory size or memory modules do not match.
0x53	Memory initialization error. No usable memory detected
0x54	Unspecified memory initialization error.
0x55	Memory not installed
0x56	Invalid CPU type or Speed
0x57	CPU mismatch
0x58	CPU self test failed or possible CPU cache error
0x59	CPU micro-code is not found or micro-code update is failed
0x5A	Internal CPU error

Status Code	Description
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 – 0x67	Reserved for CPU DXE initialization (CPU module specific)
0x68	PCI host bridge initialization
0x69	North Bridge DXE initialization is started
0x6A	North Bridge DXE SMM initialization is started
0x6B – 0x6F	Reserved for North Bridge DXE initialization (North Bridge module specific)

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

Status Code	Description
0x9E – 0x9F	Reserved for future AMI codes
0xA0	IDE initialization is started
0xA1	IDE Reset
0xA2	IDE Detect
0xA3	IDE Enable
0xA4	SCSI initialization is started
0xA5	SCSI Reset
0xA6	SCSI Detect
0xA7	SCSI Enable
0xA8	Setup Verifying Password
0xA9	Start of Setup
0xAA	Reserved for ASL (see ASL Status Codes section below)
0xAB	Setup Input Wait
0xAC	Reserved for ASL (see ASL Status Codes section below)
0xAD	Ready To Boot event
0xAE	Legacy Boot event
0xAF	Exit Boot Services event
0xB0	Runtime Set Virtual Address MAP Begin
0xB1	Runtime Set Virtual Address MAP End
0xB2	Legacy Option ROM Initialization
0xB3	System Reset
0xB4	USB hot plug

Status Code	Description
0xB5	PCI bus hot plug
0xB6	Clean-up of NVRAM
0xB7	Configuration Reset (reset of NVRAM settings)
0xB8 – 0xBF	Reserved for future AMI codes
0xC0 – 0xCF	OEM BDS initialization codes
DXE Error Codes	
0xD0	CPU initialization error
0xD1	North Bridge initialization error
0xD2	South Bridge initialization error
0xD3	Some of the Architectural Protocols are not available
0xD4	PCI resource allocation error. Out of Resources
0xD5	No Space for Legacy Option ROM
0xD6	No Console Output Devices are found
0xD7	No Console Input Devices are found
0xD8	Invalid password
0xD9	Error loading Boot Option (LoadImage returned error)
0xDA	Boot Option is failed (StartImage returned error)
0xDB	Flash update is failed
0xDC	Reset protocol is not available

8.2.6. DXE Beep Codes

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

8.2.7. ACPI/ASL Checkpoint

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

Status Code	Description
0xAA	System has transitioned into ACPI mode. Interrupt controller is in APIC mode.

8.3. OEM-Reserved Checkpoint Ranges

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

9. Software Support

9.1. Windows

Windows 10 IoT Enterprise 2021 LTSC

Windows 11 IoT Enterprise 2024 LTSC (2H' 24)

9.2. Ubuntu 24.04. LTS

Kernel version

9.3. Yocto Linux 64-bit

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

9.4. SEMA API

10. Mechanical and Thermal

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

10.1. Module Dimensions

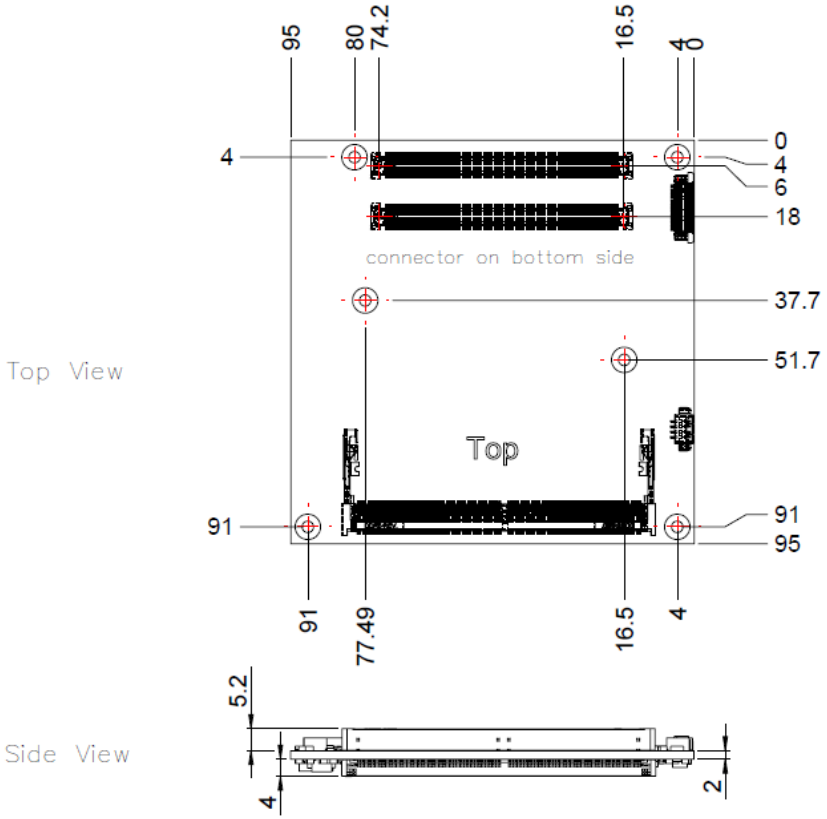
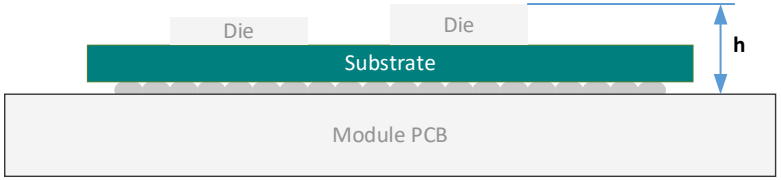


Figure 5 – Module mechanical dimensions

10.2. Height of Processor and Static Compressive Load

Processor Height Tolerance

The tolerance of the processor height is one of the key factors to consider when designing your thermal solution, as illustrated below. Please contact our ADLINK representative for further details.



	Typical	Tolerance
h	1.25 mm	+/- 0.1mm

Static Compressive Load

Another key factor to consider is the static compressive load. The cExpress-MTL module exhibits a processor maximum pressure die of 40 lbf.

10.3. Thermal Solutions

10.3.1. Heatspreader: HTS

Dimensions: mm

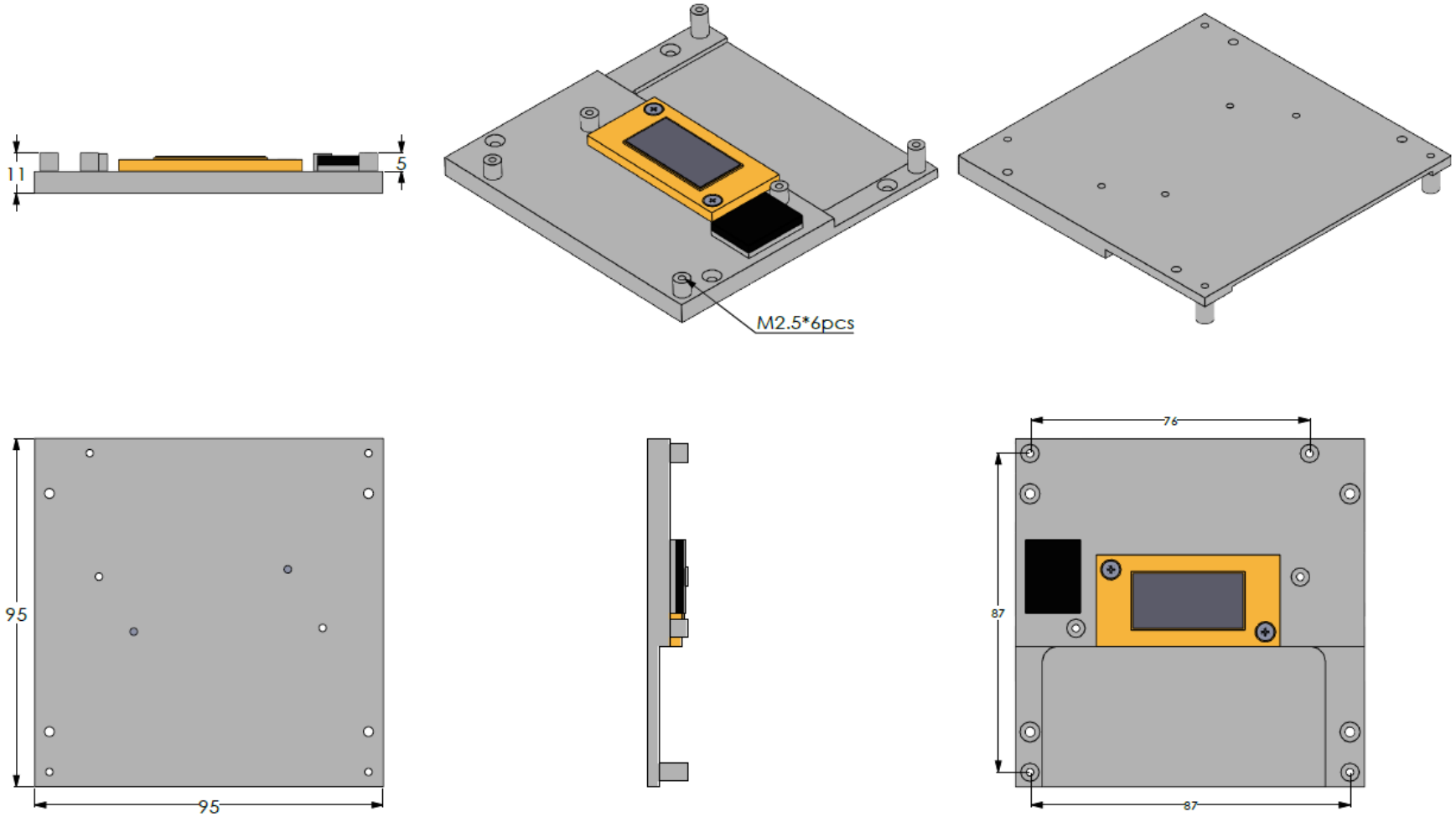


Figure 6 – Heatspreader: HTS

10.3.2. Heatsink: THS

Dimensions: mm

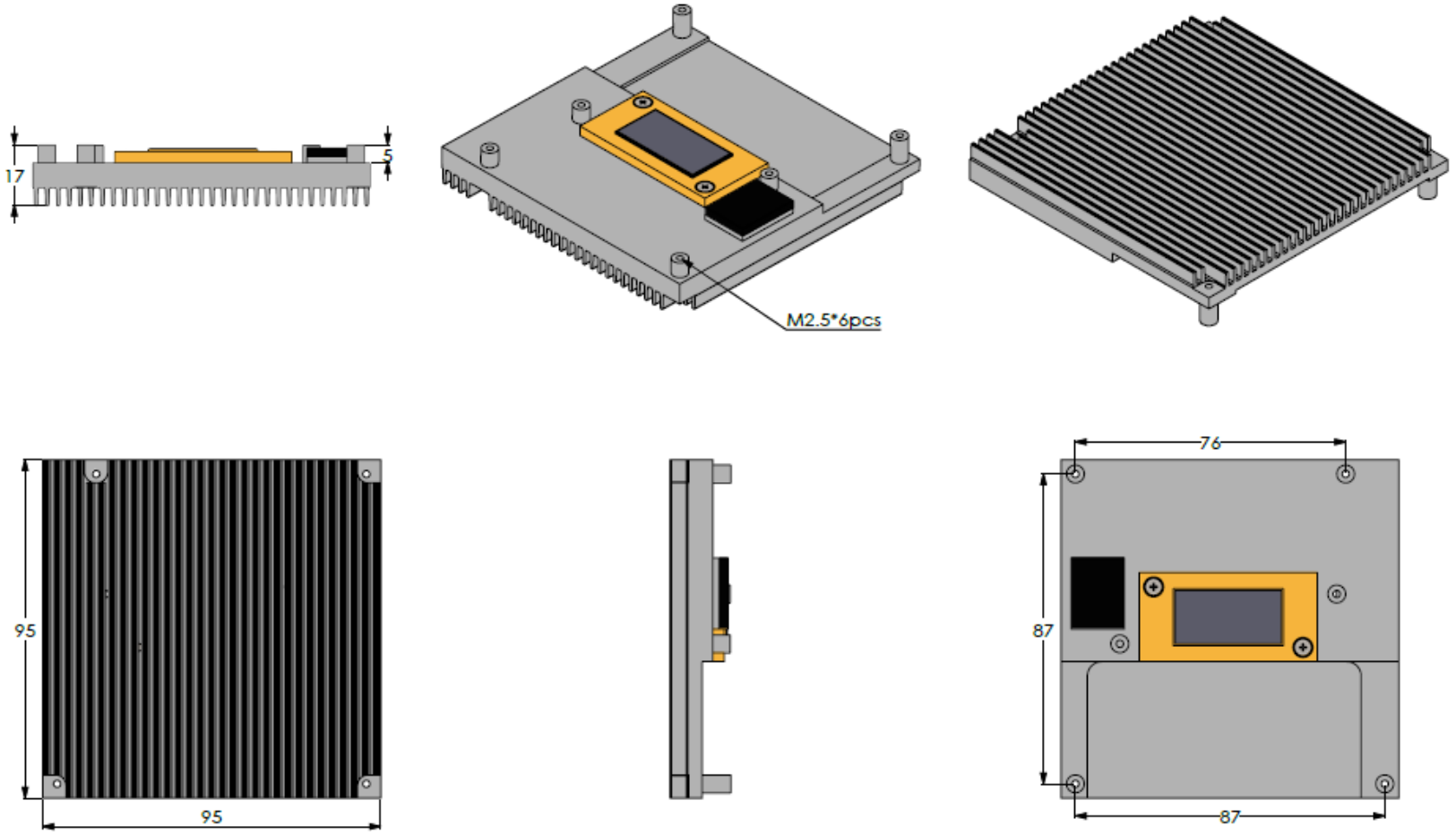


Figure 7 – Heatsink: THS

Dimensions: mm

10.3.3. Heatsink with Fan: THSF

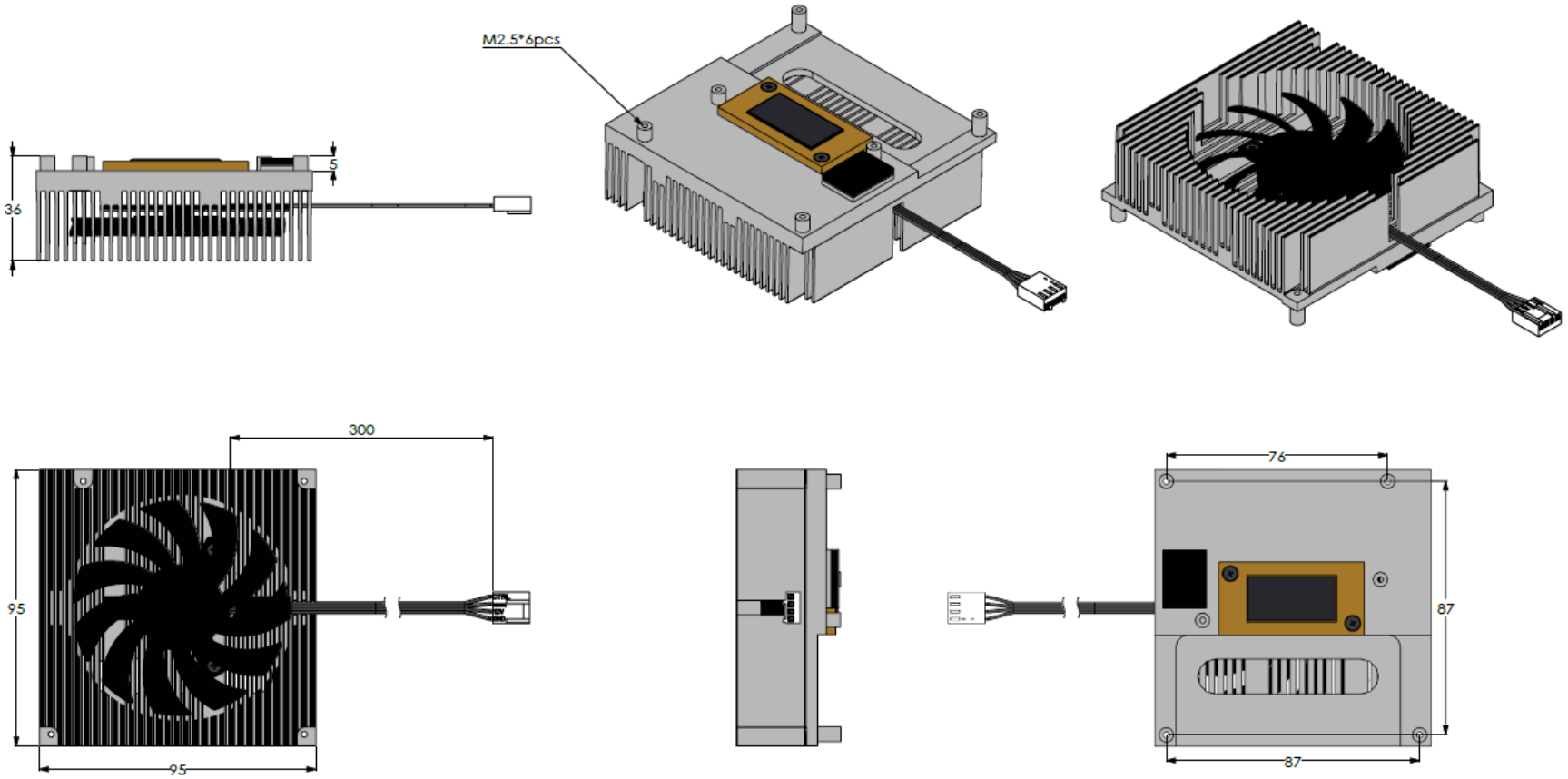


Figure 8 – Heatsink with fan: THSF

10.3.4. Heatsink High Profile: THSH

Dimensions: mm

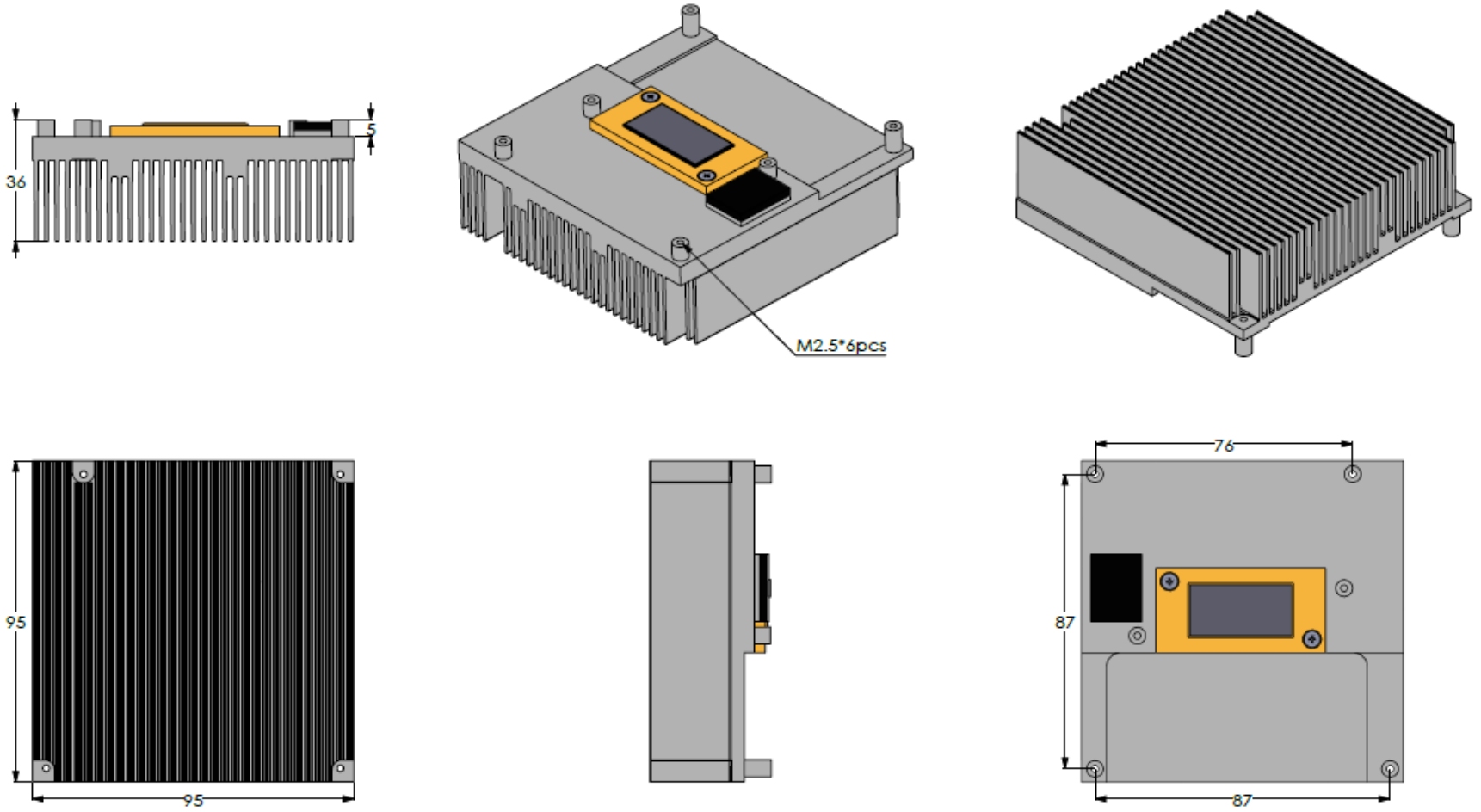


Figure 9 – Heatsink high profile: THSH

10.4. Board to Board Connectors

To accommodate different stacking heights, the receptacles for COM Express carrier boards are available in two heights: 5 mm and 8 mm. When using 5-mm receptacles, the carrier board should be free of components.

Tyco 3-1827253-6, Tyco 2357787-1

ept 401-51101-51, ept 401-51103-51

Foxconn QT002206-2141-3H, Foxconn QT5GB26-44703-3H

- 220-pin board-to-board connector with 0.5mm for a stacking height of **5 mm**.
- This connector can be used with 5-mm through-hole standoffs (SMT type).

Tyco 3-6318491-6, Tyco 2357798-1

ept 401-55101-51, ept 401-55103-51

Foxconn QT002206-4141-3H, Foxconn QT5GB26-74703-3H

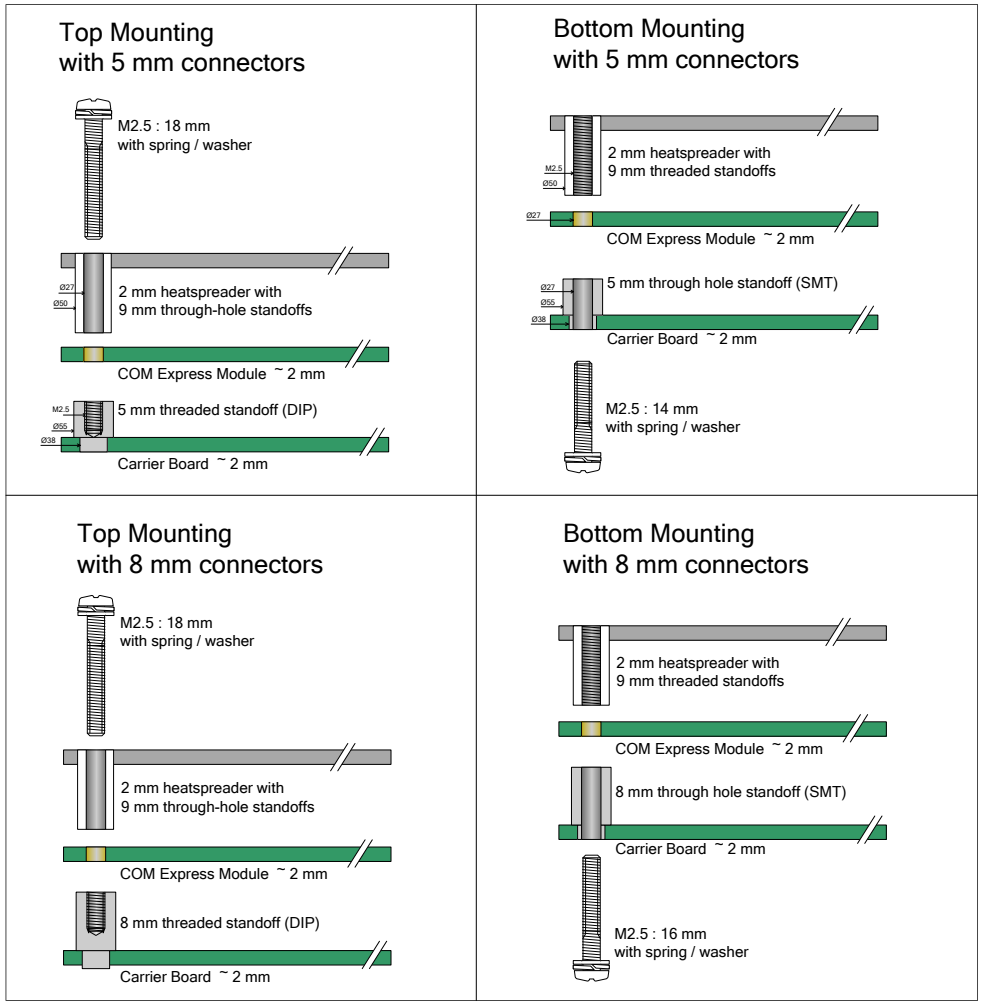
- 220-pin board-to-board connector with 0.5mm for a stacking height of **8 mm**.
- This connector can be used with 8-mm through-hole standoffs (SMT type).

Common Specifications

Current capacity: 0.5A per pin	UL certification (ECBT2.E28476)
Rated voltage: 50V AC	Copper alloy (contacts)
Insulation resistance: 100M or greater @ 500 VDC	Housing: thermo-plastic molded compound (L.C.P.)
Temperature rating: -40°C to 85°C	

10.5. Mounting Method

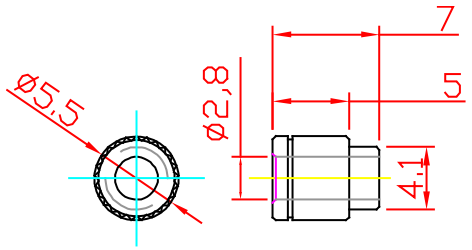
There are several standard ways to mount the COM Express module with a thermal solution onto a carrier board. In addition to the 5-mm or 8-mm board-to-board connectors, there are also top and bottom mounting. In top mounting, the threaded standoffs are on the carrier board, and the thermal solution is attached with through-hole standoffs. In bottom mounting, the threaded standoffs are on the thermal solution, and the carrier board has through-hole standoffs.



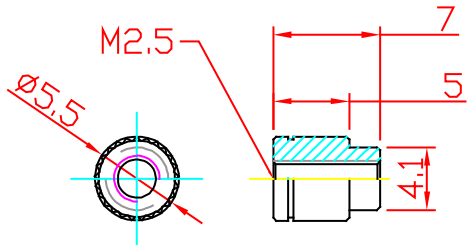
10.6. Standoff Types

The standoffs available for top and bottom mounting methods are shown below. Note that threaded standoffs are DIP type and through-hole standoffs are SMT type. Other types not listed are available upon request.

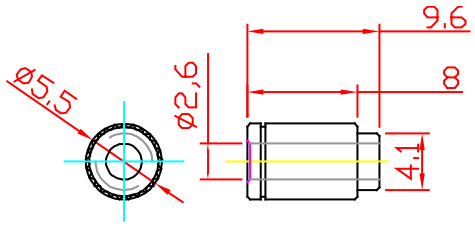
5mm through-hole standoff (SMT type)
P/N: 33-72000-0050



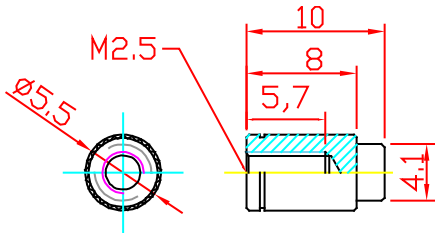
5mm threaded standoff (DIP type)
P/N: 33-72016-0050



8mm through-hole standoff (SMT type)
P/N: 33-72000-0080



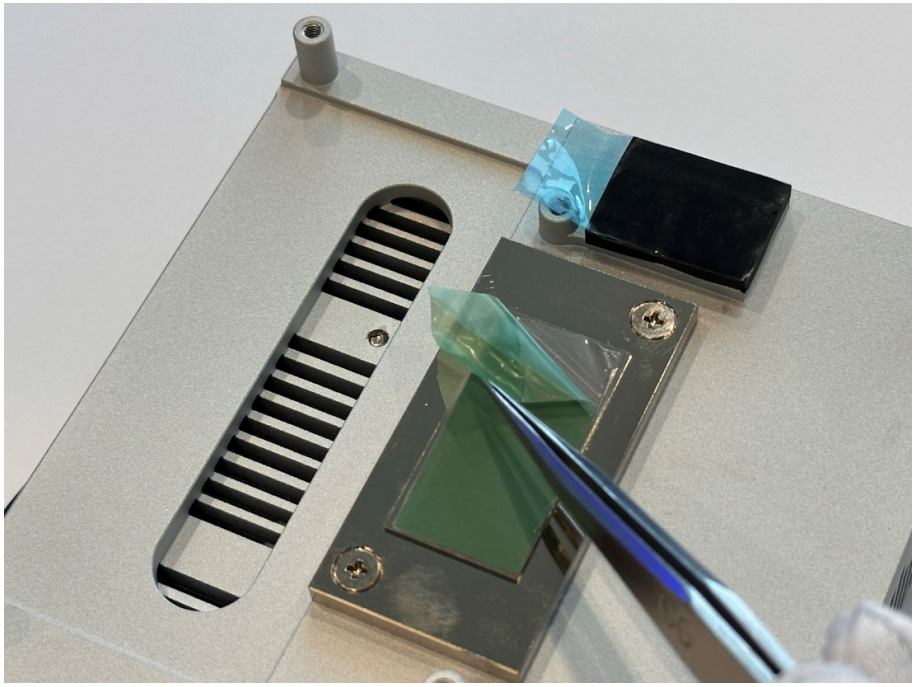
8mm threaded standoff (DIP type)
P/N: 33-72015-0050



10.7. Installation

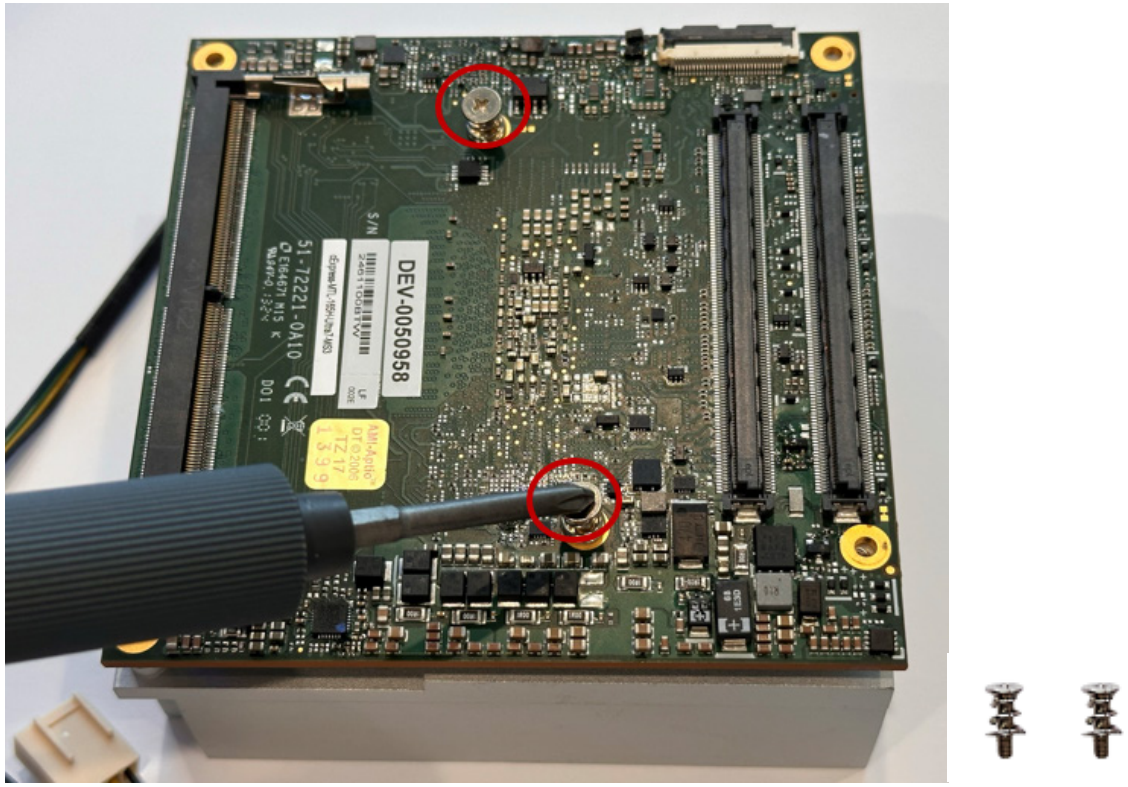
Install a heatspreader or heatsink using the following instructions. The images below are for illustration purposes only.

Step 1: Remove the protective membranes from the thermal pads.

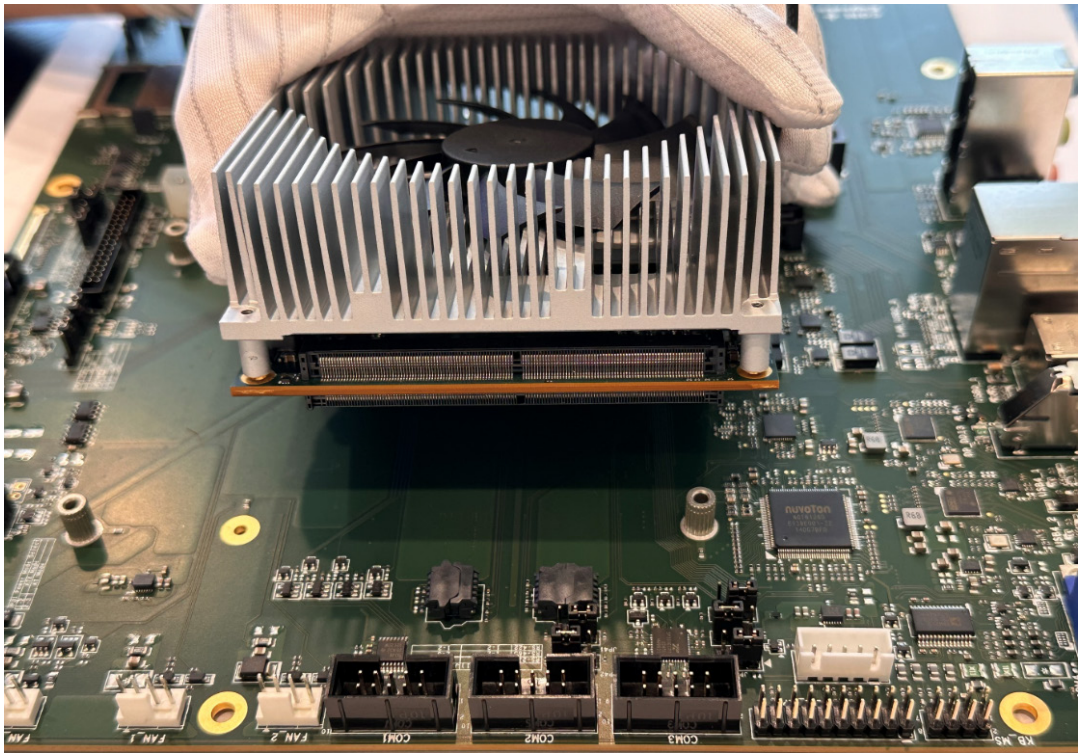


Note: All thermal pads have a protective membrane, depending on the module.

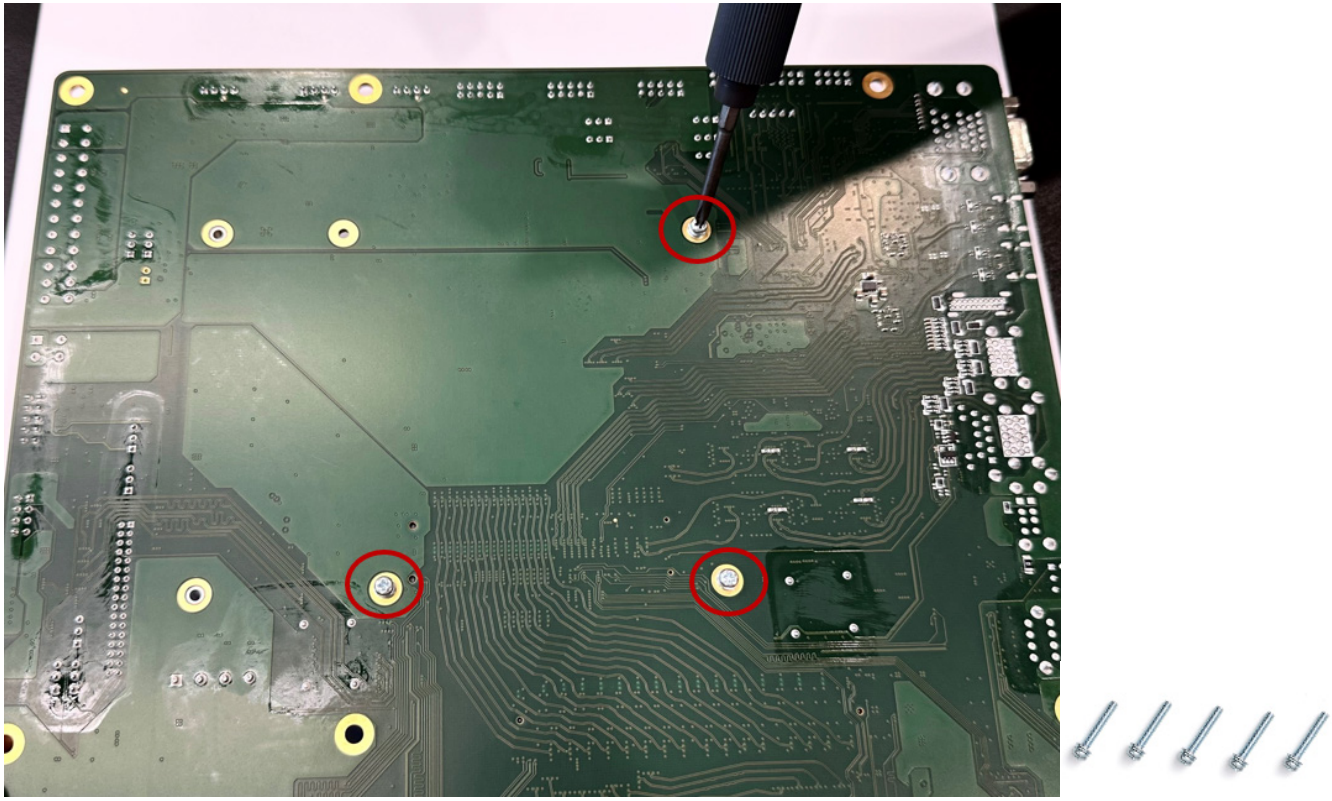
Step 2: Assemble the heatsink onto the COM Express module. Use the 3x M2.5, L=6mm screws provided to fasten the heatsink to the module. The number of screw holes and screws may vary by module.



Step 3: Place the COM Express module and heatsink assembly onto the connectors on the carrier board as shown below. Press down on the module until the module is securely seated on the carrier board.



Step 4: Use the 5x M2.5 (L=16mm) screws provided to secure the COM Express module to the carrier board from the solder side. The number of screw holes and screws are module and carrier board design dependent.



Step 5: If you are installing a heatsink with a fan, plug the fan connector into the carrier board.
The location of the FAN connector for the COM Express module depends on carrier board design.