

cExpress-TL

User's Guide

intel



COM  **Express®**

Revision: Rev. 1.1
Date: 2023-08-31
Part Number: 50M-72218-1010

 **ADLINK**
LEADING EDGE COMPUTING

Revision History

Revision	Description	Date	Author
1.0	Initial release	2021-08-23	JC
1.1	BIOS tables added	2023-08-31	CC

Preface

Disclaimer

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

Environmental Responsibility

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



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

Trademarks

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

Copyright © 2023 ADLINK Technology Incorporated

This document contains proprietary information protected by copyright. All rights are reserved. No part of this manual may be reproduced by any mechanical, electronic, or other means in any form without prior written permission of the manufacturer.

Safety Instructions

For user safety, please read and follow all Instructions, **WARNINGS**, **CAUTIONS**, and **NOTES** marked in this manual and on the associated equipment before handling/operating the equipment.

Read these safety instructions carefully.

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

Conventions

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



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



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



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

Getting Service

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

ADLINK Technology, Inc.

No. 66, Huaya 1st Rd., Guishan District, Taoyuan City 333411, Taiwan

Tel: +886-3-216-5088

Fax: +886-3-328-5706

Email: service@adlinktech.com

Ampro ADLINK Technology, Inc.

6450 Via Del Oro, San Jose, CA 95119-1208, USA

Tel: +1-408-360-0200

Toll Free: +1-800-966-5200 (USA only)

Fax: +1-408-600-1189

Email: info@adlinktech.com

ADLINK Technology (China) Co., Ltd.

300 Fang Chun Rd., Zhangjiang Hi-Tech Park, Pudong New Area, Shanghai, 201203, China

Tel: +86-21-5132-8988

Fax: +86-21-5132-3588

Email: market@adlinktech.com

ADLINK Technology GmbH

Hans-Thoma-Strasse 11, D-68163 Mannheim, Germany

Tel: +49-621-43214-0

Fax: +49-621 43214-30

Email: emea@adlinktech.com

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

Table of Contents

Revision History	2
Preface	3
List of Figures	11
1. Introduction	12
2. Specifications	13
2.1. Core System	13
2.2. Video	14
2.2.1. Display Interface Support	15
2.3. Audio	15
2.4. Expansion Busses	15
2.5. Ethernet	16
2.6. Multi I/O and Storage	16
2.7. Trusted Platform Module (TPM)	17
2.8. SEMA Board controller	17
2.9. Debug	17
2.10. Power	18
2.11. Mechanical and Environmental	18
3. Block Diagram	20
4. Pinout and Signal Descriptions	21
4.1. Pin Summary	21
4.2. Signal Terminology Descriptions	26
4.3. AB Connector Signal Descriptions	27
4.3.1. Audio	27
4.3.2. Analog VGA	28
4.3.3. LVDS or eDP	29
4.3.4. Gigabit Ethernet	32
4.3.5. SATA	33
4.3.6. PCI Express	34
4.3.7. LPC Bus	36
4.3.8. USB	37
4.3.9. SPI Bus (BIOS only)	38

4.3.10.	Miscellaneous.....	39
4.3.11.	SMBus	40
4.3.12.	I2C Bus	40
4.3.13.	General Purpose I/O (GPIO)	41
4.3.14.	Serial Interface Signals.....	41
4.3.15.	Power and System Management	42
4.3.16.	Power and Ground	43
4.4.	CD Connector Signal Descriptions	44
4.4.1.	USB 3.0 Extensions	44
4.4.2.	PCI Express	45
4.4.3.	DDI1 Port	46
4.4.4.	DDI2 Port	49
4.4.5.	DDI3 Port	52
4.4.6.	PCIe Graphics Port (PEG).....	55
4.4.7.	Module Type Definition.....	56
4.4.8.	Power and Ground	57
5.	Additional Features	58
5.1.	Debug Connector	59
5.2.	Status LEDs.....	60
5.3.	Exception Codes	61
5.4.	Fan Connector.....	62
5.5.	BIOS Default Reset Button.....	63
5.6.	BIOS Boot Select	64
6.	System Resources	65
6.1.	System Memory Map	65
6.2.	I/O Range Map	65
6.3.	Interrupt Request (IRQ) Lines	67
6.4.	PCI Configuration Space Map	68
6.5.	PCI Interrupt Routing Map	69
6.6.	SMBus Address Table	70
7.	BIOS Configurations	71
7.1.	Menu Structure.....	71
7.1.1.	Main > BIOS Information.....	72
7.1.2.	Main > System Information	72
7.1.3.	Main > Board Information.....	73
7.1.4.	Main > System Date/Time.....	74
7.2.	Advanced	75

7.2.1.	Advanced > CPU Configuration	75
7.2.2.	Advanced > Power & Performance	76
7.2.3.	Advanced > TCSS Platform Settings.....	88
7.2.4.	Advanced> Intel® Time Coordinated Computing.....	88
7.2.5.	Advanced > Graphic Configuration	90
7.2.6.	Advanced > Power Management	92
7.2.7.	Advanced > System Management	93
7.2.8.	Advanced > Thermal Management	93
7.2.9.	Advanced > Watchdog Timer	96
7.2.10.	Advanced > Super IO Configuration	97
7.2.11.	Advanced > Miscellaneous	100
7.2.12.	Advanced > AMT Configuration (shown if SKU supported)	100
7.2.13.	Advanced > USB Configuration	101
7.2.14.	Advanced > AMI Graphics Output Protocol Policy.....	102
7.2.15.	Advanced > Serial Console Redirection	102
7.2.16.	Advanced > Network Stack Configuration.....	104
7.2.17.	Advanced > Trusted Computing.....	105
7.3.	Chipset	106
7.3.1.	Chipset > System Agent (SA) Configuration	106
7.3.2.	Chipset > PCH-IO Configuration	112
7.4.	Security	121
7.4.1.	Security > Secure Boot Menu	121
7.5.	Boot.....	122
7.5.1.	Boot > Boot Configuration	122
7.6.	Save & Exit.....	123
8.	BIOS Checkpoints, Beep Codes	124
8.1.	Status Code Ranges	125
8.2.	Standard Status Codes.....	126
8.2.1.	SEC Phase	126
8.2.2.	SEC Beep Codes	127
8.2.3.	PEI Phase.....	127
8.2.4.	PEI Beep Codes.....	131
8.2.5.	DXE Status Codes	132
8.2.6.	DXE Beep Codes.....	136
8.2.7.	ACPI/ASL Checkpoint	136
8.3.	OEM-Reserved Checkpoint Ranges	137
9.	Software Support.....	138
9.1.	Windows 10 IOT Enterprise 64-bit.....	138

9.2. Yocto Linux 64-bit.....	138
9.3. Ubuntu	138
9.4. VxWorks 64-bit	138
10. Mechanical and Thermal.....	139
10.1. Module Dimensions.....	139
10.2. Thermal Solutions.....	140
10.2.1. Heatspreader: HTS.....	140
10.2.2. Heatsink: THS	141
10.2.3. Heatsink High Profile: THSH	142
10.2.4. Heatsink with Fan: THSF	143

List of Figures

Figure 1 – Module function diagram.....20

Figure 2 - Module rear side row and pin numbering21

Figure 3 – Module feature locations.....58

Figure 4 – cExpress-TL and Debug Module59

Figure 5 – Module mechanical dimensions 139

Figure 6 – Heatspreader: HTS..... 140

Figure 7 – Heatsink: THS..... 141

Figure 8 – Heatsink High Profile: THSH 142

Figure 9 – Heatsink with Fan: THSF 143

1. Introduction

The cExpress-TL is the first COM Express® COM.0 R3.0 Compact Size Type 6 module based on the ultra-low-power 11th Generation Intel® Core™ i7/i5/i3, Celeron® processors (formerly "Tiger Lake-UP3") featuring a brand new Intel® Iris® Xe high performance graphics core and supporting AVX512-VNNI (Vector Neural Network Instructions) that almost triples AI inferencing performance. A configurable power range of 12 to 28 watts makes it ideally suited for fan less space-constraint embedded applications. Typical industries in need of such high performance, low power characteristics are transport, medical, industrial automation and control, edge controllers, robotics and multi camera-based AI.

The cExpress-TL supports BIOS configurable In-band ECC (IB ECC) that provides ECC level error correction on standard DDR4 memory. A maximum 64GB DDR4 3200 MT/s memory capacity, wide operating temperature range, and MIL-STD environmental specifications make it well suited for mission critical or extreme rugged applications.

The integrated Intel® Iris® Xe Graphics(Gen12) includes features such as OpenGL 4.5, DirectX 12, OpenCL 2.1/2.0/1.2, Intel® Clear Video HD Technology, and DirectX Video Acceleration (DXVA) support for full H.265/HEVC 10-bit, VP9 hardware codecs. In addition, High Dynamic Range is supported for enhanced picture color and quality and digital content protection has been upgraded to HDCP 2.2. Graphics outputs include LVDS and three DDI ports supporting HDMI/DVI/DisplayPort and eDP/VGA as a build option, with a maximum of four 4K displays supported.

Input/output features include up to eight PCIe Gen3 lanes (through a PCIe switch, project basis support) and PCIe x4 Gen4 lanes that can be used for NVMe SSD, allowing applications access to the highest speed storage solutions, as well as a single onboard 2.5Gigabit Ethernet port (SKU dependent) with optional Time Sensitive Network (TSN), four USB 3.2 Gen2 ports, four USB 2.0 ports, two SATA 6 Gb/s ports. Support is provided for SMBus and I2C. The module is equipped with SPI AMI EFI BIOS with CMOS backup, supporting embedded features such as remote console, hardware monitor, and watchdog timer.

2. Specifications

2.1. Core System

CPU

11th Gen Intel® Core™ and Intel® Celeron® Processor (formerly "Tiger Lake UP3")

- Intel® Core™ i7-1185G7E, 2.8(4.4) GHz, 12MB, 28W (15W-12W cTDP), 4C/Iris Xe (non-ECC)
- Intel® Core™ i5-1145G7E, 2.6(4.1) GHz, 8MB, 28W (15W-12W cTDP), 4C/Iris Xe (non-ECC)
- Intel® Core™ i3-1115G4E, 3.0(3.9) GHz, 6MB, 28W (15W-12W cTDP), 2C/UHD (non-ECC)
- Intel® Celeron® 6305E, 1.8GHz, 4MB, 15W, 2C/UHD (non-ECC)
- Intel® Core™ i7-1185GRE, 2.8(4.4) GHz, 12MB, 28W (15W-12W cTDP), 4C/Iris Xe (IBECC/non-ECC)
- Intel® Core™ i5-1145GRE, 2.6(4.1) GHz, 8MB, 28W (15W-12W cTDP), 4C/Iris Xe (IBECC/non-ECC)
- Intel® Core™ i3-1115GRE, 3.0(3.9) GHz, 6MB, 28W (15W-12W cTDP), 2C/UHD (IBECC/non-ECC)

Supporting: Intel® VT, Intel® VT-d, Intel® TXT, Intel® SSE4.2, Intel® HT Technology, Intel® 64 Architecture, Execute Disable Bit, Intel® Turbo Boost Technology 2.0, Intel® AVX-512, Intel® AVX2, Intel® AES-NI, PCLMULQDQ Instruction, Intel® Device Protection Technology with Intel® Secure Key, Intel® TSX-NI (availability of features may vary between processor SKUs)

Memory

Up to 64GB 3200 MT/s DDR4 in two SODIMM sockets, maximum 32GB per socket

In-band ECC (IBECC) with standard DDR4 memory support on selected SKUs (Core™ i7-1185GRE, Core™ i5-1145GRE, Core™ i3-1115GRE)

Cache

12MB for Core™ i7, 8MB for Core™ i5, 6MB for Core™ i3, 4MB for Celeron®

Embedded BIOS

AMI Aptio V UEFI with CMOS backup in 32 (or 16, TBC) MB SPI BIOS, dual BIOS by build option

2.2. Video

GPU

Intel® Iris® Xe Graphics (Gen12) core architecture for Core™ i7/ i5

Intel® Iris® UHD Graphics (Gen12) core architecture for Core™ i3, Celeron®

GPU Feature Support

4 independent and simultaneous combinations of DisplayPort/HDMI/LVDS graphics outputs (4x 4K @60Hz)

(eDP optional in place of LVDS, VGA optional in place of DDI 3)

Encode/transcode HD content

Playback of high-definition content including Blu-ray Disc and Blu-ray Disc 3D content using HDMI (1.4a spec compliant with 3D)

DirectX Video Acceleration (DXVA) support for accelerated video processing

HEVC/H.265, H.264, M/JPEG, MPEG2, AV1, WMV9, VP9 HW decode

HEVC/H.265, H.264, JPEG, VP9 HW encode

Advanced Scheduler 2.0, 1.0, XPDM support

DirectX up to 12

OpenGL up to 4.5 and ES 2.0 support

OpenCL up to 2.1 support



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

2.2.1. Display Interface Support

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

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

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

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

2.3. Audio

Intel® HD Audio integrated

Located on carrier Express-BASE6 (ALC886 standard support)

2.4. Expansion Busses

5 PCI Express x1 Gen3: Lanes 0,1,2,3 (configurable to 4 x1, 2 x2, 1 x4, 2 x1 + 1 x2, 1 x2 + 2 x1) and Lane 4 (x1 only)

A PCIe switch is HW BOM option by project basis to offer more x1 lanes via Lanes 5,6,7

1 PCI Express x4 Gen4: Lanes 16, 17, 18, 19 (x4 only), Gen4 support dependent on carrier design

Other: SMBus (system), I2C (user), LPC bus (via eSPI to LPC bridge IC)

2.5. Ethernet

2.5Gigabit Intel® Ethernet Controller i225 Series (V, IT or LM version)

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

V version supports up to 2.5GbE (without TSN, selected for Standard Operating Temperature SKU)

IT version supports TSN feature (at Linux OS) at maximum 2.5GbE connection (selected for Extreme Rugged Operating Temperature SKU)

GbE0_SDP available if TSN support enabled

Other combinations supported by project basis

2.6. Multi I/O and Storage

USB

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

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



Note: Carrier board must be designed for Gen2 operation.

UART

Two UART interfaces SER0 and SER1 RX/TX on module

Console Redirection COM 1 or COM 2 selectable in BIOS

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

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

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

GPIO or SD

4 GPO and 4 GPI (GPI with interrupt)

SATA

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

2.7. Trusted Platform Module (TPM)

Chipset: Infineon solution

Type: TPM 2.0 (SPI bus based)

TPM chip is BOM option

2.8. SEMA Board controller

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

2.9. Debug

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

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

2.10. Power

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

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

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

Power Management: ACPI 5.0 compliant, Smart Battery support

Power States: C1-C6, S0, S1, S3, S4, S5, S5 ECO mode (Wake-on-USB S3/S4, WoL S3/S4/S5)

ECO Mode support for deep S5 for 5Vsb power saving

Power Consumption

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

2.11. Mechanical and Environmental

Form Factor and specification

PICMG COM Express Rev 3.0 (COM.0 R3.0), Type 6, Compact size 95 x 95 mm

Operating Temperature

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

Extreme Rugged -40°C to +85°C (Standard Voltage Input) Storage: -40°C to +85°C
(Selected SoC SKUs)

Humidity

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

Shock and Vibration

IEC 60068-2-64 and IEC-60068-2-27

MIL-STD-202F, Method 213B, Table 213-I, Condition A and Method 214A, Table 214-I, Condition D

HALT tested

Thermal Stress, Vibration Stress, Thermal Shock and Combined Test

3. Block Diagram

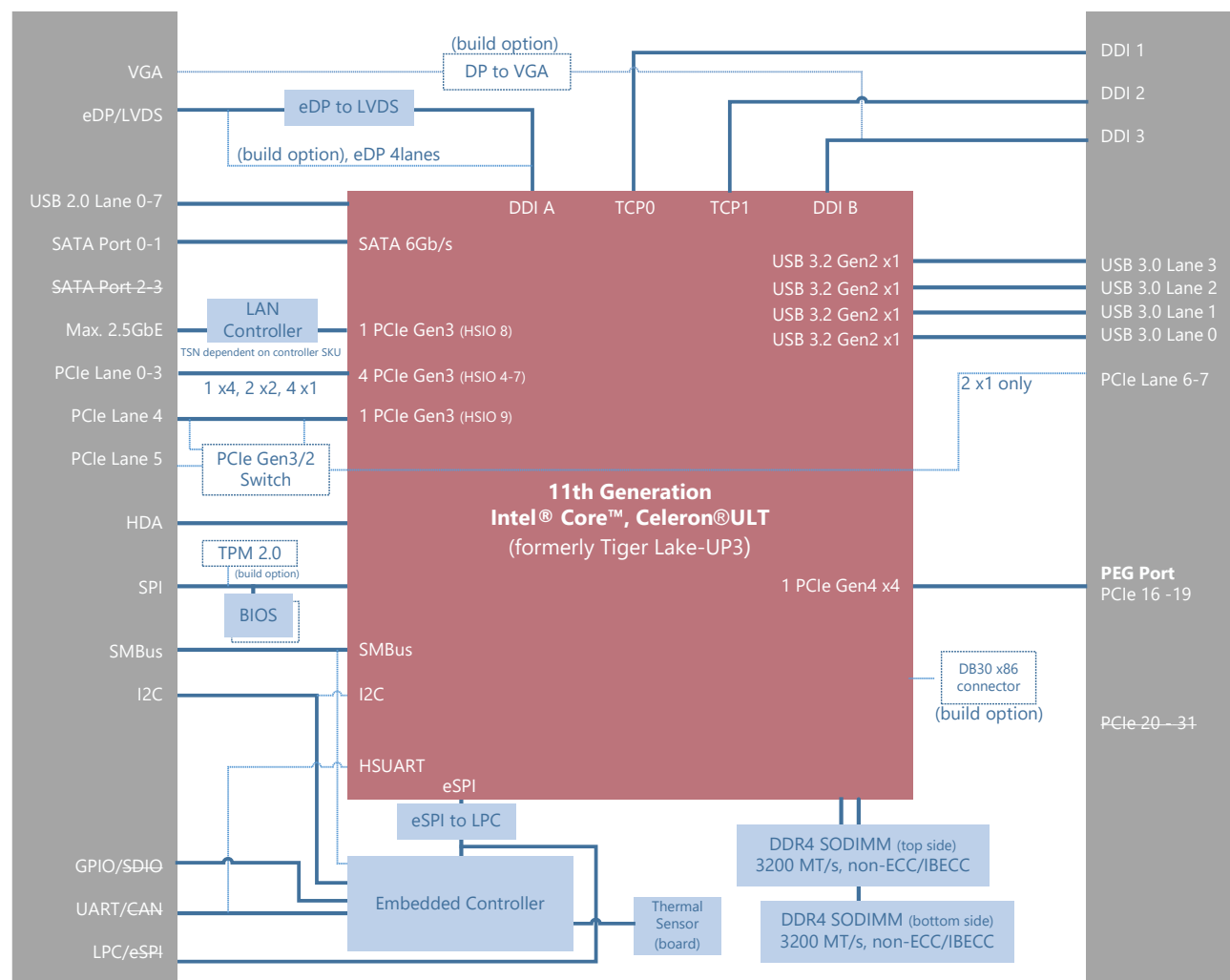


Figure 1 – Module function diagram

4. Pinout and Signal Descriptions

4.1. Pin Summary

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

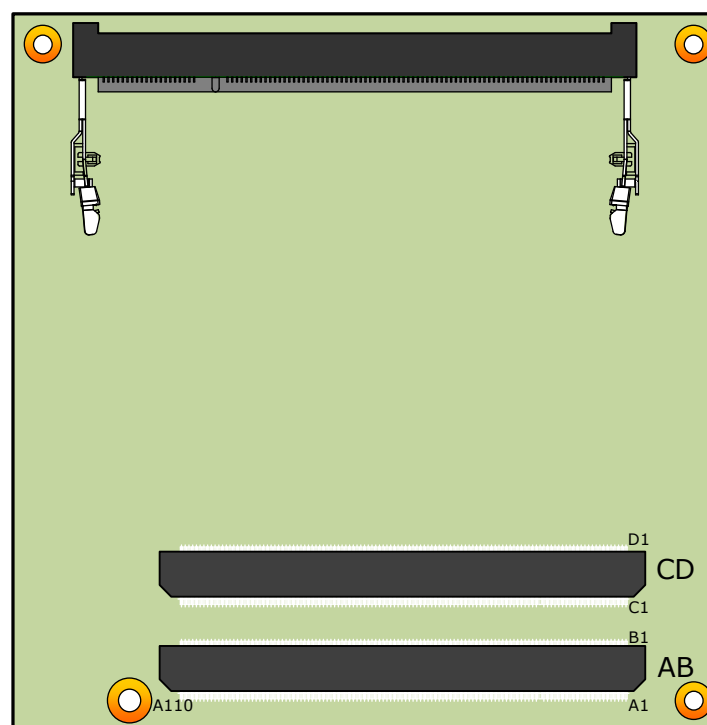


Figure 2 - Module rear side row and pin numbering

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#	C3	USB_SSRX0-	D3	USB_SSTX0-
A4	GBE0_LINK100# *	B4	LPC_AD0/ESPI_IO_0	C4	USB_SSRX0+	D4	USB_SSTX0+
A5	GBE0_LINK1000# *	B5	LPC_AD1/ESPI_IO_1	C5	GND	D5	GND
A6	GBE0_MDI2-	B6	LPC_AD2/ESPI_IO_2	C6	USB_SSRX1-	D6	USB_SSTX1-
A7	GBE0_MDI2+	B7	LPC_AD3/ESPI_IO_3	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	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	DDI1_PAIR6+	D15	DDI1_CTRLCLK_AUX+
A16	SATA0_TX+	B16	SATA1_TX+	C16	DDI1_PAIR6-	D16	DDI1_CTRLCLK_AUX-
A17	SATA0_TX-	B17	SATA1_TX-	C17	RSVD	D17	RSVD
A18	SUS_S4#	B18	SUS_STAT#/ESPI_RESET#	C18	RSVD	D18	RSVD
A19	SATA0_RX+	B19	SATA1_RX+	C19	PCIE_RX6+ *	D19	PCIE_TX6+ *
A20	SATA0_RX-	B20	SATA1_RX-	C20	PCIE_RX6- *	D20	PCIE_TX6- *
A21	GND (FIXED)	B21	GND (FIXED)	C21	GND (FIXED)	D21	GND (FIXED)
A22	SATA2_TX+	B22	SATA3_TX+	C22	PCIE_RX7+ *	D22	PCIE_TX7+ *
A23	SATA2_TX-	B23	SATA3_TX-	C23	PCIE_RX7- *	D23	PCIE_TX7- *
A24	SUS_S5#	B24	PWR_OK	C24	DDI1_HPD	D24	RSVD
A25	SATA2_RX+	B25	SATA3_RX+	C25	DDI1_PAIR4+	D25	RSVD
A26	SATA2_RX-	B26	SATA3_RX-	C26	DDI1_PAIR4-	D26	DDI1_PAIR0+
A27	BATLOW#	B27	WDT	C27	RSVD	D27	DDI1_PAIR0-
A28	(S)ATA_ACT#	B28	AC/HDA_SDIN2	C28	RSVD	D28	RSVD
A29	AC/HDA_SYNC	B29	AC/HDA_SDIN1	C29	DDI1_PAIR5+	D29	DDI1_PAIR1+
A30	AC/HDA_RST#	B30	AC/HDA_SDIN0	C30	DDI1_PAIR5-	D30	DDI1_PAIR1-
A31	GND (FIXED)	B31	GND (FIXED)	C31	GND (FIXED)	D31	GND (FIXED)
A32	AC/HDA_BITCLK	B32	SPKR	C32	DDI2_CTRLCLK_AUX+	D32	DDI1_PAIR2+
A33	AC/HDA_SDOUT	B33	I2C_CK	C33	DDI2_CTRLCLK_AUX-	D33	DDI1_PAIR2-
A34	BIOS_DIS0#/ESPI_SAFS	B34	I2C_DAT	C34	DDI2_DDC_AUX_SEL	D34	DDI1_DDC_AUX_SEL
A35	THRMTRIP#	B35	THRM#	C35	RSVD	D35	RSVD

Row A		Row B		Row C		Row D	
A36	USB6-	B36	USB7-	C36	DDI3_CTRLCLK_AUX+	D36	DDI1_PAIR3+
A37	USB6+	B37	USB7+	C37	DDI3_CTRLDATA_AUX-	D37	DDI1_PAIR3-
A38	USB_6_7_OC#	B38	USB_4_5_OC#	C38	DDI3_DDC_AUX_SEL	D38	RSVD
A39	USB4-	B39	USB5-	C39	DDI3_PAIR0+	D39	DDI2_PAIR0+
A40	USB4+	B40	USB5+	C40	DDI3_PAIR0-	D40	DDI2_PAIR0-
A41	GND (FIXED)	B41	GND (FIXED)	C41	GND (FIXED)	D41	GND (FIXED)
A42	USB2-	B42	USB3-	C42	DDI3_PAIR1+	D42	DDI2_PAIR1+
A43	USB2+	B43	USB3+	C43	DDI3_PAIR1-	D43	DDI2_PAIR1-
A44	USB_2_3_OC#	B44	USB_0_1_OC#	C44	DDI3_HPD	D44	DDI2_HPD
A45	USB0-	B45	USB1-	C45	RSVD	D45	RSVD
A46	USB0+	B46	USB1+	C46	DDI3_PAIR2+	D46	DDI2_PAIR2+
A47	VCC_RTC	B47	ESPI_EN#	C47	DDI3_PAIR2-	D47	DDI2_PAIR2-
A48	RSVD	B48	USB0_HOST_PRSNT	C48	RSVD	D48	RSVD
A49	GBE0_SDP	B49	SYS_RESET#	C49	DDI3_PAIR3+	D49	DDI2_PAIR3+
A50	LPC_SERIRQ/ESPI_CS1#	B50	CB_RESET#	C50	DDI3_PAIR3-	D50	DDI2_PAIR3-
A51	GND (FIXED)	B51	GND (FIXED)	C51	GND (FIXED)	D51	GND (FIXED)
A52	PCIE_TX5+ *	B52	PCIE_RX5+ *	C52	PEG_RX0+	D52	PEG_TX0+
A53	PCIE_TX5- *	B53	PCIE_RX5- *	C53	PEG_RX0-	D53	PEG_TX0-
A54	GPIO	B54	GPO1	C54	TYPE0#	D54	PEG_LANE_RV#
A55	PCIE_TX4+	B55	PCIE_RX4+	C55	PEG_RX1+	D55	PEG_TX1+
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	RSVD	D63	RSVD
A64	PCIE_TX1+	B64	PCIE_RX1+	C64	RSVD	D64	RSVD
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)

Row A		Row B		Row C		Row D	
A71	LVDS_A0+ / eDP_TX2+	B71	LVDS_B0+	C71	PEG_RX6+	D71	PEG_TX6+
A72	LVDS_A0- / eDP_TX2-	B72	LVDS_B0-	C72	PEG_RX6-	D72	PEG_TX6-
A73	LVDS_A1+ / eDP_TX1+	B73	LVDS_B1+	C73	GND	D73	GND
A74	LVDS_A1- / eDP_TX1-	B74	LVDS_B1-	C74	PEG_RX7+	D74	PEG_TX7+
A75	LVDS_A2+ / eDP_TX0+	B75	LVDS_B2+	C75	PEG_RX7-	D75	PEG_TX7-
A76	LVDS_A2- / eDP_TX0-	B76	LVDS_B2-	C76	GND	D76	GND
A77	LVDS_VDD_EN / eDP_VDD_EN	B77	LVDS_B3+	C77	RSVD	D77	RSVD
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+	B81	LVDS_B_CK+	C81	PEG_RX9+	D81	PEG_TX9+
A82	LVDS_A_CK- / eDP_TX3-	B82	LVDS_B_CK-	C82	PEG_RX9-	D82	PEG_TX9-
A83	LVDS_I2C_CK / eDP_AUX+	B83	LVDS_BKLT_CTRL / eDP_BKLT_CTRL	C83	RSVD	D83	RSVD
A84	LVDS_I2C_DAT / eDP_AUX-	B84	VCC_5V_SBY	C84	GND	D84	GND
A85	GPI3	B85	VCC_5V_SBY	C85	PEG_RX10+	D85	PEG_TX10+
A86	RSVD	B86	VCC_5V_SBY	C86	PEG_RX10-	D86	PEG_TX10-
A87	eDP_HP	B87	VCC_5V_SBY	C87	GND	D87	GND
A88	PCIE0_CK_REF+	B88	BIOS_DIS1#	C88	PEG_RX11+	D88	PEG_TX11+
A89	PCIE0_CK_REF-	B89	VGA_RED *	C89	PEG_RX11-	D89	PEG_TX11-
A90	GND (FIXED)	B90	GND (FIXED)	C90	GND (FIXED)	D90	GND (FIXED)
A91	SPI_POWER	B91	VGA_GRN *	C91	PEG_RX12+	D91	PEG_TX12+
A92	SPI_MISO	B92	VGA_BLU *	C92	PEG_RX12-	D92	PEG_TX12-
A93	GPO0	B93	VGA_HSYNC *	C93	GND	D93	GND
A94	SPI_CLK	B94	VGA_VSYNC *	C94	PEG_RX13+	D94	PEG_TX13+
A95	SPI_MOSI	B95	VGA_I2C_CK *	C95	PEG_RX13-	D95	PEG_TX13-
A96	TPM_PP	B96	VGA_I2C_DAT *	C96	GND	D96	GND
A97	TYPE10#	B97	SPI_CS#	C97	RSVD	D97	RSVD
A98	SER0_TX	B98	RSVD	C98	PEG_RX14+	D98	PEG_TX14+
A99	SER0_RX	B99	RSVD	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

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



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

PCIe lane 5,6,7 are BOM option support (through a PCIe switch) by project basis.

eDP (in place of LVDS) and VGA (in place of DDI 3) are BOM option support by project basis.

Ethernet support up to 2.5GbE. The LAN LED behavior (GBE0_LINK 100#, GBE0_LINK1000#) is optimized based on maximum 2.5GbE speed (see [4.3.4 Gigabit Ethernet on page 32](#)).

4.2. Signal Terminology Descriptions

Meaning of the terms used for signal description tables

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

4.3. AB Connector Signal Descriptions

4.3.1. Audio

Name	Pin #	Description	I/O	PU / PD	Comment
AC_RST# / HDA_RST#	A30	Reset output to CODEC, active low.	O 3.3VSB		
AC_SYNC / HDA_SYNC	A29	Sample-synchronization signal to the CODEC(s).	O 3.3VSB		
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		
AC_SDIN[2:0] / HDA_SDIN[2:0]	B28- B30	Serial TDM data inputs from up to 3 CODECs.	I/O 3.3VSB		B28 Not supported Tiger Lake UP3 doesn't offer this pin

4.3.2. Analog VGA

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



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

4.3.3. LVDS or eDP

The module default supports a single or dual channel LVDS display panel with up to 24-bit colours.

There is a BOM option 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 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: <table><tr><th></th><th>1000</th><th>100</th><th>10</th></tr><tr><td>MDI[0]+/-</td><td>B1_DA+/-</td><td>TX+/-</td><td>TX+/-</td></tr><tr><td>MDI[1]+/-</td><td>B1_DB+/-</td><td>RX+/-</td><td>RX+/-</td></tr><tr><td>MDI[2]+/-</td><td>B1_DC+/-</td><td></td><td></td></tr><tr><td>MDI[3]+/-</td><td>B1_DD+/-</td><td></td><td></td></tr></table>		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.
	1000	100	10																						
MDI[0]+/-	B1_DA+/-	TX+/-	TX+/-																						
MDI[1]+/-	B1_DB+/-	RX+/-	RX+/-																						
MDI[2]+/-	B1_DC+/-																								
MDI[3]+/-	B1_DD+/-																								
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																				

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

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 10	
SATA1	HSIO 11	
SATA2	N/A	Not supported
SATA3	N/A	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 By a PCIe switch, project basis
PCIE_RX5+ PCIE_RX5-	B52 B53	PCI Express channel 5, Receive Input differential pair.	I PCIE		AC coupled off Module By a PCIe switch, project basis
PCIE_CLK_REF+ PCIE_CLK_REF-	A88 A89	PCI Express Reference Clock output for all PCI Express and PCI Express Graphics Lanes.	O PCIE		



Note : PCIe Lane 5, 6, 7 are supported by PCIe switch, by project basis

4.3.6.1. PCH HSIO Lane Assignments

Name	HSIO name on SOC	Comment
PCIE0	HSIO 4	
PCIE1	HSIO 5	
PCIE2	HSIO 6	
PCIE3	HSIO 7	
PCIE4	HSIO 9	
PCIE5	N/A	BOM option support by project basis through a PCIe switch
PCIE6	N/A	BOM option support by project basis through a PCIe switch
PCIE7	N/A	BOM option support by project basis through a PCIe switch

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 a 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_PRSENT	B48	Module USB client may detect the presence of a USB host on USB0. A high value indicates that a host is present.	I 3.3VSB		Not supported



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

4.3.9. SPI Bus (BIOS only)

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

4.3.10. Miscellaneous

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

4.3.11. 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 10K 3.3VSB	

4.3.12. I2C Bus

Name	Pin #	Description	I/O	PU / PD	Comment
I2C_CK	B33	General purpose I ² C 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 ² C 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 3.3V	After hardware RESET output low
GPO[1]	B54	General purpose output pins.	O 3.3V	PD 10K 3.3V	After hardware RESET output low
GPO[2]	B57	General purpose output pins.	O 3.3V	PD 10K 3.3V	After hardware RESET output low
GPO[3]	B63	General purpose output pins.	O 3.3V	PD 10K 3.3V	After hardware RESET output low
GPI[0]	A54	General purpose input pins. Pulled high internally on the module.	I 3.3V	PU 10K 3.3V	
GPI[1]	A63	General purpose input pins. Pulled high internally on the module.	I 3.3V	PU 10K 3.3V	
GPI[2]	A67	General purpose input pins. Pulled high internally on the module.	I 3.3V	PU 10K 3.3V	
GPI[3]	A85	General purpose input pins. Pulled high internally on the module.	I 3.3V	PU 10K 3.3V	

4.3.14. Serial Interface Signals

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

4.3.15. Power and System Management

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

4.3.16. Power and Ground

Name	Pin #	Description	I/O	PU / PD	Comment
VCC_12V	A104, A105, A106, A107, A108, A109, B104, B105, B106, B107, B109	Primary power input supports wide range 5~ 20V input All available VCC_12V pins on the connector(s) shall be used.	P		8.5-20 V
VCC_5V_SBY	B84, B85, B86, B87	Standby power input: +5.0V nominal. If VCC5_SBY is used, all available VCC_5V_SBY pins on the connector(s) shall be used. Only used for standby and suspend functions. May be left unconnected if these functions are not used in the system design.	P		5Vsb $\pm$ 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 By a PCIe switch, project basis
PCIE_RX6+ PCIE_RX6-	C19 C20	PCI Express channel 6, Receive Input differential pair.	I PCIE		AC coupled off Module By a PCIe switch, project basis
PCIE_TX7+ PCIE_TX7-	D22 D23	PCI Express channel 7, Transmit Output differential pair.	O PCIE		AC coupled on Module By a PCIe switch, project basis
PCIE_RX7+ PCIE_RX7-	C22 C23	PCI Express channel 7, Receive Input differential pair.	I PCIE		AC coupled off Module By a PCIe switch, project basis



Note : PCIe Lane 5, 6, 7 are supported by PCIe switch, by project basis

4.4.2.1. PCH HSIO Lane Assignments

Name	HSIO name on SOC	Comment
PCIE0	HSIO 4	
PCIE1	HSIO 5	
PCIE2	HSIO 6	
PCIE3	HSIO 7	
PCIE4	HSIO 9	
PCIE5	N/A	BOM option support by project basis through a PCIe switch
PCIE6	N/A	BOM option support by project basis through a PCIe switch
PCIE7	N/A	BOM option support by project basis through a PCIe switch

4.4.3. DDI1 Port

Name	Pin #	Displayport (DP)	HDMI
DDI1_PAIR0+	D26	DP1_LANE0+	TMDS1_DATA2+
DDI1_PAIR0-	D27	DP1_LANE0-	TMDS1_DATA2-
DDI1_PAIR1+	D29	DP1_LANE1+	TMDS1_DATA1+
DDI1_PAIR1-	D30	DP1_LANE1-	TMDS1_DATA1-
DDI1_PAIR2+	D32	DP1_LANE2+	TMDS1_DATA0+
DDI1_PAIR2-	D33	DP1_LANE2-	TMDS1_DATA0-
DDI1_PAIR3+	D36	DP1_LANE3+	TMDS1_CLK+
DDI1_PAIR3-	D37	DP1_LANE3-	TMDS1_CLK-
DDI1_PAIR4+	C25	-	-
DDI1_PAIR4-	C26	-	-
DDI1_PAIR5+	C29	-	-
DDI1_PAIR5-	C30	-	-
DDI1_PAIR6+	C15	-	-
DDI1_PAIR6-	C16	-	-
DDI1_HPD	C24	DP1_HPD	HDMI1_HPD
DDI1_CTRLCLK_AUX+	D15	DP1_AUX+	HMDI1_CTRLCLK
DDI1_CTRLCLK_AUX-	D16	DP1_AUX-	HMDI1_CTRLCLK
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_CLK lines are DC coupled, but the DP_AUX+ /- pair must be AC coupled. A set of FET switches is usually used to sort this out. The FET gates can be controlled by the AUX_SEL pin function.

4.4.3.1. Displayport (DP) Mode

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

4.4.3.2. HDMI Mode

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

4.4.4. DDI2 Port

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



Note:

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

4.4.4.1. Displayport (DP) Mode

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

4.4.4.2. HDMI Mode

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

4.4.5. DDI3 Port

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



Note:

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

4.4.5.1. Displayport (DP) Mode

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

4.4.5.2. HDMI Mode

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

4.4.6. PCIe Graphics Port (PEG)

Name	Pin #	Description	I/O	PU / PD	Comment
PEG_TX0+ PEG_TX0-	D52 D53	PCI Express Graphics transmit differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	O PCIE		AC coupled on Module
PEG_RX0+ PEG_RX0-	C52 C53	PCI Express Graphics receive differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	I PCIE		AC coupled off Module
PEG_TX1+ PEG_TX1-	D55 D56	PCI Express Graphics transmit differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	O PCIE		AC coupled on Module
PEG_RX1+ PEG_RX1-	C55 C56	PCI Express Graphics receive differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	I PCIE		AC coupled off Module
PEG_TX2+ PEG_TX2-	D58 D59	PCI Express Graphics transmit differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	O PCIE		AC coupled on Module
PEG_RX2+ PEG_RX2-	C58 C59	PCI Express Graphics receive differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	I PCIE		AC coupled off Module
PEG_TX3+ PEG_TX3-	D61 D62	PCI Express Graphics transmit differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	O PCIE		AC coupled on Module
PEG_RX3+ PEG_RX3-	C61 C62	PCI Express Graphics receive differential pairs. These are the same lines as PCIE_TX[16:31]+ and – in Module pin-out Type 6	I PCIE		AC coupled off Module
PEG_LANE_RV#	D54	PCI Express Graphics lane reversal input strap. Pull low on the Carrier Board to reverse lane order.	I 3.3V		



Note: Form the 16 lanes on the PEG port only lanes 0-3 are supported. The configuration is one x4

4.4.7. Module Type Definition

Name	Pin #	Description	I/O	PU / PD	Comment																																				
TYPE0# TYPE1# TYPE2#	C54 C57 D57	The TYPE pins indicate to the Carrier Board the Pin-out Type that is implemented on the Module. The pins are tied on the Module to either ground (GND) or are no-connects (NC). For Pin-out Type 1 and Type 10 that lack a CD connector, these pins are not present (X) <table><thead><tr><th>TYPE2#</th><th>TYPE1#</th><th>TYPE0#</th><th></th></tr></thead><tbody><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></tbody></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.	TYPE2#	TYPE1#	TYPE0#		X	X	X	Pinout Type 1	X	X	X	Pinout Type 10	NC	NC	NC	Pinout Type 2	NC	NC	GND	Pinout Type 3	NC	GND	NC	Pinout Type 4	NC	GND	GND	Pinout Type 5	GND	NC	NC	Pinout Type 6	GND	NC	GND	Pinout Type 7			Type 6
TYPE2#	TYPE1#	TYPE0#																																							
X	X	X	Pinout Type 1																																						
X	X	X	Pinout Type 10																																						
NC	NC	NC	Pinout Type 2																																						
NC	NC	GND	Pinout Type 3																																						
NC	GND	NC	Pinout Type 4																																						
NC	GND	GND	Pinout Type 5																																						
GND	NC	NC	Pinout Type 6																																						
GND	NC	GND	Pinout Type 7																																						
TYPE10#	A97	In case of a type 10 module this pin signal is tied to GND through a 47K resistor on the module.			No PD																																				

4.4.8. Power and Ground

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

5. Additional Features

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

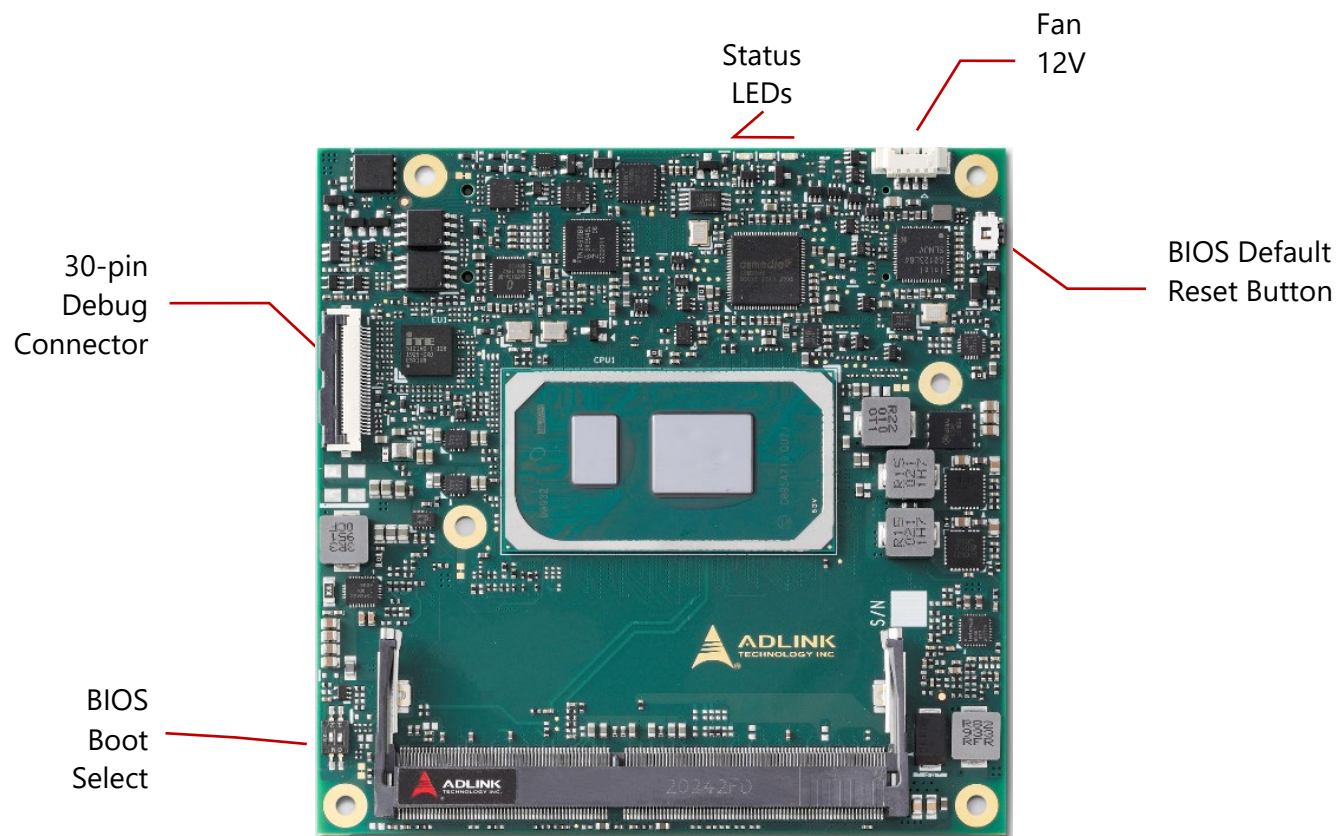


Figure 3 – Module feature locations

5.1. Debug Connector

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

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

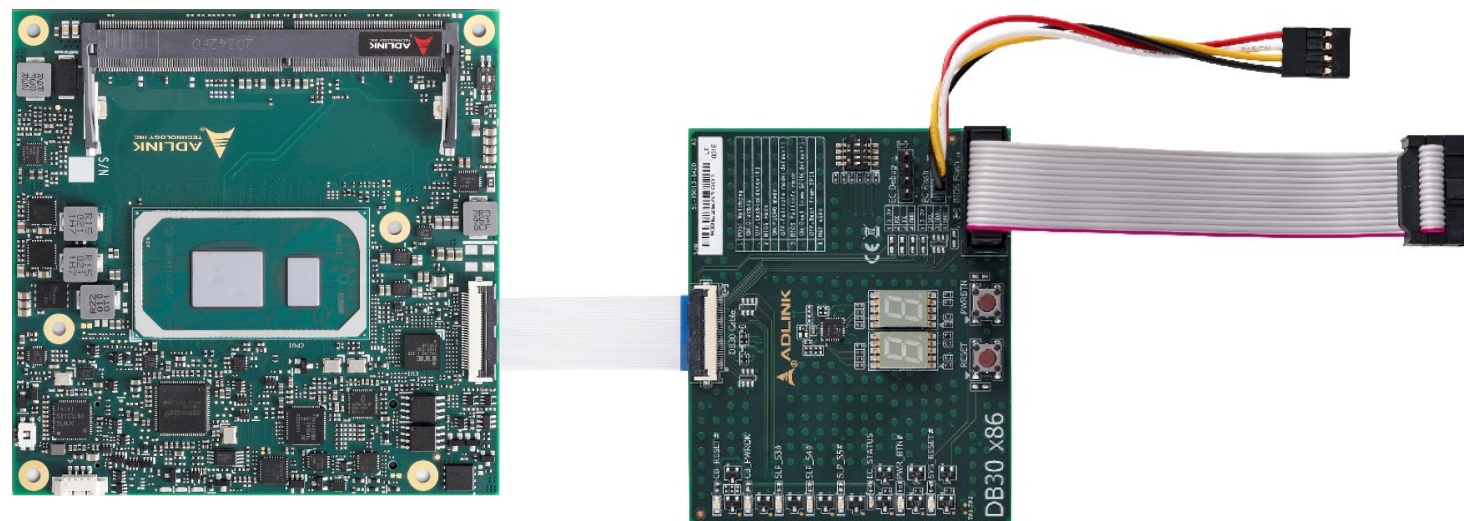
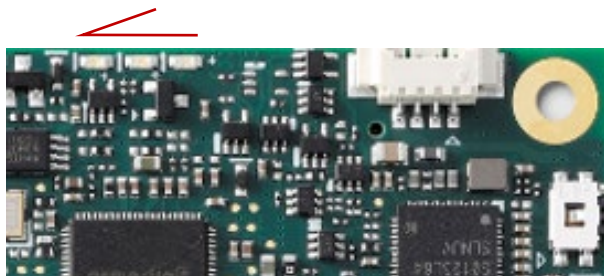


Figure 4 – cExpress-TL and Debug Module

5.2. Status LEDs

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

LED1 LED2 LED3



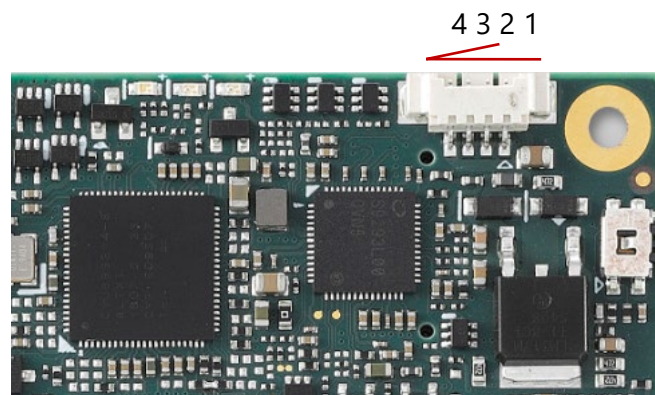
Name	Color	Connection	Function
LED1	Blue	BMC output	Power Sequence Status Code (BMC) Power Changes, RESET (see Exception Codes below)
LED2	Green	Power Source 3Vcc	S0 LED ON S3/S4/S5 LED OFF ECO mode LED OFF
LED3	Red	BMC output and same signal as WDT (B27) on BtB connector	Module power up WD LED = LED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

5.3. Exception Codes

Exception Code	Error Message
0	NOERROR
3	NO_SLP_S5
4	NO_SLP_S4
5	NO_SLP_S3
6	BIOS_FAIL
7	RESET_FAIL
8	RESETIN_FAIL
9	NO_CB_PWROK
10	CRITICAL_TEMP
11	POWER_FAIL
12	VOLTAGE_FAIL
13	RSMRST_FAIL
14	NO_VDDQ_PG
15	NO_V1P05A_PG
16	NO_VCORE_PG
17	NO_SYS_GD
19	NO_V3P3A
21	NO_PWRSRC_GD

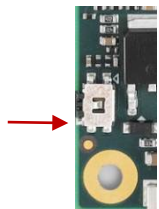
5.4. Fan Connector

Connector type: JVE 24W1125A-04M00



Name	Description
1	FAN_PWMOUT
2	FAN_TACHIN
3	GND
4	12V

5.5. BIOS Default Reset Button



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

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



5.6. BIOS Boot Select

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

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

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

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

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

6. System Resources

6.1. System Memory Map

Memory Range	Dependency / Comments
FFE00000 – FFFFFFFF	High BIOS Area
FEE00000 – FEEFFFFF	MSI Interrupt
FEC00000 – FECFFFFF	APIC Configuration Space
F00000 – FFFFFF	ISA Hole
100000 – EFFFFF	Main Memory
0K – 1MB	DOS Compatibility Memory

6.2. I/O Range Map

Hex Range	Device
000h-CF7h	PCIe Root Complex
020h – 02Dh & 030h – 03Dh	Programmable interrupt controller
02Eh – 02Fh	Motherboard resource
040h – 043h & 050h – 053h	System Timer
04Eh – 04Fh	Motherboard resource
060h, 064h	8042 equivalent (keyboard)
061h, 063h, 065h, 067h, 070h, 080h, 92h	Motherboard resource
062h, 066h	Embedded Controller
0A0h – 0A1h & 0A4h – 0A5h, 0A8h – 0A9h & 0ACh – 0ADh, & 0B0h – 0B1h & 0B4h – 0B5h & 0B8h – 0B9h & 0BCh – 0BDh	Programmable interrupt controller

Hex Range	Device
240h – 247h	Serial Port 3
248h – 24Fh	Serial Port 4
2F8h – 2FFh	Serial Port 2
3F8h – 3FFh	Serial Port 1
4D0h-4D1h	Programmable interrupt controller
680h-69Fh, A00h-A1Fh,A20h-A2Fh,A30h-A3Fh,A40h-A4Fh,A50h-A5Fh,A60h-A6Fh	Motherboard resource
FFF8h-FFFFh	AMT SOL Serial COM 5
0D00h- – FFFFh	PCIe Root Complex
164Eh – 164Fh,1800h-18FEh,1854h-1857h,2000h-20FEh	Motherboard resource
03000h-303Fh	Intel Graphics Driver
03060h – 307Fh, 03080h-03083h, 3090h-3097h	SATA AHCI Controller
EFA0h-EFBFh	SMBUS
FFF8h-FFFFh	AMT SOL Serial COM 5

6.3. Interrupt Request (IRQ) Lines

APIC Mode

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



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

6.4. PCI Configuration Space Map

Bus Number	Device Number	Function Number	Routings	Description
00h	00h	00h	N/A	HOST and DRAM Controller
00h	02h	00h	Internal	Processor Graphics
00h	06h	00h	Internal	PCI Express* Controller(x4 PCIe)
00h	08h	00h	Internal	Gauss Newton Algorithm Device
00h	0Ah	00h	Internal	Intel Data AcquisitionSignal Processing
00h	0Dh	00h	Internal	USB Host Controller
00h	0Dh	01h	Internal	USB Device Controller
00h	0Dh	02h	Internal	Thunderbolt DMA
00h	0Dh	03h	Internal	Thunderbolt DMA
00h	0Eh	00h	Internal	Volume Management Device
00h	10h	00h	Internal	Intel Serial Bus Controller
00h	10h	05h	Internal	Intel Host Bridge PCIe
00h	14h	00h	Internal	USB 3.2 Gen 2x1 (10 Gb/s) xHCI HC
00h	14h	01h	Internal	USB 3.2 Gen 1x1 (5 Gb/s) Device Controller (xHCI)
00h	14h	02h	Internal	Shared SRAM
00h	15h	00h	Internal	I2C Controller #0
00h	15h	02h	Internal	I2C Controller #2
00h	15h	03h	Internal	I2C Controller #3
00h	16h	00h	Internal	Intel® CSME: HECI #1
00h	16h	01h	Internal	Intel® CSME: HECI #2
00h	16h	02h	Internal	Intel® CSME: IDE Redirection (IDE-R)
00h	16h	03h	Internal	Intel® CSME: Keyboard and Text (KT) Redirection
00h	17h	00h	Internal	SATA Controller (AHCI)
00h	19h	00h	Internal	I2C Controller #4
00h	19h	01h	Internal	I2C Controller #5
00h	1Dh	00h	Internal	Intel PCI Express Root port 9

Bus Number	Device Number	Function Number	Routings	Description
00h	1Dh	01h	Internal	Intel PCI Express Root port 10
00h	1Fh	00h	Internal	eSPI Controller
00h	1Fh	03h	Internal	Intel® High Definition Audio (Intel® HD Audio) (Audio, Voice, Speech)
00h	1Fh	04h	Internal	Intel SMBUS
00h	1Fh	05h	Internal	SPI (flash) Controller
00h	1Eh	00h	Internal	UART #0
00h	1Eh	01h	Internal	UART #1

6.5. PCI Interrupt Routing Map

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

INT Line	PCIe Port 5	PCIe Port 6	PCIe Port 7	PCIe Port 8	PCIe Port 9	PCIe Port 10
Int0	INTA: 16	INTB: 17	INTC: 18	INTD: 19	INTA: 16	INTB: 17
Int1	INTB: 17	INTC: 18	INTD: 19	INTA: 16	INTB: 17	INTC: 18
Int2	INTC: 18	INTD: 19	INTA: 16	INTB: 17	INTC: 18	INTD: 19
Int3	INTD: 19	INTA: 16	INTB: 17	INTC: 18	INTD: 19	INTA: 16

6.6. SMBus Address Table

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

7. BIOS Configurations

7.1. Menu Structure

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

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

7.1.1. Main > BIOS Information

Feature	Options	Description
BIOS Vendor	Info only	American Megatrends
BIOS Version	Info only	Display Core version
Build Date	Info only	Display compliancy information
MRC Version	Info only	Display compliancy information
GOP Version	Info only	ADLINK BIOS version.
ME FW Version	Info only	ADLINK BIOS version.
BIOS Boot Source	Info only	SPI Boot Source

7.1.2. Main > System Information

Board Information	Options	Description
Project Name	Info only	Display Project Name.
CPU Board Version	Info only	Display CPU Signature.
CPU Brand String	Info only	Display CPU Brand Name.
CPU Frequency	Info only	Display CPU Frequency
Total Memory	Info only	Display installed memory size.
Memory Frequency	Info only	Display memory frequency.
PCH SKU	Info only	Display PCH Information.
Board Information	Submenu	

7.1.3. Main > Board Information

Feature	Options	Description
Serial Number	Read only	Display SMC serial Number
Manufacturing Date	Read only	Display SMC manufacturing date.
Last Repair Date	Read only	Display SMC last repair date.
MAC ID	Read only	Display SMC MAC ID.
Runtime Statistics	Info only	
Total Runtime	Read only	The returned value specifies the total time in minutes the system is running in S0 state.
Current Runtime	Read only	The returned value specifies the time in seconds the system is running in S0 state. This counter is cleared when the system is removed from the external power supply.
Power Cycles	Read only	The returned value specifies the number of times the external power supply has been shut down.
Boot Cycles	Read only	The 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.

7.1.4. Main > System Date/Time

Feature	Options	Description
System Date	Weekday, MM/DD/YYYY	Requires the alpha-numeric entry of the day of the week, day of the month, calendar month, and all 4 digits of the year, indicating the century and year (Fri XX/XX/20XX)
System Time	HH/MM/SS	Presented as a 24-hour clock setting in hours, minutes, and seconds
Access Level	Read only	It shows what access level is used to enter BIOS setup menu.

7.2. Advanced

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

7.2.1. Advanced > CPU Configuration

Feature	Options	Description
Type	Info only	Display CPU information.
ID	Info only	Display CPU information.
Speed	Info only	Display CPU Frequency.
L1 Data Cache	Info only	Display cache info.
L1 Instruction Cache	Info only	Display cache info.
L2 Cache	Info only	Display cache info.
L3 Cache	Info only	Display cache info.
L4 Cache	Info only	Display cache info.
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 Processor Cores	All, 1, 2, 3, 4, 5, 6, 7, 8	Number of cores to enable in each processor package.
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.

7.2.2. Advanced > Power & Performance

7.2.2.1. Advanced > Power & Performance > CPU – Power Management

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.
Intel(R) Turbo Boost Max Technology 3.0	Disabled, Enabled	Enable/Disable Intel(R) Turbo Boost Max Technology 3.0 support. Disabling will report the maximum ratio of the slowest core in _CPC object.
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 Fast MSR Support	Disabled, Enabled	Enable/Disable HwP Fast MSR Support for IA32_HWP_REQUEST 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	
Energy Efficient P-state	Disabled, Enabled	Enable/Disable Energy Efficient P-state feature. When

Feature	Options	Description
		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.
1-Core Turbo Ratio Limit Ratio (TRLR) Override	[Max-Value, Min-Value, Step-Value] = [0x53, 0x00, 0x01]	1-Core Turbo Ratio Limit Ratio (TRLR) with range of Max Non-Turbo Ratio up to 120. This 1-Core Turbo Ratio Limit Must be greater than or equal to other Turbo Core Ratio Limit.
2-Core Turbo Ratio Limit Ratio (TRLR) Override	[Max-Value, Min-Value, Step-Value] = [0x53, 0x00, 0x01]	2-Core Turbo Ratio Limit Ratio (TRLR) with range of Max Non-Turbo Ratio up to 120. This 2-Core Turbo Ratio Limit Must be Less than or equal to 1-Core Turbo Ratio Limit.
3-Core Turbo Ratio Limit Ratio (TRLR) Override	[Max-Value, Min-Value, Step-Value] = [0x53, 0x00, 0x01]	3-Core Turbo Ratio Limit Ratio (TRLR) with range of Max Non-Turbo Ratio up to 120. This 3-Core Turbo Ratio Limit Must be Less than or equal to 1-Core Turbo Ratio Limit.
4-Core Turbo Ratio Limit Ratio (TRLR) Override	[Max-Value, Min-Value, Step-Value] = [0x53, 0x00, 0x01]	4-Core Turbo Ratio Limit Ratio (TRLR) with range of Max Non-Turbo Ratio up to 120. This 4-Core Turbo Ratio Limit Must be Less than or equal to 1-Core Turbo Ratio Limit.
Energy Efficient Turbo	Disabled, Enabled	Enable/Disable Energy Efficient Turbo Feature. This feature will opportunistically lower the turbo frequency to increase efficiency. Recommended only to disable in overclocking situations where turbo frequency must remain constant. Otherwise, leave enabled.
Config TDP Configurations	Submenu	
Config TDP Configurations	Config TDP Configurations	Config TDP Configurations

Feature	Options	Description
Enable Configurable TDP	Applies to non-cTDP, Applies to cTDP	Applies TDP initialization settings based on non-cTDP or cTDP. Default is 1: Applies to cTDP; if 0 then applies non-cTDP and BIOS will bypass cTDP initialization flow
Configurable TDP Boot Mode	Nominal , Down2, Down1, Deactivate	Configurable 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.
CTDP BIOS control	Enabled, Disabled	Enables CTDP control via runtime ACPI BIOS methods. This "BIOS only" feature does not require EC or driver support.
ConfigTDP Levels	3	
ConfigTDP Turbo Activation Ratio	27 (Unlocked)	
Power Limit 1	28.0W (MSR:28.0)	
Power Limit 2	64.0W (MSR:64.0)	
Custom Settings Nominal		
ConfigTDP Nominal	Ratio:28 TAR:27 PL1:28.0W	
Power Limit 1	[Max-Value, Min-Value, Step-Value] = [0x003E7F83, 0x00000000, 0x0000007D]	Power Limit 1 in Milli Watts. BIOS will round to the nearest 1/8W when programming. 0 = no custom override. For 12.50W, enter 12500. Overclocking SKU: Value must be between Max and Min Power Limits (specified by PACKAGE_POWER_SKU_MSR). Other SKUs: This value must be between Min Power Limit and TDP
Power Limit 2	[Max-Value, Min-Value, Step-Value] = [0x003E7F83, 0x00000000,	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
	0x0000007D]	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 Down2		
ConfigTDP Level1	Ratio:12 TAR:11 PL1:12.0W	
Power Limit 1	[Max-Value, Min-Value, Step-Value] = [0x003E7F83, 0x00000000 , 0x0000007D]	Power Limit 1 in Milli Watts. BIOS will round to the nearest 1/8W when programming. 0 = no custom override. For 12.50W, enter 12500. Overclocking SKU: Value must be between Max and Min Power Limits (specified by PACKAGE_POWER_SKU_MSR). Other SKUs: This value must be between Min Power Limit and TDP
Power Limit 2	[Max-Value, Min-Value, Step-Value] = [0x003E7F83, 0x00000000 , 0x0000007D]	Power Limit 2 value in Milli Watts. BIOS will round to the nearest 1/8W when programming. 0 = no custom override. For 12.50W, enter 12500. Processor applies control policies such that the package power does not exceed this limit.
Power Limit 1 Time Window*	0 , 1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 14, 16, 20, 24, 28, 32, 40, 48, 56, 64, 80, 96, 112, 128	Power Limit 1 Time Window value in seconds. The value may vary from 0 to 128. 0 = default value (28 sec for Mobile and 8 sec for Desktop). Defines 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 Down1		
ConfigTDP Level2	Ratio:18 TAR:17 PL1:15.0W	
Power Limit 1	[Max-Value, Min-Value, Step-Value] =	Power Limit 1 in Milli Watts. BIOS will round to the nearest 1/8W when programming. 0 = no custom

Feature	Options	Description
	[0x003E7F83, 0x00000000 , 0x0000007D]	override. For 12.50W, enter 12500. Overclocking SKU: Value must be between Max and Min Power Limits (specified by PACKAGE_POWER_SKU_MSR). Other SKUs: This value must be between Min Power Limit and TDP
Power Limit 2	[Max-Value, Min-Value, Step-Value] = [0x003E7F83, 0x00000000 , 0x0000007D]	Power Limit 2 value in Milli Watts. BIOS will round to the nearest 1/8W when programming. 0 = no custom override. For 12.50W, enter 12500. Processor applies control policies such that the package power does not exceed this limit.
Power Limit 1 Time Window*	0, 1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 14, 16, 20, 24, 28, 32, 40, 48, 56, 64, 80, 96, 112, 128	Power Limit 1 Time Window value in seconds. The value may vary from 0 to 128. 0 = default value (28 sec for Mobile and 8 sec for Desktop). Defines 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.
CPU VR Settings	Submenu	
CPU VR Settings		
PSYS Slope	[Max-Value, Min-Value, Step-Value] = [0xC8, 0x00 , 0x01]	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	[Max-Value, Min-Value, Step-Value] = [0xF9FF, 0x0000 , 0x0001]	PSYS Offset defined in 1/1000 increments. Range is 0-63999. For an offset of 25.348, enter 25348. PSYS Uses BIOS VR mailbox command 0x4.
PSYS Prefix	+, -	Sets the offset value as positive or negative.
PSYS PMax Power	[Max-Value, Min-Value, Step-Value] = [0x1FFF, 0x0000 , 0x0001]	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.
Acoustic Noise Settings	Submenu	
Acoustic Noise Mitigation	Disabled , Enabled	Enabling this option will help mitigate acoustic noise on certain SKUs when the CPU is in deeper C state

Feature	Options	Description
Pre Wake Time	[Max-Value, Min-Value, Step-Value] = [0xFF, 0x00 , 0x01]	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	[Max-Value, Min-Value, Step-Value] = [0xFF, 0x00 , 0x01]	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	[Max-Value, Min-Value, Step-Value] = [0xFF, 0x00 , 0x01]	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.
VccIn VR Domain		
Latency	[Max-Value, Min-Value, Step-Value] = [0x03FF, 0x0000, 0x0001]	Interrupt Response Time Limit value- bits [9:0], Enter 0-1023
Disable Fast PKG C State Ramp for VccIn 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 VccIn Domain	Fast/2 , Fast/4, Fast/8, Fast/16	Set VR VccIn 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
VccIn VR Settings	Submenu	
VccIn VR Domain		
VR Config Enable	Disabled, Enabled	VR Config Enable
Current AC Loadline	440	
Current DC Loadline	200	
PS Current Threshold1	[Max-Value, Min-Value, Step-Value] = [0x0200, 0x0000, 0x0001], 0x0050	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	[Max-Value, Min-Value, Step-Value] = [0x0200, 0x0000, 0x0001],	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

Feature	Options	Description
	0x0014	0x3.
PS Current Threshold3	[Max-Value, Min-Value, Step-Value] = [0x0200, 0x0000, 0x0001], 0x0004	PS Current Threshold3, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO. Uses BIOS VR mailbox command 0x3.
PS3 Enable	Disabled, Enabled	PS3 Enable/Disable. 0 - Disabled, 1 - Enabled. Uses BIOS VR mailbox command 0x3.
PS4 Enable	Disabled, Enabled	PS4 Enable/Disable. 0 - Disabled, 1 - Enabled. Uses BIOS VR mailbox command 0x3
IMON Slope	[Max-Value, Min-Value, Step-Value] = [0x00C8, 0x0000 , 0x0001]	IMON Slope defined in 1/100 increments. Range is 0-200. For a 1.25 slope, enter 125. 0 = AUTO. Uses BIOS VR mailbox command 0x4.
IMON Offset	[Max-Value, Min-Value, Step-Value] = [0xF9FF, 0x0000 , 0x0001]	IMON Offset defined in 1/1000 increments. 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	[Max-Value, Min-Value, Step-Value] = [0x03FF, 0x0000 , 0x0001]	Voltage Regulator Current Limit (Icc Max). This value represents the Maximum instantaneous current allowed at any given time. The value is represented in 1/4 A increments. A value of 400 = 100A. 0 means AUTO. Uses BIOS VR mailbox command 0x6.
TDC Enable	Disabled, Enabled	TDC Enable. 0- Disable, 1 - Enable
TDC Current Limit	[Max-Value, Min-Value, Step-Value] = [0x7FFF, 0x0000 , 0x007D]	TDC Current Limit, defined in 1/8A increments. Range 0-32767. For a TDC Current Limit of 125A, enter 1000. 0 = 0 Amps. Uses BIOS VR mailbox command 0x1A.
TDC Time Window	1 ms , 2 ms, 3 ms, 4 ms, 5 ms, 6 ms, 7 ms, 8 ms, 10 ms	TDC Time Window, value in milliseconds. 1ms is default. Range from 1ms to 10ms, except for 9ms. 9ms has no valid encoding in the MSR definition.
TDC Lock	Disabled , Enabled	TDC Lock
VccIn Demotion Override Enable	Disabled , Enabled	Enable VccIn Demotion Override Configuration.
VccIn Demotion	[Max-Value, Min-Value, Step-Value] =	Customize VccIn Shutdown Demotion in milli-second. Value 0 will disable VccIn Demotion Knob. Value 1

Feature	Options	Description
	[0x000003E8, 0x00000000, 0x00000001], 0x0000001E	means 1ms, value 2 means 2ms, and so on.
RFI Settings	Submenu	
RFI Domain		
RFI Current Frequency	139.800MHz	
RFI Frequency	[Max-Value, Min-Value, Step-Value] = [0x077E, 0x0000, 0x0000]	Set desired RFI frequency, in increments of 100KHz. (For a frequency of 100.6MHz, enter 1006.)
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
RFI Mitigation	Disabled , Enabled	Disable - DCM is the IO_N default; Enable - Enable IO_N DCM/CCM switching as RFI mitigation.
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 PL1 Power	[Max-Value, Min-Value, Step-Value] = [0x003E7F83, 0x00000000 , 0x0000007D]	Platform Power Limit 1 Power in Milli Watts. BIOS will round to the nearest 1/8W when programming. Any value can be programmed between Max and Min Power Limits (specified by PACKAGE_POWER_SKU_MSR). For 12.50W, enter 12500. This setting will act as the new PL1 value for the Package RAPL algorithm.
Platform PL1 Time Window	0 , 1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 14, 16, 20, 24, 28, 32, 40, 48, 56, 64, 80, 96, 112, 128	Platform Power Limit 1 Time Window value in seconds. The value may vary from 0 to 128. 0 = default values. Indicates the time window over which Platform TDP value should be maintained.
Platform PL2 Enable	Disabled , Enabled	Enable/Disable Platform Power Limit 2 programming. If this option is disabled, BIOS will program the default values for Platform Power Limit 2.
Platform PL2 Power	[Max-Value, Min-Value,	Platform Power Limit 2 Power in Milli Watts. BIOS will

Feature	Options	Description
	Step-Value] = [0x003E7F83, 0x00000000 , 0x0000007D]	round to the nearest 1/8W when programming. Any value can be programmed between Max and Min Power Limits (specified by PACKAGE_POWER_SKU_MSR). For 12.50W, enter 12500. This setting will act as the new PL2 value for the Package RAPL algorithm.
Power Limit 4 Override	Disabled , Enabled	Enable/Disable Power Limit 4 override. If this option is disabled, BIOS will leave the default values for Power Limit 4.
Power Limit 4	[Max-Value, Min-Value, Step-Value] = [0x003E7F83, 0x00000000 , 0x0000007D]	Power Limit 4 in Milli Watts. BIOS will round to the nearest 1/8W when programming. For 12.50W, enter 12500. If the value is 0, BIOS leaves default value
Power Limit 4 Lock	Disabled , Enabled	Power Limit 4 MSR 601h Lock. When enabled PL4 configurations are locked during OS. When disabled PL4 configuration can be changed during OS.
C states	Disabled, Enabled	Enable/Disable CPU Power Management. Allows CPU to go to C states when it's not 100% utilized.
Enhanced C-states	Disabled, Enabled	Enable/Disable C1E. When enabled, CPU will switch to minimum speed when all cores enter C-State.
C-State Auto Demotion	Disabled, C1	Configure C-State Auto Demotion
C-State Un-demotion	Disabled, C1	Configure C-State Un-demotion
Package C-State Demotion	Disabled, Enabled	Package C-State Demotion
Package C-State Un-demotion	Disabled, Enabled	Package C-State Un-demotion
CState Pre-Wake	Disabled, Enabled	Disable - Sets bit 30 of POWER_CTL MSR(0x1FC) to 1 to disable the Cstate Pre-Wake
IO MWAIT Redirection	Disabled , Enabled	When set, will map IO_read instructions sent to IO registers PMG_IO_BASE_ADDRBASE+offset to MWAIT(offset)
Package C State Limit	C0/C1, C2, C3, C6, C7, C7S, C8, C9, C10, Cpu Default, Auto , 0xFF, 0x00, 0x01	Maximum Package C State Limit Setting. Cpu Default: Leaves to Factory default value.Auto: Initializes to deepest available Package C State Limit.

Feature	Options	Description
C6/C7 Short Latency Control(MSR 0x60B)		
Time Unit	1 ns, 32 ns, 1024 ns , 32768 ns, 1048576 ns, 33554432 ns	Unit of measurement for IRTL value - bits [12:10]
Latency	[Max-Value, Min-Value, Step-Value] = [0x03FF, 0x0000 , 0x0001]	Interrupt Response Time Limit value- bits [9:0], Enter 0-1023
C6/C7 Long Latency Control(MSR 0x60C)		
Time Unit*	1 ns, 32 ns, 1024 ns , 32768 ns, 1048576 ns, 33554432 ns	Unit of measurement for IRTL value - bits [12:10]
Latency	[Max-Value, Min-Value, Step-Value] = [0x03FF, 0x0000 , 0x0001]	Interrupt Response Time Limit value- bits [9:0], Enter 0-1023
C8 Latency Control(MSR 0x633)		
Time Unit*	1 ns, 32 ns, 1024 ns , 32768 ns, 1048576 ns, 33554432 ns	Unit of measurement for IRTL value - bits [12:10]
Latency	[Max-Value, Min-Value, Step-Value] = [0x03FF, 0x0000 , 0x0001]	Interrupt Response Time Limit value- bits [9:0], Enter 0-1023
C9 Latency Control(MSR 0x634)		
Time Unit*	1 ns, 32 ns, 1024 ns , 32768 ns, 1048576 ns, 33554432 ns	Unit of measurement for IRTL value - bits [12:10]
Latency	[Max-Value, Min-Value, Step-Value] = [0x03FF, 0x0000 , 0x0001]	Interrupt Response Time Limit value- bits [9:0], Enter 0-1023
C10 Latency Control(MSR 0x635)		
Time Unit*	1 ns, 32 ns, 1024 ns , 32768 ns, 1048576 ns,	Unit of measurement for IRTL value - bits [12:10]

Feature	Options	Description
	33554432 ns	
Latency	[Max-Value, Min-Value, Step-Value] = [0x03FF, 0x0000 , 0x0001]	Interrupt Response Time Limit value- bits [9:0], Enter 0-1023
Thermal Monitor	Disabled, Enabled	Enable/Disable Thermal Monitor
Interrupt Redirection Mode Selection	Fixed Priority , Round robin, Hash Vector, No Change	Interrupt Redirection Mode Select for Logical Interrupts
Timed MWAIT	Disabled , Enabled	Enable/Disable Timed MWAIT Support
Custom P-state Table	Submenu	
Energy Performance Gain	Disabled , Enabled	Enable/disable Energy Performance Gain.
EPG DIMM Idd3N	[Max-Value, Min-Value, Step-Value] = [0x07D0, 0x0000, 0x0001] , 0x001A	Active standby current (Idd3N) in milliamps from datasheet. Must be calculated on a per DIMM basis.
EPG DIMM Idd3P	[Max-Value, Min-Value, Step-Value] = [0x07D0, 0x0000, 0x0001], 0x000B	Active power-down current (Idd3P) in milliamps from datasheet. Must be calculated on a per DIMM basis.
Power Limit 3 Settings	Submenu	
Power Limit 3 Override	Disabled , Enabled	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.
Power Limit 3	[Max-Value, Min-Value, Step-Value] = [0x003E7F83, 0x00000000 , 0x0000007D]	Power Limit 3 in Milli Watts. BIOS will round to the nearest 1/8W when programming. For 12.50W, enter 12500. XE SKU: Any value can be programmed. Overclocking SKU: Value must be between Max and Min Power Limits (specified by PACKAGE_POWER_SKU_MSR). Other SKUs: This value must be between Min Power L
Power Limit 3 Time Window	0 , 3, 4, 5, 6, 7, 8, 10, 12, 14, 16, 20, 24, 28, 32, 40, 48, 56, 64	Power Limit 3 Time Window value in Milli seconds. The value may vary from 3 to 64(max).Indicates the time window over which Power Limit 3 value should be maintained. If the value is 0, BIOS leaves the

Feature	Options	Description
		hardware default value
Power Limit 3 Duty Cycle	[Max-Value, Min-Value, Step-Value] = [0x64, 0x00, 0x00]	Specify the duty cycle in percentage that the CPU is required to maintain over the configured time window. Range is 0-100.
Power Limit 3 Lock	Disabled , Enabled	Power Limit 3 MSR 615h Lock. When enabled PL3 configurations are locked during OS. When disabled PL3 configuration can be changed during OS.
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

7.2.2.2. Advanced > Power & Performance > 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

7.2.3. Advanced > TCSS Platform Settings

Feature	Options	Description
Control Iommu Pre-boot Behavior	Disable IOMMU , Enable IOMMU during boot	Enable IOMMU in Pre-boot environment (If DMAR table is installed in DXE and If VTD_INFO_PPI is installed in PEI.)

7.2.4. Advanced > Intel® Time Coordinated Computing

Feature	Options	Description
#AC Split Lock*	Enabled, Disabled	Enable or Disable Alignment Check Exception (#AC). When enabled, this will assert an #AC when any atomic operation has an operand that crosses two cache lines.
IFU Enable*	Enabled, Disabled	Enable or Disable Instruction Fetch Unit(IFU). When enabled, Instructions will be prefetch to the cache.
Intel(R) TCC Mode*	Enabled, Disabled	Enable or Disable Intel(R) TCC Mode. When enabled, this will modify system settings to improve real-time performance. The full list of settings and their current state are displayed below when Intel(R) TCC mode is enabled.
Intel(R) TCC Authentication*	Disabled, Enabled	Enable or Disable authentication of Intel(R) TCC Subregions.
Intel(R) TCC Mode Affected Settings		
IO Fabric Low Latency*	Disabled , Enabled	Enable or Disable IO Fabric Low Latency. This will turn off some power management in the PCH IO fabrics. This option provides the most aggressive IO Fabric performance setting. S3 state is NOT supported.
GT CLOS*	Disabled , Enabled	Enable or Disable Graphics Technology(GT) Class of Service. Enable will reduce Gfx LLC allocation to minimize impact of Gfx workload on LLC

Feature	Options	Description
OPIO Recentering*	Disabled, Enabled	Enable or Disable Opio Recentering to improve Pcie latency.
C states*	Disabled, Enabled	Enable/Disable CPU Power Management. Allows CPU to go to C states when it's not 100% utilized.
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.
Intel(R) SpeedStep(tm)*	Disabled, Enabled	Allows more than two frequency ranges to be supported.
Hyper-Threading*	Disabled, Enabled	Enable or Disable Hyper-Threading Technology.
ACPI D3Cold Support*	Disabled, Enabled	Enable/Disable ACPI D3Cold support to be executed on D3 entry and exit
Low Power S0 Idle Capability*	Disabled , Enabled	This variable determines if we enable ACPI Lower Power S0 Idle Capability (Mutually exclusive with Smart connect). While this is enabled, it also disable 8254 timer for SLP_S0 support.
SA GV*	Disabled , Fixed to 1st Point, Fixed to 2nd Point, Fixed to 3rd Point, Fixed to 4th Point, Enabled	System Agent Geyserville. Can disable, fix to a specific point, or enable frequency switching.
WRC Feature*	Enabled, Disabled	Enable/Disable SA WRC(Write Cache) Feature of IOP. When enabled, supports IO devices allocating onto the ring and into LLC.
Page Close Idle Timeout*	Enabled , Disabled	Page Close Idle Timeout Control
Power Down Mode*	Auto , No Power Down, APD,PPD-DLLoff	CKE Power Down Mode Control
RC6(Render Standby)*	Disabled, Enabled	Check to enable render standby support.
DMI Link ASPM Control*	Disabled , L0s, L1, Auto	The control of Active State Power Management of the DMI Link.
PCI Express Clock Gating*	Disabled, Enabled	PCI Express Clock Gating Enable/Disable for each root port.
PCH TSN Multi-Vc*	Disabled , Enabled	Enable/Disable PCH TSN Multi Virtual Channels.

Feature	Options	Description
Legacy IO Low Latency*	Disabled, Enabled	Set to enable low latency of legacy IO. Some systems require lower IO latency irrespective of power. This is a tradeoff between power and IO latency.

7.2.5. Advanced > Graphic Configuration

Feature	Options	Description
Nxp configuration	Info Only	
Data format and Color Depth	VESA 24 bpp JEIDA 24 bpp JEIDA/vesa 18 bpp	Data format and Color Depth select
LVDS Output Mode	Dual LVDS bus Single LVDS bus	Single/Dual mode select
DE Polarity	Active High Active Low	DE Polarity select
Vsync Polarity	Active High Active Low	Vsync Polarity select
Spreading depth	No Spreading 0.5% 1.0% 1.5% 2.0% 2.5%	Clock frequency center spreading depth.
Integrated Display Configuration	Info only	
eDP/LVDS	Disabled Enabled	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.

Feature	Options	Description
	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 1	No Device Display Port HDMI DisplayPort With HDMI/DVI Compatible	DDI port 1 function choose to Display Port or HDMI
DDI port 2	No Device Display Port HDMI DisplayPort With HDMI/DVI Compatible	DDI port 2 function choose to Display Port or HDMI
DDI port 3	No Device Display Port HDMI DisplayPort With HDMI/DVI Compatible	DDI port 3 function choose to Display Port or HDMI

7.2.6. Advanced > 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:
Power Consumption	Submenu	

7.2.6.1. Advanced > Power Management > Power Consumption

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

Feature	Options	Description
VMEM	Read only	Display the sensed voltage based on hardware design
3.3VSB	Read only	Display the sensed voltage based on hardware design
VCORE	Read only	Display the sensed voltage based on hardware design

7.2.7. Advanced > System Management

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

7.2.7.1. Advanced > System Management > SEMA Flags

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

7.2.8. Advanced > Thermal Management

Feature	Options	Description
Thermal Management	Info Only	

Feature	Options	Description
DTS SMM	Disabled, Enabled	Enabled: ACPI thermal management uses DTS SMM mechanism to obtain CPU temperature values.
Tcc Activation Offset	[Max-Value, Min-Value, Step-Value] = [0x3F, 0x00, 0x00]	Offset from factory set Tcc activation temprature at which the Thermal Control Circuit must be activated. Tcc will be activated at: Tcc Activation Temp - Tcc Activation Offset. Tcc Activation Offset range is 0 to 63.
Critical Trip Point	Disabled 80 C 90 C 95 C	The value is the temperature threshold of the Critical Trip Point.
Passive Cooling Trip Point	Disabled 70 C 80 C 90 C 100 C	The value is the temperature threshold of the Passive Cooling Trip Point.
Active Cooling Trip Point	40 C 50 C 60 C 70 C Refer to BMC	This value is the temperature threshold of the active cooling trip point.
Watchdog ACPI Event Shutdown	Disabled Enabled	Watchdog ACPI Event Shutdown Enabled/Disabled
Temperature and Fan Speed	Submenu	

7.2.8.1. Advanced > Thermal Management > Thermal 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

Feature	Options	Description
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	

7.2.8.1.1 Advanced > Thermal Management > Thermal and Fan Speed > Smart Fan

Feature	Options	Description
Smart Fan	Info Only	
CPU Smart FanTemperature Source	CPU Sensor Board Sensor	CPU Smart FanTemperature Source
CPU Fan Mode	AUTO (Smart Fan) Fan Off Fan On	Select CPU Fan control mode.
Trigger Point 1	Info-only	
Trigger Temperature	45	Set the temperature value for trigger point 1 to control CPU fan.
PWM Level	25	When configured sensor reaches the trigger temperature value, set PWM level for this condition.
Trigger Point 2	Info-only	
Trigger Temperature	60	Set the temperature value for trigger point 2 to control CPU fan.
PWM Level	50	When configured sensor reaches the trigger temperature value, set PWM level for this condition.
Trigger Point 3	Info-only	
Trigger Temperature	75	Set the temperature value for trigger point 3 to control CPU fan.
PWM Level	75	When configured sensor reaches the trigger

Feature	Options	Description
		temperature value, set PWM level for this condition.
Trigger Point 4	Info-only	
Trigger Temperature	90	Set the temperature value for trigger point 4 to control CPU fan.
PWM Level	100	When configured sensor reaches the trigger temperature value, set PWM level for this condition.
Trigger Point 1	Info-only	

7.2.9. Advanced > Watchdog Timer

Feature	Options	Description
Watchdog Timer	Info only	
Power-Up Watchdog	Disabled Enabled	The Power Up Watchdog resets the system after a certain amount of time after power up. Pressing F12 during start up disables the Power Up Watchdog
Timeout	65535	Here you can enter the time the Power Up Watchdog should wait until it resets the system. The value range starts by 24 and ends by 65535
RunTime Watchdog	Disabled Enabled	The RunTime Watchdog resets the system after a certain amount of time after power up.
Timeout	90	Here you can enter the time the Runtime Watchdog should wait until it resets the system. The value range starts by 30 and ends by 65535.

7.2.10. Advanced > Super IO Configuration

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

7.2.10.1. Advanced > Super IO Configuration > IT5121E Super IO Configuration

Feature	Options	Description
IT5121E Super IO Configuration		
Serial Port 1 Configuration	Submenu	
Serial Port 2 Configuration	Submenu	
Serial Port 1 Configuration		
Serial Port 1 Configuration	Disabled, Enabled	Set Parameters of Serial Port 1
Device Settings	4;	
Change Settings	Auto, IO=3F8h; IRQ=4;, IO=3F8h; IRQ=3,4,5,6,7,9,10,11,12;, IO=2F8h; IRQ=3,4,5,6,7,9,10,11,12;, IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12;, IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12;	Select an optimal settings for Super IO Device
Change Settings	Normal, High Speed	Select an optimal settings for Super IO Device
Serial Port 2 Configuration		
Serial Port 2 Configuration	Disabled, Enabled	Set Parameters of Serial Port 2
Device Settings	3;	
Change Settings	Auto, IO=2F8h; IRQ=3;, IO=3F8h; IRQ=3,4,5,6,7,9,10,11,12;, IO=2F8h; IRQ=3,4,5,6,7,9,10,11,12;, IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12;, IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12;, Normal, High Speed	Select an optimal settings for Super IO Device

7.2.10.2. Advanced > Super IO Configuration > W83627DHGSEC Super IO Configuration

Feature	Options	Description
W83627DHGSEC Super IO Configuration		
Serial Port 1 Configuration	Submenu	
Serial Port 2 Configuration	Submenu	
Serial Port 1 Configuration		
Serial Port 1 Configuration	Disabled, Enabled	Set Parameters of Serial Port 1
Device Settings	5	
Change Settings	Auto, IO=240h; IRQ=10; IO=240h; IRQ=3,4,5,6,7,10,11,12; IO=248h; IRQ=3,4,5,6,7,10,11,12; IO=250h; IRQ=3,4,5,6,7,10,11,12; IO=258h; IRQ=3,4,5,6,7,10,11,12; IO=260h; IRQ=3,4,5,6,7,10,11,12; IO=268h; IRQ=3,4,5,6,7,10,11,12;	Select an optimal settings for Super IO Device
Serial Port 2 Configuration		
Serial Port 2 Configuration	Disabled, Enabled	Set Parameters of Serial Port 2
Device Settings	7;	
Change Settings	Auto, IO=248h; IRQ=10; IO=240h; IRQ=3,4,5,6,7,10,11,12; IO=248h; IRQ=3,4,5,6,7,10,11,12; IO=250h; IRQ=3,4,5,6,7,10,11,12; IO=258h; IRQ=3,4,5,6,7,10,11,12; IO=260h; IRQ=3,4,5,6,7,10,11,12; IO=268h; IRQ=3,4,5,6,7,10,11,12;	Select an optimal settings for Super IO Device
Device Mode	Standard Serial Port Mode, IrDA Active pulse 1.6 uS, IrDA Active pulse 3/16 bit time, ASKIR Mode	Change the Serial Port mode.

7.2.11. Advanced > Miscellaneous

Feature	Options	Description
Power Supply Unit	Emulate AT Mode ATX Mode	Select Emulation AT or ATX function. If this option set to [Emulation AT], BIOS will report no suspend functions (S3 & S4) to ACPI OS. In windows XP, it will make OS show shutdown message during system shutdown. ATX: OS will turn off system power when shutdown.
I2C Speed Control	100 kbps 400 kbps	I2C Speed Control
WOL From S5	OFF ON	This Config to control power on/off LAN in S5 State by SEMA(EC).
Smart Battery Function	Disabled Enabled Auto	Enable/Disable Smart Battery function. Auto: disable Smart Battery function if charger IC not be detected.
SMBUS Select Configuration	From EC, From PCH	SMBUS Select Configuration from PCH or EC.

7.2.12. Advanced > AMT Configuration (shown if SKU supported)

Feature	Options	Description
MEBx hotkey Pressed	Disabled , Enabled	To enable or disable console redirection of COMx.

7.2.13. Advanced > 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.
Legacy USB Support	Enabled Disabled Auto	Enables Legacy USB support. Auto option disables legacy support if no USB devices are connected. Disable option will keep USB devices available only for EFI applications.
XHCI Hand-off	Enabled Disabled	This is a workaround for 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 Storage Driver Support.
USB hardware delays and time-outs:	Info Only	
USB transfer time-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 Host Controller. 'Auto' uses default value: for a Root port it is 100 ms, for a Hub port the delay is taken from Hub descriptor.

7.2.14. Advanced > 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.

7.2.15. Advanced > 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.

7.2.15.1. Advanced > Serial Console Redirection > Console Redirection Settings

Feature	Options	Description
Terminal Type	VT100 VT100+ VT-UTF8 ANSI	Configure the type of console emulation. Emulation: ANSI: Extended ASCII char set. VT100: ASCII char set. VT100+: Extends VT100 to support color, function keys, etc. VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.
Bits per second	9600 19200 38400 57600 115200	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speed.
Data Bits	7 8	Configure the number of data bits in each transmitted or received serial character for both serial ports.
Parity	None Even Odd	Configures if parity bit is generated (transmit data) or checked. A parity bit can be sent with the data bits to detect some transmission errors. Even: 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. They can be used as an additional data bit.
Stop Bits	1 2	Configures the number of stop bits transmitted and received in each serial character for both serial ports. Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit.
Flow Control	None Hardware Software	Configures flow control for console redirection. Hardware flow control uses RTC/CTS. Software flow control uses XON/XOFF.

Feature	Options	Description
VT-UTF8 Combo Key Support	Disabled Enabled	Enable VT-UTF8 combination key support for ANSI/VT100 terminals.
Recorder Mode	Disabled Enabled	With this mode enabled only text will be sent. This is to capture terminal data.
Resolution 100x31	Disabled Enabled	Enables or disables extended terminal resolution.
Legacy OS Redirection Resolution	80x24 80x25	Set console display resolution.
Putty KeyPad	VT100 LINUX XTERMR6 SCO ESCN VT400	Select Function Keys and Key Pad on Putty.
Redirection After BIOS POST	Always Enabled BootLoader	The setting specify if BootLoader is selected, then legacy console redirection is disabled before booting to legacy OS.

7.2.16. Advanced > 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 HTTP boot support. If disabled, IPv4 HTTP 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	[Max-Value, Min-Value, Step-Value] = [0x05, 0x00 ,	Wait time in seconds to press ESC key to abort the PXE boot. Use either +/- or numeric keys to set the

Feature	Options	Description
	0x01]	value.
Media detect count	[Max-Value, Min-Value, Step-Value] =[0x32, 0x01 , 0x01]	Number of times the presence of media will be checked. Use either +/- or numeric keys to set the value.

7.2.17. Advanced > 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.

7.3. Chipset

7.3.1. Chipset > System Agent (SA) Configuration

Feature	Options	Description
Memory RC Version	Info-only	
Memory Speed	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

Feature	Options	Description
Max TOLUD	Dynamic 1 GB 1.25 GB 1.5 GB 1.75 GB 2 GB 2.25 GB 2.5 GB 2.75 GB 3 GB 3.25 GB 3.5 GB	Maximum Value of TOLUD. Dynamic assignment would adjust TOLUD automatically based on largest MMIO length of installed graphic controller
Controller 0, Channel 0 DIMM Control	Enabled , Disabled	Controller 0, Channel 0 DIMM Control Support - Enable or Disable Dimms on Controller 0, Channel 0.
Controller 1, Channel 0 DIMM Control	Enabled , Disabled	Controller 1, Channel 0 DIMM Control Support - Enable or Disable Dimms on Controller 1, Channel 0.
In-Band ECC Support (Industrial SKU only)	Enabled , Disabled	Enable/Disable In-Band ECC. Either the IBECC or the TME can be enabled.
In-Band ECC 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

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

Feature	Options	Description
Skip Scanning of External Gfx Card	Disabled , Enabled	If Enable, it will not scan for External Gfx Card on PEG and PCH PCIE Ports
Primary Display	Auto , IGFX, PEG Slot, PCH PCI, HG	Select which of IGFX/PEG/PCI Graphics device should be Primary Display Or select HG for Hybrid Gfx.

Feature	Options	Description
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, 20M, 24M, 28M, 32M/F7, 36M, 40M, 44M, 48M, 52M, 56M, 60M	Select DVMT 5.0 Pre-Allocated (Fixed) Graphics Memory size used by the Internal Graphics Device.
DVMT Total Gfx Mem	128M, 256M , MAX	Select DVMT5.0 Total Graphic Memory size used by the Internal Graphics Device.
Intel Graphics Pei Display Peim	Enabled , Disabled	Enable/Disable Pei (Early) Display

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

Feature	Options	Description
Graphics Configuration	Info Only	
Primary Display	Auto IGFX PEG PCIe	Select which of IGFX/PEG/PCIe Graphics device should be Primary Display Or select HG for Hybrid Gfx.
External Gfx Card Primary Display Configuration	Submenu	External Gfx Card Primary Display Configuration
Internal Graphics	Auto Disabled Enabled	Keep IGFX enabled based on the setup options.
GTT Size	2MB	Select the GTT Size

Feature	Options	Description
	4MB 8MB	
Aperture Size	128MB 256MB 512MB 1024MB 2048MB	Select the Aperture Size
DVMT Pre-Allocated	0M 32M 46M 96M 128M 60M	Select DVMT 5.0 Pre-Allocated (Fixed) Graphics Memory size used by the Internal Graphics Device.
DVMT Total Gfx Mem	128 256 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

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

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

7.3.1.4. Chipset > System Agent (SA) Configuration > PCIe Configuration

Feature	Options	Description
PCI Express Root Port 1	Disabled, Enabled	Control the PCI Express Root Port.
Connection Type	Built-in, Slot	Built-In: a built-in device is connected to this rootport. SlotImplemented bit will be clear. Slot: this rootport connects to user-accessible slot. SlotImplemented bit will be set.
ASPM	Disabled , L1	Set the ASPM Level:
L1 Substates	Disabled, L1.1, L1.1 & L1.2	PCI Express L1 Substates settings.L1SS cannot be enabled when CLKREQMSG is disabled
Gen3 Eq Phase3 Method	Hardware , Static Coeff.	PCIe Gen3 Equalization Phase 3 Method
Gen4 Eq Phase3 Method	Hardware , Static Coeff.	PCIe Gen3 Equalization Phase 3 Method
ACS	Disabled, Enabled	Enable/Disable Access Control Services Extended Capability
PTM	Disabled, Enabled	Enable/Disable Precision Time Measurement
DPC	Disabled, Enabled	Enable/Disable Downstream Port Containment
FOM Scoreboard Control Policy	Auto , Gen3, Gen4, Gen3/Gen4	Select the FOM Scoreboard Control Policy, when set to Auto, speed is based on TLS
VC	Disabled, Enabled	Enable/Disable Virtual Channel
Multi-VC	Disabled , Enabled	Enable/Disable Multi Virtual Channel
EDPC	Disabled, Enabled	Enable/Disable Rootport extensions for Downstream Port Containment
URR	Disabled , Enabled	PCI Express Unsupported Request Reporting Enable/Disable.
FER	Disabled , Enabled	PCI Express Device Fatal Error Reporting Enable/Disable.
NFER	Disabled , Enabled	PCI Express Device Non-Fatal Error Reporting Enable/Disable.
CER	Disabled , Enabled	PCI Express Device Correctable Error Reporting Enable/Disable.

Feature	Options	Description
CTO	Disabled , Enabled	PCI Express Completion Timer TO Enable/Disable.
SEFE	Disabled , Enabled	Root PCI Express System Error on Fatal Error Enable/Disable.
SENEFE	Disabled , Enabled	Root PCI Express System Error on Non-Fatal Error Enable/Disable.
SECE	Disabled , Enabled	Root PCI Express System Error on Correctable Error Enable/Disable.
PME SCI	Disabled, Enabled	PCI Express PME SCI Enable/Disable.
Hot Plug	Disabled , Enabled	PCI Express Hot Plug Enable/Disable.
Advanced Error Reporting	Disabled, Enabled	Advanced Error Reporting Enable/Disable.
PCIe Speed	Auto , Gen1, Gen2, Gen3, Gen4	Configure PCIe Speed
IOTG Mode	Disabled , Enabled	IOTG Mode Enable/Disable
Transmitter Half Swing	Disabled , Enabled	Transmitter Half Swing Enable/Disable.
Detect Timeout	[Max-Value, Min-Value, Step-Value] = [0xFFFF, 0x0000 , 0x0001]	The number of milliseconds reference code will wait for link to exit Detect state for enabled ports before assuming there is no device and potentially disabling the port.
P2P Support	Disabled , Enabled	Program P2P Support Registers according to setup option
SA PCIe LTR Configuration		
LTR	Disabled, Enabled	SA PCIE Latency Reporting Enable/Disable
Snoop Latency Override	Disabled, Manual, Auto	Snoop Latency Override for SA PCIE.
Snoop Latency Value	[Max-Value, Min-Value, Step-Value] = [0x03FF, 0x0000, 0x0001]	LTR Snoop Latency value of SA PCIE
Snoop Latency Multiplier	1 ns, 32 ns, 1024 ns , 32768 ns, 1048576 ns, 33554432 ns	LTR Snoop Latency Multiplier of SA PCIE
Non Snoop Latency Override	Disabled, Manual, Auto	Non Snoop Latency Override for SA PCIE.

Feature	Options	Description
Non Snoop Latency Value	[Max-Value, Min-Value, Step-Value] = [0x03FF, 0x0000, 0x0001]	LTR Non Snoop Latency value of PCH PCIE
Non Snoop Latency Multiplier	1 ns, 32 ns, 1024 ns , 32768 ns, 1048576 ns, 33554432 ns	LTR Non Snoop Latency Multiplier of SA PCIE
Force LTR Override	Disabled , Enabled	Force LTR Override for SA PCIE.
LTR Lock	Disabled , Enabled	PCIE LTR Configuration Lock
CPU PCIe Gen3 HWEQ Config		
UPTP	[Max-Value, Min-Value, Step-Value] = [0x0A, 0x00, 0x01]	Upstream Port Transmitter Preset
DPTP	[Max-Value, Min-Value, Step-Value] = [0x0A, 0x00, 0x01]	Downstream Port Transmitter Preset
CPU PCIe Gen4 HWEQ Config		
UPTP	[Max-Value, Min-Value, Step-Value] = [0x0A, 0x00, 0x01]	Upstream Port Transmitter Preset
DPTP	[Max-Value, Min-Value, Step-Value] = [0x0A, 0x00, 0x01]	Downstream Port Transmitter Preset

7.3.2. Chipset > PCH-IO Configuration

Feature	Options	Description
PCI Express Configuration	Submenu	
SATA Configuration	Submenu	
USB Configuration	Submenu	
Security Configuration	Submenu	

Feature	Options	Description
HD Audio Configuration	Submenu	
Seriallo Configuration	Submenu	
PCH LAN Controller	Info-Only	No GbE Region
Port 80h Redirection	Fixed setting - LPC Bus	Control where the Port 80h cycles are sent.
Enhance Port 80h LPC Decoding	Enabled , Disabled	Support the word/dword decoding of port 80h behind LPC
Enable TCO Timer	Disabled , Enabled	Enable/Disable TCO timer. When disabled, it disables PCH ACPI timer, stops TCO timer, and ACPI WDAT table will not be published.
Pcie PII SSC	Auto , 0.0%, 0.1%, 0.2%, 0.3%, 0.4%, 0.5%, 0.6%, 0.7%, 0.8%, 0.9%, 1.0%, 1.1%, 1.2%, 1.3%, 1.4%, 1.5%, 1.6%, 1.7%, 1.8%, 1.9%, 2.0%, Disable	Pcie PII SSC percentage.AUTO - Keep hw default, no BIOS override. Range is 0.0%-2.0%.
SPD Write Disable	TRUE , FALSE	Enable/Disable setting SPD Write Disable. For security recommendations, SPD write disable bit must be set.

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

Feature	Options	Description
DMI Link ASPM Control	Disabled , L0s, L1, L0sL1, Auto	The control of Active State Power Management of the DMI Link.
Port8xh Decode	Disabled , Enabled	PCI Express Port8xh Decode Enable/Disable.
PCIE Ports 5-8 Configuration	4x1 Port , 1x2 2x1 Port, 2x2 Port, 1x4 Port	To configure PCI-E Port 5-8 of PCH.[4X1]:Port 1-4 (x1) and Port 8 (x1) / [1x2 2x1]:Port 1 (x2), Port 2 (disabled), Ports 3 and Port 4 (x1) / [2x2]:Port 1-2 (x2) and Port 3-4 (x2) / [1x4]:Port 1 (x4), Ports 2-4 (disabled)
PCI Express Root Port 5 (COMe	Submenu	

Feature	Options	Description
Lane 0)		
PCI Express Root Port 6 (COMe Lane 1)	Submenu	
PCI Express Root Port 7 (COMe Lane 2)	Submenu	
PCI Express Root Port 8 (COMe Lane 3)	Submenu	
PCI Express Root Port 9 (LAN I225)	Submenu	
PCI Express Root Port 10 (COMe Lane 4~7 (option))	Submenu	

7.3.2.1.1 Advanced > PCH-IO Configuration > PCI Express Configuration > PCI Express Root Port

Feature	Options	Description
PCI Express Root Port	Disabled Enable	Control the PCI Express Root Port.
Topology	Board specific Unknown x1 x4 Sata Express M2	Identify the SATA Topology: Default, ISATA, Flex, DirectConnect or M2.
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; Disabled - Disables ASPM

Feature	Options	Description
L1 Substates	Disabled L1.1 L1.1 & L1.2	PCI Express L1 Substates settings.
Gen3 Eq Phase3 Method	Hardware Static Coeff.	PCIe Gen3 Equalization Phase 3 Method
UPTP	5	Upstream Port Transmitter Preset
DPTP	7	Downstream Port Transmitter Preset
ACS	Disabled Enable	Enable/Disable Access Control Services Extended Capability
PTM	Disabled Enable	Enable/Disable Precision Time Measurement
DPC	Disabled Enable	Enable/Disable Downstream Port Containment
EDPC	Disabled Enable	Enable/Disable Rootport extensions for Downstream Port Containment
URR	Disabled Enable	PCI Express Unsupported Request Reporting Enable/Disable.
FER	Disabled Enable	PCI Express Device Fatal Error Reporting Enable/Disable.
NFER	Disabled Enable	PCI Express Device Non-Fatal Error Reporting Enable/Disable.
CER	Disabled Enable	PCI Express Device Correctable Error Reporting Enable/Disable.
CTO	Disabled Enable	PCI Express Completion Timer TO Enable/Disable
SEFE	Disabled Enable	Root PCI Express System Error on Fatal Error Enable/Disable.
SENFE	Disabled Enable	Root PCI Express System Error on Non-Fatal Error Enable/Disable.

Feature	Options	Description
SECE	Disabled Enable	Root PCI Express System Error on Correctable Error Enable/Disable.
PME SCI	Disabled Enable	PCI Express PME SCI Enable/Disable.
Hot Plug	Disabled Enable	PCI Express Hot Plug Enable/Disable.
Advanced Error Reporting	Disabled Enable	Advanced Error Reporting Enable/Disable.
PCIe Speed	Auto Gen1 Gen2 Gen3	Configure PCIe Speed.
Transmitter Half Swing	Disabled Enabled	Transmitter Half Swing Enable/Disable.
Detect Non-Compliance	Disabled Enable	Detect Non-Compliance PCI Express Device. If enabled, it will take more time at POST time.
Detect Timeout	0	The number of milliseconds reference code will wait for link to exit Detect state for enabled ports before assuming there is no device and potentially disabling the port.
Extra Bus Reserved	0	Extra Bus Reserved (0-7) for bridges behind this Root Bridge.
Reserved Memory	10	Reserved Memory for this Root Bridge (1-20) MB.
Reserved I/O	4	Reserved I/O (4K/8K/12K/16K/20K) Range for this Root Bridge.
PCH PCIe LTR Configuration	Info only	
LTR	Disabled Enable	PCH PCIE Latency Reporting Enable/Disable.
Snoop Latency Override	Disabled Manual Auto	Snoop Latency Override for PCH PCIE. Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow."

Feature	Options	Description
Non Snoop Latency Override	Disabled Manual Auto	Non Snoop Latency Override for PCH PCIE. Disabled: Disable override.Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.
Force LTR Override	Disabled Enable	Force LTR Override for PCH PCIE.
LTR Lock	Disabled Enable	PCIE LTR Configuration Lock

7.3.2.2. Chipset > PCH-IO Configuration > SATA Configuration

Feature	Options	Description
SATA Controller(s)	Disabled, Enabled	Enable/Disable SATA Device.
SATA Controller Speed	Default, Gen1, Gen2 , Gen3	Indicates the maximum speed the SATA controller can support.
Serial ATA Port X	Info-Only	
Software Preserve	Info-Only	
Port X	Disabled, Enabled	Enable or Disable SATA Port
Hot Plug	Disabled , Enabled	Designates this port as Hot Pluggable.
Configured as eSATA	Info Only	
External	Disabled , Enabled	Marks this port as external.
Spin Up Device	Disabled , Enabled	If enabled for any of ports Staggered Spin Up will be performed and only the drives which have this option enabled will spin up at boot. Otherwise all drives spin up at boot.
SATA Device Type	Hard Disk Drive , Solid State Drive	Identify the SATA port is connected to Solid State Drive or Hard Disk Drive

7.3.2.3. Chipset > PCH-IO Configuration > USB Configuration

Feature	Options	Description
xDCI Support	Disabled, Enabled	Enable/Disable xDCI (USB OTG Device).
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 Port Disable Override	Disabled , Select Per-Pin	Selectively Enable/Disable the corresponding USB port from reporting a Device Connection to the controller.
USB SS Physical Connector #0	Disabled, Enabled	Enable/Disable this USB Physical Connector (physical port). Once disabled, any USB devices plug into the connector will not be detected by BIOS or OS.
USB SS Physical Connector #1	Disabled, Enabled	Enable/Disable this USB Physical Connector (physical port). Once disabled, any USB devices plug into the connector will not be detected by BIOS or OS.
USB SS Physical Connector #2	Disabled, Enabled	Enable/Disable this USB Physical Connector (physical port). Once disabled, any USB devices plug into the connector will not be detected by BIOS or OS.
USB SS Physical Connector #3	Disabled, Enabled	Enable/Disable this USB Physical Connector (physical port). Once disabled, any USB devices plug into the connector will not be detected by BIOS or OS.
USB HS Physical Connector #0	Disabled, Enabled	Enable/Disable this USB Physical Connector (physical port). Once disabled, any USB devices plug into the connector will not be detected by BIOS or OS.
USB HS Physical Connector #1	Disabled, Enabled	Enable/Disable this USB Physical Connector (physical port). Once disabled, any USB devices plug into the connector will not be detected by BIOS or OS.
USB HS Physical Connector #2	Disabled, Enabled	Enable/Disable this USB Physical Connector (physical

Feature	Options	Description
		port). Once disabled, any USB devices plug into the connector will not be detected by BIOS or OS.
USB HS Physical Connector #3	Disabled, Enabled	Enable/Disable this USB Physical Connector (physical port). Once disabled, any USB devices plug into the connector will not be detected by BIOS or OS.
USB HS Physical Connector #4	Disabled, Enabled	Enable/Disable this USB Physical Connector (physical port). Once disabled, any USB devices plug into the connector will not be detected by BIOS or OS.
USB HS Physical Connector #5	Disabled, Enabled	Enable/Disable this USB Physical Connector (physical port). Once disabled, any USB devices plug into the connector will not be detected by BIOS or OS.
USB HS Physical Connector #6	Disabled, Enabled	Enable/Disable this USB Physical Connector (physical port). Once disabled, any USB devices plug into the connector will not be detected by BIOS or OS.
USB HS Physical Connector #7	Disabled, Enabled	Enable/Disable this USB Physical Connector (physical port). Once disabled, any USB devices plug into the connector will not be detected by BIOS or OS.

7.3.2.4. 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

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

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

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

Feature	Options	Description
I2C3 Controller	Disabled, Enabled	Enables/Disables Seriallo Controller
I2C4 Controller	Disabled, Enabled	Enables/Disables Seriallo Controller
UART0 Controller	Disabled , Enabled, Communication port (COM)	Enables/Disables Seriallo Controller
UART1 Controller	Disabled , Enabled, Communication port (COM)	Enables/Disables Seriallo Controller
GPIO IRQ Route	IRQ14 , IRQ15	Route all GPIOs to one of the IRQ.

7.4. Security

Feature	Options	Description
Password Description	Info only	
Administrator Password	Enter password	
User Password	Enter password	
Secure Boot menu	submenu	

7.4.1. Security > Secure Boot Menu

Feature	Options	Description
Secure Boot	Info only	
Secure Boot Control	Disabled Enabled	Secure Boot feature is Active if Secure Boot is Enabled, platform Key(PK) is enrolled and the System is in User mode, The mode change requires platform reset

7.5. Boot

7.5.1. Boot > Boot Configuration

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

Feature	Options	Description
	Enabled	
Boot Configuration	Info only	
Boot Option Priorities	Info only	

7.6. Save & Exit

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

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



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

Viewing Checkpoints

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

Aptio V Checkpoint and Beep Codes

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

8.1. Status Code Ranges

Status Code Range	Description
0x01 – 0x0B	SEC execution
0x0C – 0x0F	SEC errors
0x10 – 0x2F	PEI execution up to and including memory detection
0x30 – 0x4F	PEI execution after memory detection
0x50 – 0x5F	PEI errors
0x60 – 0x8F	DXE execution up to BDS
0x90 – 0xCF	BDS execution
0xD0 – 0xDF	DXE errors
0xE0 – 0xE8	S3 Resume (PEI)
0xE9 – 0xEF	S3 Resume errors (PEI)
0xF0 – 0xF8	Recovery (PEI)
0xF9 – 0xFF	Recovery errors (PEI)

8.2. Standard Status Codes

8.2.1. SEC Phase

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

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

8.2.2. SEC Beep Codes

None

8.2.3. PEI Phase

Status Code	Description
Progress Codes	
0x10	PEI Core is started
0x11	Pre-memory CPU initialization is started
0x12	Pre-memory CPU initialization (CPU module specific)
0x13	Pre-memory CPU initialization (CPU module specific)
0x14	Pre-memory CPU initialization (CPU module specific)
0x15	Pre-memory North Bridge initialization is started
0x16	Pre-Memory North Bridge initialization (North Bridge module specific)
0x17	Pre-Memory North Bridge initialization (North Bridge module specific)
0x18	Pre-Memory North Bridge initialization (North Bridge module specific)
0x19	Pre-memory South Bridge initialization is started
0x1A	Pre-memory South Bridge initialization (South Bridge module specific)
0x1B	Pre-memory South Bridge initialization (South Bridge module specific)
0x1C	Pre-memory South Bridge initialization (South Bridge module specific)
0x1D – 0x2A	OEM pre-memory initialization codes
0x2B	Memory initialization. Serial Presence Detect (SPD) data reading
0x2C	Memory initialization. Memory presence detection
0x2D	Memory initialization. Programming memory timing information

Status Code	Description
0x2E	Memory initialization. Configuring memory
0x2F	Memory initialization (other).
0x30	Reserved for ASL (see ASL Status Codes section below)
0x31	Memory Installed
0x32	CPU post-memory initialization is started
0x33	CPU post-memory initialization. Cache initialization
0x34	CPU post-memory initialization. Application Processor(s) (AP) initialization
0x35	CPU post-memory initialization. Boot Strap Processor (BSP) selection
0x36	CPU post-memory initialization. System Management Mode (SMM) initialization
0x37	Post-Memory North Bridge initialization is started
0x38	Post-Memory North Bridge initialization (North Bridge module specific)
0x39	Post-Memory North Bridge initialization (North Bridge module specific)
0x3A	Post-Memory North Bridge initialization (North Bridge module specific)
0x3B	Post-Memory South Bridge initialization is started
0x3C	Post-Memory South Bridge initialization (South Bridge module specific)
0x3D	Post-Memory South Bridge initialization (South Bridge module specific)
0x3E	Post-Memory South Bridge initialization (South Bridge module specific)
0x3F-0x4E	OEM post memory initialization codes
0x4F	DXE IPL is started
PEI Error Codes	
0x50	Memory initialization error. Invalid memory type or incompatible memory speed

Status Code	Description
0x51	Memory initialization error. SPD reading has failed
0x52	Memory initialization error. Invalid memory size or memory modules do not match.
0x53	Memory initialization error. No usable memory detected
0x54	Unspecified memory initialization error.
0x55	Memory not installed
0x56	Invalid CPU type or Speed
0x57	CPU mismatch
0x58	CPU self test failed or possible CPU cache error
0x59	CPU micro-code is not found or micro-code update is failed
0x5A	Internal CPU error
0x5B	reset PPI is not available
0x5C-0x5F	Reserved for future AML error codes
S3 Resume Progress Codes	
0xE0	S3 Resume is started (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 AML 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 (Install Pei Memory routine in PEI Core called twice)
2	Recovery started
3	DXE IPL was not found
3	DXE Core Firmware Volume was not found
4	Recovery failed
4	S3 Resume failed
7	Reset PPI is not available

8.2.5. DXE Status Codes

Status Code	Description
0x60	DXE Core is started
0x61	NVRAM initialization
0x62	Installation of the South Bridge Runtime Services
0x63	CPU DXE initialization is started
0x64	CPU DXE initialization (CPU module specific)
0x65	CPU DXE initialization (CPU module specific)
0x66	CPU DXE initialization (CPU module specific)
0x67	CPU DXE initialization (CPU module specific)
0x68	PCI host bridge initialization
0x69	North Bridge DXE initialization is started
0x6A	North Bridge DXE SMM initialization is started
0x6B	North Bridge DXE initialization (North Bridge module specific)
0x6C	North Bridge DXE initialization (North Bridge module specific)
0x6D	North Bridge DXE initialization (North Bridge module specific)
0x6E	North Bridge DXE initialization (North Bridge module specific)
0x6F	North Bridge DXE initialization (North Bridge module specific)
0x70	South Bridge DXE initialization is started
0x71	South Bridge DXE SMM initialization is started
0x72	South Bridge devices initialization
0x73	South Bridge DXE Initialization (South Bridge module specific)

Status Code	Description
0x74	South Bridge DXE Initialization (South Bridge module specific)
0x75	South Bridge DXE Initialization (South Bridge module specific)
0x76	South Bridge DXE Initialization (South Bridge module specific)
0x77	South Bridge DXE Initialization (South Bridge module specific)
0x78	ACPI module initialization
0x79	CSM initialization
0x7A – 0x7F	Reserved for future AMI DXE codes
0x80 – 0x8F	OEM DXE initialization codes
0x90	Boot Device Selection (BDS) phase is started
0x91	Driver connecting is started
0x92	PCI Bus initialization is started
0x93	PCI Bus Hot Plug Controller Initialization
0x94	PCI Bus Enumeration
0x95	PCI Bus Request Resources
0x96	PCI Bus Assign Resources
0x97	Console Output devices connect
0x98	Console input devices connect
0x99	Super IO Initialization
0x9A	USB initialization is started
0x9B	USB Reset
0x9C	USB Detect
0x9D	USB Enable

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 (Load Image returned error)
0xDA	Boot Option is failed (Start Image returned error)
0xDB	Flash update is failed
0xDC	Reset protocol is not available

8.2.6. DXE Beep Codes

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

8.2.7. ACPI/ASL Checkpoint

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

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

8.3. OEM-Reserved Checkpoint Ranges

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

9. Software Support

9.1. Windows 10 IOT Enterprise 64-bit

9.2. Yocto Linux 64-bit

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

9.3. Ubuntu

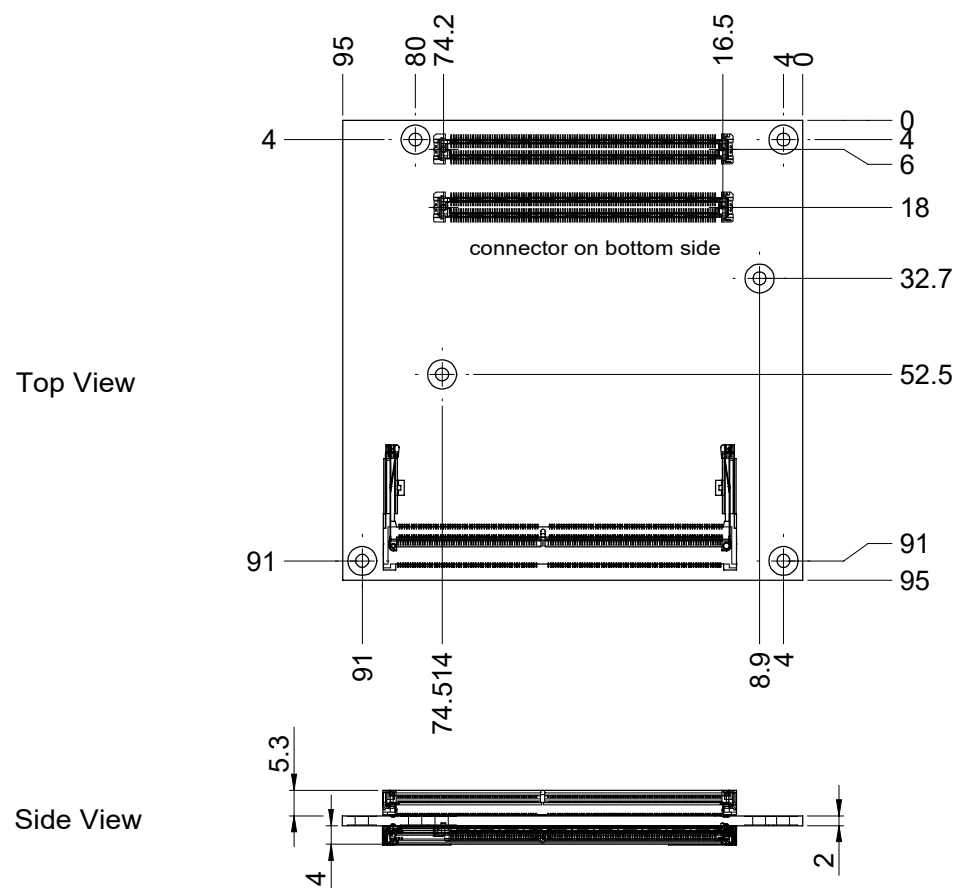
Under planning, TBC

9.4. VxWorks 64-bit

Under planning, TBC

10. Mechanical and Thermal

10.1. Module Dimensions



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

Dimensions: mm

Figure 5 – Module mechanical dimensions

10.2. Thermal Solutions

10.2.1. Heatspreader: HTS

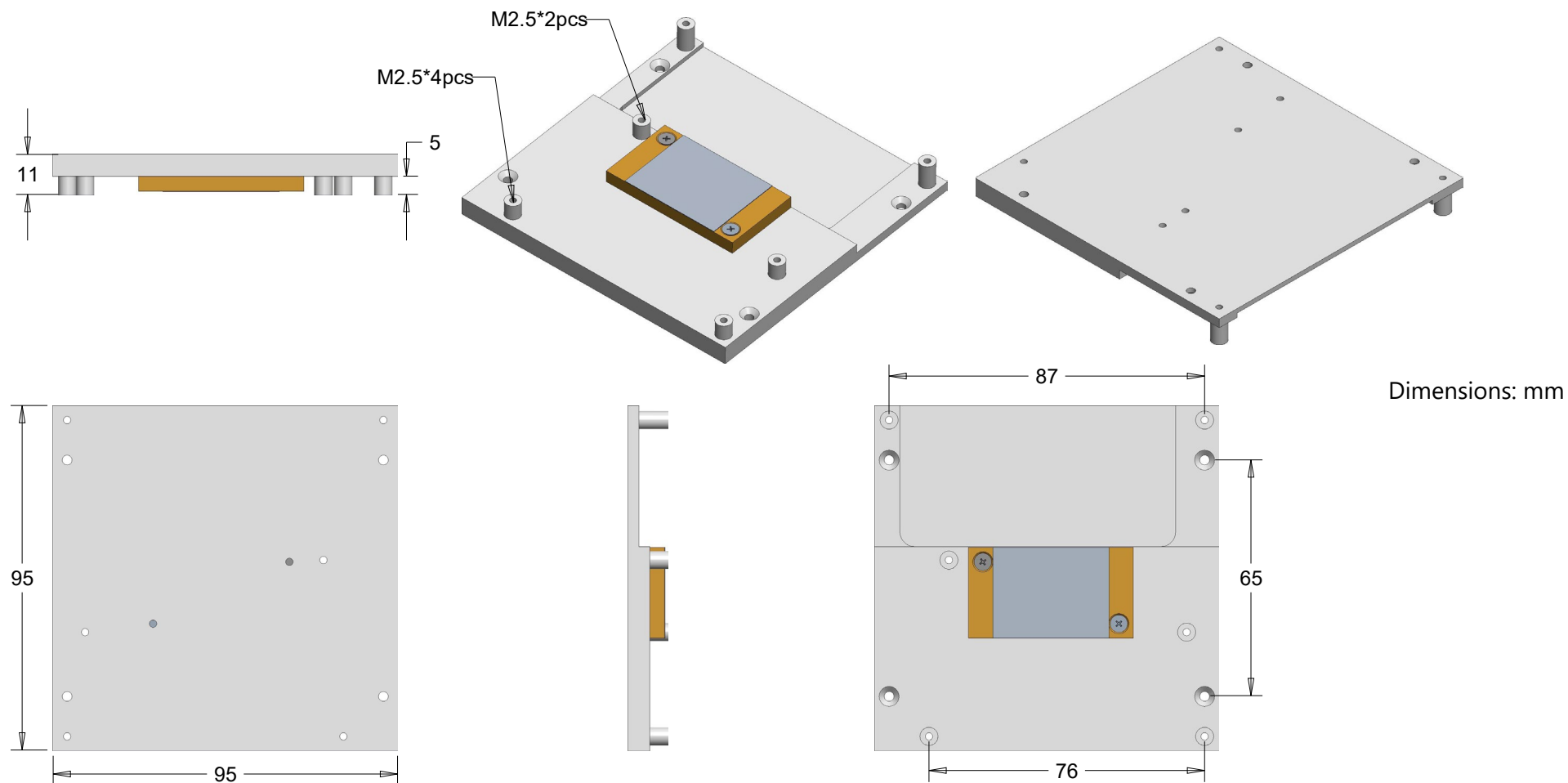


Figure 6 – Heatspreader: HTS

10.2.2. Heatsink: THS

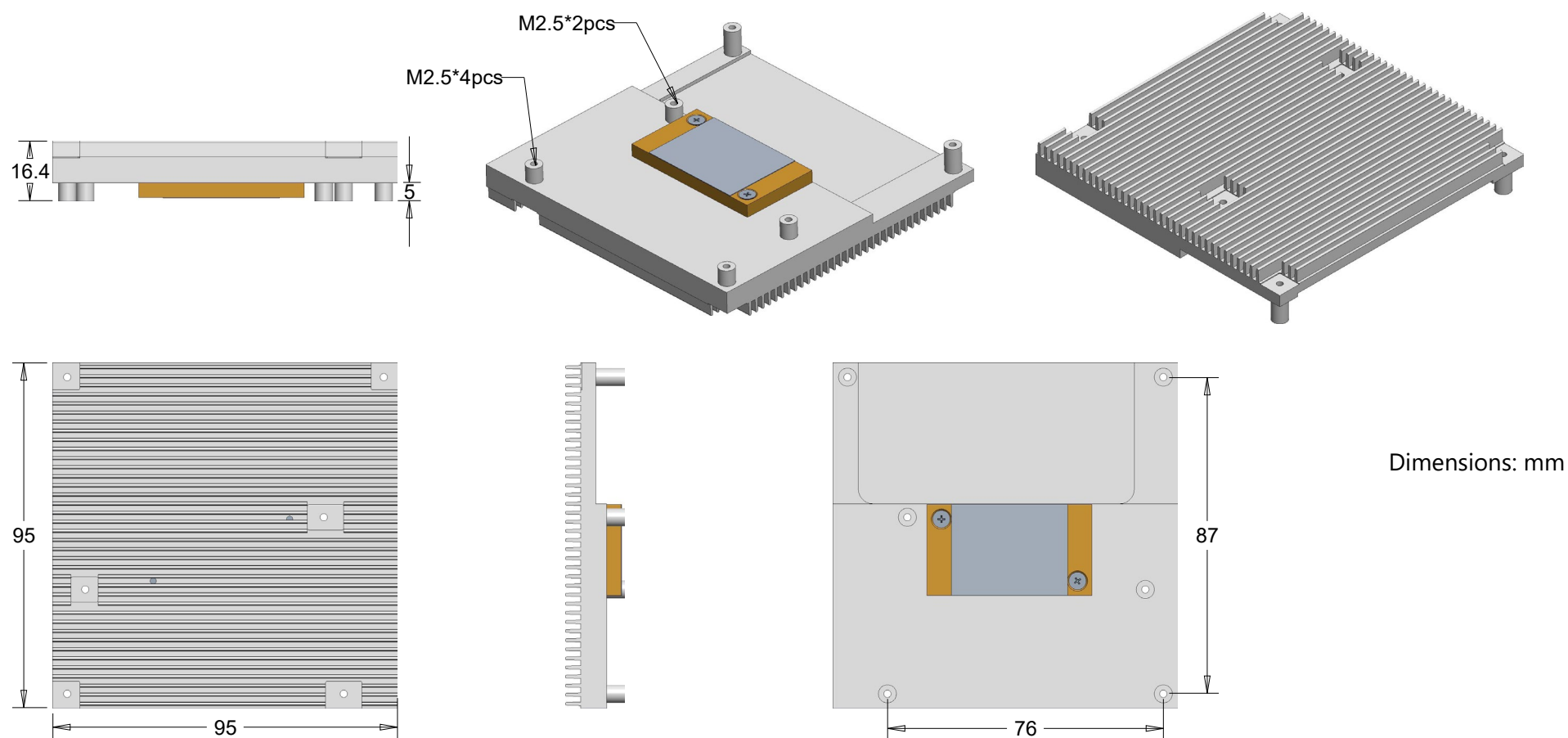


Figure 7 – Heatsink: THS

10.2.3. Heatsink High Profile: THSH

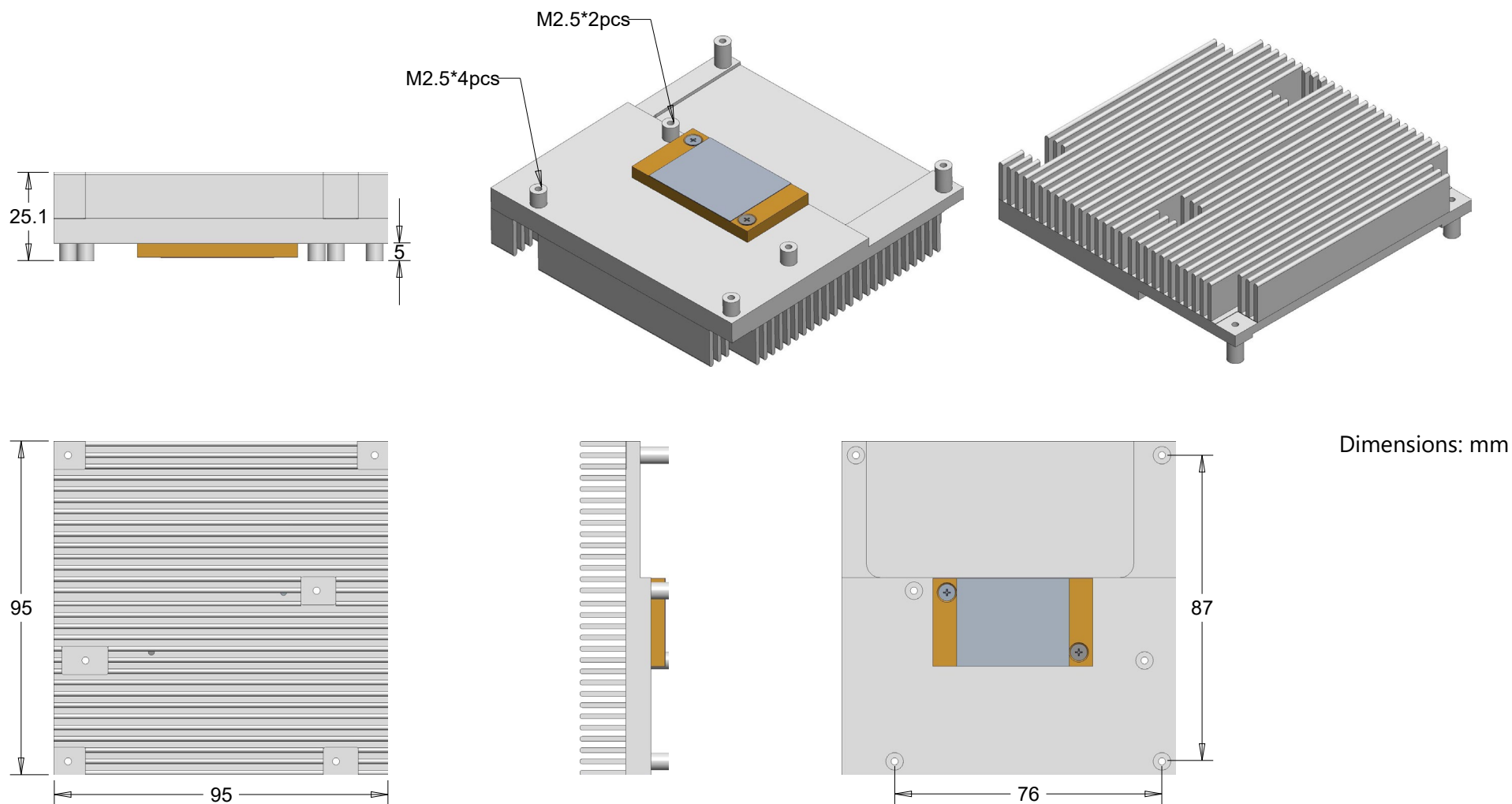


Figure 8 – Heatsink High Profile: THSH

10.2.4. Heatsink with Fan: THSF

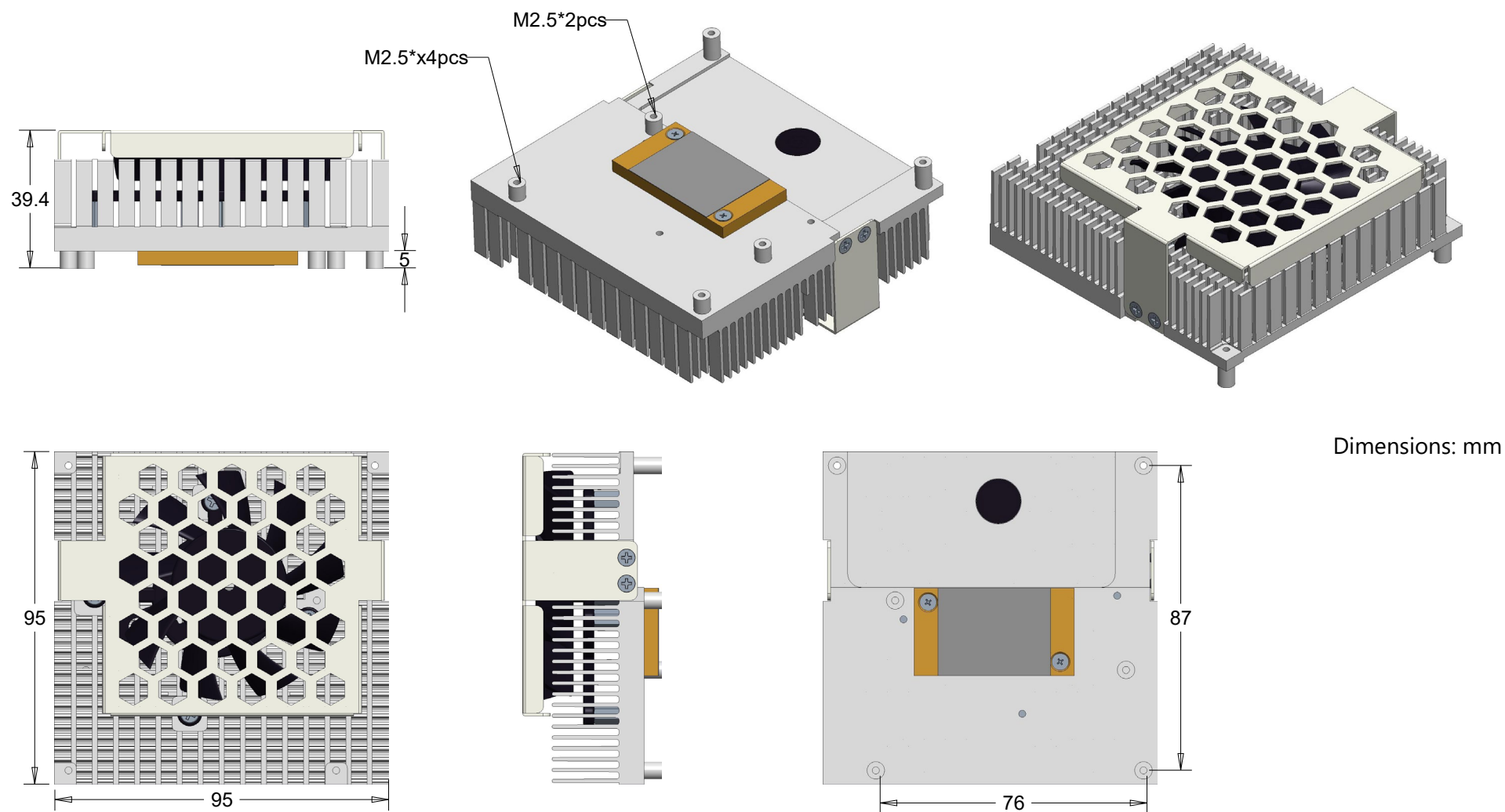


Figure 9 – Heatsink with Fan: THSF